

Standards Today

A Journal of News, Ideas and Analysis

A publication of
**CONSORTIUM
INFO.ORG**
GesmerUpdegrove^{LLP}

July 2013

Vol. XII, No. 1

THE VALUE OF OPEN STANDARDS

ABOUT THIS ISSUE: [Whose Standard is This?](#)..... 2
Should you care where your standards come from?

EDITORIAL: [The Dollars and Sense of Open Standards](#)..... 4
Whether using standards that are “open” can save money is an important question, but not as important as knowing whether they will be effective in protecting fundamental rights.

FEATURE ARTICLE: [Measuring the Benefits of Open Standards:
A Contribution to Dutch Politics](#) 6

In 2011 the Dutch Court of Audit released a report on the benefits of using open standards and open source software for government IT, concluding that there were hardly any benefits to be gained. The Court's underlying research was widely criticized. In this article, the authors analyze the report's omissions and weaknesses, introduce an economic framework for evaluating standardization, apply that framework to the subject of switching costs, and conclude that the framework, in combination with elements from other existing methodologies, can provide a starting point for more systematically performing international policy research relating to the benefits of open standards.

CASE WATCH: [Judge Robart's Opinion in Motorola vs.
Microsoft and the Future of FRAND](#)..... 19

It took Judge Robart 207 pages to decide what a “fair, reasonable and non-discriminatory” price would be for the use of Motorola’s “Standards Essential Patents.” A standards setting organization could have done so in a few sentences.

STANDARDS BLOG: [The Problem with Patents: Operating with
Blunt Instruments](#) 23

The U.S. patent system has been taking heavy fire for years from critics who contend that it is “irretrievably broken.” This year, those critics gained a new supporter: President Obama – at least when it comes to patents wielded by “non-practicing entities.”

CONSIDER THIS: [The Devil's in the Cloud: It's Time to Stop
our Headlong Rush into Cyber Insecurity](#) 26

Ten years from now, most of the data, hardware and software in any nation will be housed in a few hundred enormous data farms, heavily defended against cyberattack – and completely vulnerable to kinetic weapons. Remember something called “war?”

Standards Today is a free electronic Journal sponsored by the Boston law firm of Gesmer Updegrove LLP. For a free subscription, [complete the form](#) at <http://www.consortiuminfo.org/subscribe/subscribe.php?addentry=1>. Please direct questions or comments about Standards Today or ConsortiumInfo.org to Andrew Updegrove at updegrove@consortiuminfo.org, or by telephone at 617/350-6800. To learn more about Gesmer Updegrove's standards and open source practice, [visit](http://tinyurl.com/buyek4d): <http://tinyurl.com/buyek4d>, or contact Andrew Updegrove.

© 2013 Andrew Updegrove. All rights reserved.

ABOUT THIS ISSUE:

Whose Standard is This?

Andrew Updegrove



In the last issue of *Standards Today*, I tackled the always contentious question of what we really mean when we call a specification an “open standard.” In this issue, I take on an even thornier inquiry: are there greater advantages to be gained from complying with a standard that is “open” than with one that is not?

The value of open standards in comparison to ones that are proprietary, or the product of a process that is not open to all, has never been more relevant. In particular, because policy debates are being held in Europe and elsewhere relating to whether openness should be mandated in government procurement of standards-compliant products and services. These debates are complicated by the equally vexing question of how “open” should be defined, and how “open” is open enough. Absent precision in the definition of openness, vendors can’t know which standards to preferentially adopt, and disagreements can arise over whether procurement directives have in fact been met.

So it is that this issue will focus on whether requiring compliance with open standards can convey advantages, and also what types of advantages – direct and indirect, economic and otherwise – these might be.

In my *Editorial*, I argue that in the public sector, the positive downstream economic (and other) impacts of requiring compliance with only open standards will often far outweigh the immediate impact that altering standards-related rules might have on the costs of goods and services procured by governments.

In a change from my usual practice, the *Feature Article* for this month was contributed by two guest authors who believe that the Dutch government has incorrectly evaluated the value of open standards in government procurement. I’m particularly pleased to be able to expose this paper to a wider audience (it was previously delivered at two conferences), because thoroughly researched and persuasively argued analyses of the economic dimensions of openness work are rare.

In a new occasional feature I call *Case Watch*, you’ll find a report on another definition that seems to defy consensus. Unhappily, it applies to one of the most fundamental concepts relating to standards. The defined term is FRAND, which stands for “fair, reasonable and non-discriminating,” and is used in reference to licensing a patent claim that would be unavoidably infringed by implementing a standard. Recently it took a U.S. federal judge 207 pages to provide the answer. I argue that there has to be (and in fact is) a better way.

In my *Standards Blog* selection for this month, I turn to another aspect of the same problem: the parlous state of patents in the United States today. For years now, many in the tech sector (and most especially those in the software field) have bemoaned this sad state of affairs, contending that patents are too easy to get, that bad ones are too difficult and expensive to break, and that more and more companies are getting into the game of buying up patents simply to assert them. Earlier this year, no less a personage than President Obama entered the debate on the side of those who are critical of such “non-practicing entities” (also known as NPEs, or, less charitably, as “trolls”).

As always, I close with a more free-form and (I hope) provocative *Consider This* essay. The topic is one that I've addressed before – cyber security – but from a perspective that I can almost guarantee you have never seen it addressed before. If the story I spin scares the bejeebers out of you, that would be a good thing. Why? Because everything you'll read could happen very soon, and no one is doing anything to stop it from happening.

As always, I hope you enjoy this issue. But either way, it's always great to hear what you think. Let me know, why don't you? My email address is andrew.updegrove@gesmer.com

Andrew Updegrove
Editor and Publisher
2005 ANSI President's
Award for Journalism

The complete series of Standards Today issues can be accessed on-line at <http://www.consortiuminfo.org/bulletins/> It can also be found in libraries around the world as part of the EBSCO Publishing bibliographic and research databases

Sign up for a [free subscription](#) to **Standards Today** at

<http://www.consortiuminfo.org/subscribe/2.php?addentry=1>

EDITORIAL:

The Dollars and Sense of Open Standards

Andrew Updegrove

A perennial challenge faced by standards advocates is how to quantify the economic benefits they contend standards can provide. Absent such data, it can be difficult to convince those in positions of authority that the expense of developing, promoting and requiring compliance with standards is justified. Happily, although well-researched data in this area has been surprisingly hard to come by, knowledgeable policy makers and industry leaders have long acknowledged the value of standards to society, safety and commerce.

A finer question is whether the way in which a standard has been created can have impact on its value. That query can be sliced even finer when it is recognized that there can be many different types of value, and also that what may benefit one type of stakeholder may sometimes burden another, at least in the near term.

Because standards can come from many sources, from most proprietary (based on products that have become dominant in the marketplace) through various gradations (e.g., self-selected groups of companies forming special interest groups to pool patent rights underlying a single specification) to least proprietary (open-membership, consensus-based, non-profit organizations).

The true value of open standards should not be assessed in purely economic terms.

One result of this reality has been an effort to differentiate standards deemed to be less virtuous from those thought to be less so – the latter usually being referred to as “open standards.” Depending on the person doing the differentiating, the criteria may relate to the process employed in the development of the standard and those permitted to participate, or to the terms under which the resulting standards (and any underlying intellectual property rights) are made available, or to both.

From an economic point of view, however, saying why one standard is “good” and another (impliedly) is “bad” needs to be supported by results in the marketplace, or the exercise is simply an exercise in abstraction. Unless those results can be demonstrated, it’s not easy to get anyone to care which type of standards they should prefer.

In addressing that question it’s important to realize that the economic values associated with open standards can be indirect as well as direct. For example, the Cabinet Office of the United Kingdom is currently rolling out a program requiring that open standards be used in all government procurement to the greatest extent feasible. This is not only because those responsible for the policy believe that this will lower the costs of public procurement (the direct benefit), but also because it is expected that this policy will result in a more level playing field for domestic small and medium size information technology vendors, allowing them to successfully bid for more government work (the indirect benefit).

The use of standards can provide other types of economic value that may be very difficult to measure, such as losses avoided through the use of robust security standards. And they can

also provide important benefits that aren't economic at all, such as protecting privacy, ensuring equal access to government resources, and supporting the right to choose products of one's choice. Standards such as these should be regarded as having a different type of value than those that define a purely technical element of (say) a communications standard.

All of which makes it difficult to quantify what the true value of an "open" standard as compared to a "closed" one may be, or even to agree on an across the board definition of what "open" should mean for such purposes. Indeed, if there is consensus over any element of this question, it is likely to be that the answer will often depend on the context.

What should not become lost in this debate is the realization that the true value of open information and communications technology standards in many public contexts should not be assessed in purely economic terms. Public rights such as privacy, access to the political process, security and equal opportunity are not only insusceptible to mathematical measurement, but run to the core of the foundations of society, enabling trust in government, faith in the fairness of one's society, and the right to protect and take care of one's family.

Where public values such as these are at stake, the non-economic costs of failing to require compliance with open standards, appropriately defined for this setting, can ultimately far exceed any savings obtained in public procurement. A failure to recognize this fact can lead to misguided efforts to seek economic justifications for policies that need no savings justification at all, or worse, the adoption of an openness policy that fails to serve the greater good at all.

Not every standard will invoke such non-economic concerns. But every year more and more will as our dependency on the Internet and all things electronic continues to increase. Governments need to keep this in mind when they set procurement and other appropriate, standards-related policies so that basic rights, as well as tax dollars, are properly protected.

Copyright 2013 Andrew Updegrove

Sign up for a [free subscription](http://www.consortiuminfo.org/subscribe/2.php?addentry=1) to **Standards Today** at

<http://www.consortiuminfo.org/subscribe/2.php?addentry=1>

FEATURE ARTICLE:

Measuring the Benefits of Open Standards: A Contribution to Dutch Politics

Tineke Egyedi and Bert Enserink*

Abstract: *In 2010 the Dutch Parliament requested the Court of Audit to measure the benefits of using open standards and open source software for government IT. In its report of 2011 the Dutch Court of Audit concluded that there were hardly any benefits to be gained. The Court's underlying research was widely and harshly criticized, especially with regard to open source software. In this article we focus on the open standards part of the Court's research, a subject which was barely addressed. We analyze the report's omissions and weaknesses. An inventory of existing international methodologies shows that these do not fully cover the required ground. As a stepping stone towards a more systematic way of measuring the benefits of open standards, we introduce an economic framework on standardization (functions and effects). To illustrate its use, we examine one effect of open standards more closely, i.e. reduced switching costs.*

We conclude that the Dutch Parliament's request regarding open standards could have received more serious consideration. Looking beyond the Court of Audit's report, in combination with elements from existing methodologies, the proposed framework appears to be a useful starting point for pursuing more systematically an international policy research agenda on measuring the benefits of open standards.

A pressing question is how to manage the rising costs of government IT projects. Several causes explain these costs, one of which is supplier-dependence (Dussel and Vos, 2012). The Dutch government addresses supplier dependence in its open standards (Updegrove, 2012)¹ and open source software² (OSOSS) policy. Among other things, its OSOSS policy focuses on improving interoperability in government IT, digital sustainability and unlimited re-use of software developed for government (EZ, 2007). It is one of the pillars of Dutch e-government policy.

In 2010 the Dutch Parliament passed the motion Gerkens³, which requested the Dutch Court of Audit (DCA) to investigate the potential savings achieved by reducing the use of closed standards (i.e., proprietary standards) and introducing open source software. The timing of the motion coincided with the final stage of the policy implementation program 'Netherlands Open in Connection' (NOiV) that was installed to support the use of OSOSS in government. Although OSOSS policy would remain in force after 2011, a need was felt to (again) highlight the benefits of OSOSS in order to ensure the policy's continuation in the years to

* Tineke M. Egyedi is Senior Researcher Standardization at Delft University of Technology. She also serves as Vice-president of the European Academy for Standardization (EURAS) and as the Director of the Delft Institute for Research on Standardization (DIRoS)

Dr.ir. Bert Enserink is Associate Professor of Policy Analysis and Programme Manager of the Engineering and Policy Analysis master at the faculty of Technology, Policy Analysis and Management of Delft University of Technology.

This paper was originally presented at 'Open iOverheid: verbindend verbroken?', held in Groningen, the Netherlands, on January 10 2013, and at the EURAS conference, held in Brussels, Belgium, on June 25 2013.

come. For despite broad political support for this policy (motion Vendrik c.s., 2002) and for successive government implementation programs (e.g., OSOSS and NOIV), the problem of supplier-dependence remained intractable. While some ministries, government agencies, local authorities etc. did embrace the idea of an open IT ecosystem, there were repeated signs of non-conformance to OSOSS policy. For example, in call for tenders for IT public procurement and document exchanges with citizens and businesses government authorities regularly required closed, vendor-specific solutions and formats, respectively (Paapst, 2012). Therefore, Members of Parliament had reasons to doubt whether future market failure resulting from supplier dependence could be avoided. If not, it would remain difficult to keep a grip on public IT spending, even apart from achieving other OSOSS goals such as sustained access to government data and unlimited re-use of government sponsored software development.

In March 2011, the Dutch Court of Audit presented its results. The [report](#) (in Dutch) concluded, in short, that cuts in public IT expenses could not be demonstrated as a result of using open standards and open source software.

There was much criticism about the quality of the report and the findings both from within the Parliament as well as from outside⁴ (e.g., Commission for Government Expenditure, 2011⁵; Sleurink, 2011a, 2011b). In particular, the report was criticized for the lack of a sound scientific approach and the narrow empirical basis for its main conclusions. Regarding this basis, the Court reported a crucial lack of data on government IT expenses. Amongst other reasons, it had therefore limited its investigation to only part of the public sector (e.g. not local governments and not the education sector) and in particular to the licensing and maintenance costs of software (and not the entire life cycle). See further on.

The Court's scientific approach shows a number of flaws⁶. It lacks a consistent methodology and methodological accountability; the literature study is unbalanced and very limited; far-reaching statements lack references; decisions about which data is admissible and which is not are arbitrarily made⁷; and research questions remain unanswered. Moreover, in determining possible savings no distinction is made between open standards and open source software. Regarding possible savings in software costs by central government, the report states that "because standards are implemented in software or organizational procedures, we will not separately address the costs of standards. These costs are part of the software costs." (DCA, 2011a, p. 41; *translation TE & BE*)

Our motive to write this article is the – unjustified, for unsubstantiated – influence the Court's report may have on IT decisions of governments internationally⁸, and the scientific-methodological challenge embedded in the motion Gerkens, namely to measure the benefits of open standards. This is not easy and several countries are currently struggling with this topic (CIPPM, 2012). It therefore deserves considered treatment.

In this article, we provide building blocks to contribute to such an effort. We explore what should be measured when it comes to the – here: market – effects of open standards, and which methodologies already exist. It is intended as a stepping stone for further research.

The article is structured as follows. First, we analyze the Court of Audit report and introduce our line of reasoning. Next, we present an economic framework which identifies the effects on open standards that could be measured. We then discuss three methodologies for measuring the benefits of open standards that emerge from an initial inventory of the literature. To illustrate the use of the framework, we elaborate on means to measure one of the listed effects: increased vendor independence. We conclude by reflecting on our findings in the light of the motion Gerkens and making recommendations for further research.

Criticism on the Court of Audit Report: Our article focuses, first, on open standards because they are hardly addressed in the Dutch Court of Audit report; and, second, on

exploring the benefits of open standards for the functioning of the market because this, we argue, is what the motion Gerkens is most interested in.

Open standards remain underexposed and are confused with open source:

Open standards are hardly mentioned in the report of the Court of Audit. Their costs and benefits are not measured separately, as the earlier quote indicates. Thus, the questionnaire sent to the ministries to map their savings exclusively addresses open source software; it contains no questions on open standards (see DCA, 2011a, Appendix 6). Moreover, the Court's report does not clearly distinguish the two. The authors seem to confuse the two. For example, without any further explanation standardization committees are called 'communities' in analogy with open source communities; and, as "often cited benefits of open standards" the report mentions that, compared to closed standards, open standards have a higher quality (because of their open process) and lead to more cost savings (because they contain no patents) - without mentioning any sources. These benefits are not typically quoted in listings of the benefits of open standards. They do typically appear, however, in lists on the benefits of open source software. In open source projects "given enough eyeballs, all bugs are shallow" (Raymond, 1999). The more people that work on the source code, the better the quality. The assumption that, because of the open process, this also applies to standardization may seem obvious, but ignores the dilemma that in open standards processes, where interests differ, ambiguous compromises are sometimes forged (Sherif et al, 2007).

The proposition that open standards lead to cost savings is widely endorsed, but not so much because of the absence of patents and user licenses (DCA, 2011a, pp.28-29) but rather because standards lead to a level playing field (David and Steinmueller, 1994). That is, the source of the frequently mentioned advantage lies elsewhere.⁹

The motion Gerkens is about the functioning of the market: In the motion Gerkens (19 May 2010) the Dutch Parliament notes that competition in the IT market should be improved and that more openness will yield substantial savings in public IT expenditure. Open standards contribute to a better functioning of the market. The motion Gerkens builds upon an earlier motion, the motion Vendrik (Vendrik c.s., November 20, 2002). Therein the Parliament requests the cabinet "to ensure that in 2006 all public sector software complies with open standards". The motion Vendrik specifies the problem to be addressed – and thus in which areas the (measured) benefits of a better functioning market may lie. It notes that the software market is highly concentrated (read: oligopolies); that "changing suppliers often entails high switching costs" (read: vendor lock-in); that "this restricts competition" (read: market failure); and that therefore "society is not taking full advantage of the possibilities software provides" (read: too high IT costs for consumers and too little innovation). By fully by-passing the impact of open standards on the IT market and limiting itself to the direct savings of open source software, we therefore conclude that the Court of Audit inappropriately narrows down the Parliaments request for research.

Economic framework: functions and effects of open standards: To more systematically address open standards and how they affect the IT market, we introduce a conceptual framework drawn from economic studies of standardization (Swann, 2000) and apply it to compatibility standards. In the IT sector compatibility standards, also known as interoperability or interface standards, are most prominent. This category of standards allows software from different vendors to inter-operate, data to be exchanged, and so on. In the following, we will focus on open compatibility standards unless stated otherwise. Compatibility standards have certain effects to which benefits are attributed. By 'effects' we mean: the impact of open compatibility standards for users (i.e., those who implement them such as software vendors), end users (e.g. government authorities) and others who experience their benefits and drawbacks. By 'benefits' we mean the value (monetary and otherwise) that society attaches to standards to realize these effects (see also ECORYS, 2007, p.41).

To gain insight into their economic effects, we apply a heuristic framework that classifies different functions of compatibility standards (see Table 1; revision of Swann, 2000). These functions, while not mutually exclusive, are: providing information, creating interoperability and reducing variety. We discuss them and their effect on the market below.

With regard to providing information, standards ease our lives because we can refer to them and thus reduce informational transaction costs (Kindleberger, 1983). They reduce the cost of negotiation because parties to a deal know what is being dealt in (Kindleberger, 1983, p. 395). They reduce the search costs of consumers because less time and money is needed to evaluate products (Jones and Hudson, 1996). This is particularly important in markets where consumers have difficulty recognizing the quality of products, as in the IT market, and where consumers are disadvantaged in the information they have relative to producers (information asymmetry; Akerlof, 1970). In such situations, market failure is more likely to occur - that is, too little functionality for too much money. Open standards reduce the risk of market failure. They make it easier for consumers to compare products (e.g., energy consumption of mobile chargers - once the plugs are the same) thereby increasing market transparency (Reddy, 1990). Standards thus reduce the chance that the supplier of an inferior product gets a larger market share via competitive pricing because the supplier of the higher quality product has no way to signal this to potential customers (adverse selection; Akerlof, 1970). Transparency is also of high importance in anonymous international markets, where trading partners do not know each other. Thus, open standards also facilitate international trade. See Table 1.

Functions of open standards	Effect on the market
Information	Increases market transparency Reduces transaction costs (e.g. reduces information asymmetry) Corrects adverse selection Facilitates trade
Interoperability, Compatibility	Creates network externalities Increases competition (i.e., increases number of producers, quality and choice of products, lowers prices, incentive for innovation) Decreases vendor lock-in (e.g. decreases costs of switching vendors and of maintenance)
Variety reduction	Allows economies of scale Facilitates building a critical mass

Table 1: Main features of open compatibility standards and their impact on the market (revision of Swann, 2000)

With regard to creating interoperability, the second main function of open compatibility standards, the latter constitute an 'infrastructure' (Swann, 2010) based on which competition and innovation may occur (David and Steinmueller, 1994). The intended economic effect is full competition between suppliers of a technology (Ghosh, 2005). This creates a playing field that reduces the threshold for new producers, increases the incentive to innovate, leads to better value for money and leads to a greater variety of products for consumers. Moreover, standards facilitate the emergence of new economic clusters. An example is the Internet services that were able to develop based on agreed network and transport protocols. Because the use of open standards is not restricted to certain parties, the effort required to enter standards-based markets is smaller, the number of providers is

likely to increase, and consumers are less likely to be tied to a single supplier (less 'lock-in'; Farrell and Saloner, 1985). Even if consumers switch supplier, they can continue to reap the benefits of adjacent and complementary products that often co-determine the consumer value of a product or service.

Reducing variety, the third function, is closely allied with the information and compatibility functions of open standards. The purpose of standardization is to curb unnecessary and unwanted variety by agreeing on a specification that can then serve as a common point of reference (Van den Beld, 1991). Overviews of the economic standardization literature (Swann, 2000, 2010; Blind, 2004) show that variety is sometimes equaled to innovation. However, variety does not have an intrinsic value. For consumers, this is well-illustrated by the different plugs for mobile chargers and the metric and imperial measurement systems. For producers, less variety allows larger production volumes, which leads to lower costs per unit produced (scale advantage). Standards can thus help to build the critical mass needed to open up new markets. And finally, less variety makes markets more transparent and efficient.

The motion Gerkena and its predecessor, the motion Vendrik, mainly cover the interoperability effects of open standards. In the following, we therefore focus in particular on ways of measuring these effects.

Measuring the benefits of open standards: The benefits of open standards can be diverse. We mention here some that gave rise to the development of 'The Netherlands in Open Connection: An action plan for the use of Open Standards and Open Source Software in the public and semi-public sector' (EZ, 2007, p. 28¹⁰); and which would therefore seem to be an obvious point to start research for the motion Gerkena:

- improved exchangeability of data;
- better accessibility to data (e.g., on websites);
- independence from suppliers encourages the market;
- reduced software production costs;
- greater independence from hardware systems and operating systems;
- reduced monopoly formation on the ICT supply side;
- potential positive effect on the trade balance and local knowledge economy.

Box 1: Dutch Court of Audit report on the benefits of open standards

The Dutch Court of Audit report quotes four frequently mentioned benefits of open standards, that is: next to 'increased quality' and 'saved patents costs' (see earlier comments), also vendor independence and digital sustainability (meaning that data will remain accessible even if suppliers decide to no longer support older software versions or go bankrupt). The report, however, adds at the same time - without revealing its source - that "there is no evidence of the general validity of the aforementioned benefits" (DCA, p.31). This leads to much incomprehension. In their reaction the Dutch Parliament asks "How does the Dutch Court of Audit assess the 'frequently mentioned benefits of open standards' given its remark that 'There is no evidence for the general validity of these potential benefits?'" (DCA, 2011b, question 30) The Court then replies that with this remark it had wanted to add a practical angle to the discussion on open standards. Also the minister of Interior Affairs challenges the Court's statement. He views open standards, in particular, but also open source software, as a means to "diminish the complexity [of IT systems], their intertwinedness and vendor dependence. (...) [There are] long-term advantages and economic-social benefits [to be gained] by better cooperation and more

efficient exchange of information within and between organizations" (letter by minister of Interior Affairs Donner, March 9, 2011, p.2).

Below we summarize relevant research and methodologies on the benefits of standards in the Netherlands and internationally identified by Yang (2012)¹¹.

CBA cases in the Court of Audit Report: The Court observes that attempts to measure the impact of open standards have not yielded much useful insights. This also applies to the three existing cost-benefit analyses (CBAs) of projects introducing open standards, which it includes as business cases in its report¹².

CBA is an instrument to assess the economic viability of projects. It provides a "systematic, rational basis for making a societal choice between relevant alternatives. Thereby all societal aspects should be taken into consideration, including non-financial ones such as safety or environmental impact. It also provides insight into the distribution of costs and benefits across relevant groups in society."(ECORYS, 2007, p.12).

The CBAs in the three business cases include financial estimates of efficiency advantages for end users and data suppliers, increased effectiveness of services, and costs avoided via synergies and reduced administrative burdens. However, according to the Court of Audit, these figures cannot be used to answer the parliamentary motion because the cases "do not [concern] completed projects that made the transition from 'closed' to 'open'" (DCA, 2011a, p.49). (We will address whether this dismissal is justified later on.) Furthermore, according to the Court, the project documents do not indicate whether it is important that these standards are open. The Court notes the lack of other quantitative data, and does not conduct any studies of its own. In sum, the Court of Audit report contains no appropriate data, according to the Court itself, to answer the question on standards in the motion Gerkens.

Baarsma report: A previous study that seeks to answer a question very similar to that of the Dutch Court of Audit, is that of Barbara Baarsma of the Foundation for Economic Research (Baarsma, 2004). Her research question is 'Are there societal benefits to be gained if the public sector as a whole would switch to software based on open standards and/or open source software?' The study is not discussed in the report of the Court of Audit. In the following we summarize its methodological approach and main conclusions.

The research methodology proposed in the Baarsma study was a cost-benefit analysis as detailed in the Dutch governmental guideline for evaluating infrastructure projects (Eijgenraam et al, 2000). Because there was too little data on the costs of government IT, Baarsma was unable to determine the Total Cost of Ownership of standardized IT, which was to be part of the CBA. Therefore she developed a more qualitative assessment framework to support those involved in deciding whether to switch towards open standards (see Baarsma, 2004, Table 4/3). A case study was conducted to further elaborate the assessment framework. The case, that is, information exchange between cooperating organizations in the public sector (meso-level measurement), focused on interoperability and included several types of effects: direct, indirect and external effects and transition costs.

The Baarsma report draws a number of highly relevant conclusions. It notes that most benefits lie in efficiency gains resulting from improved information exchange and functioning of the market. The issue is not merely using open standards but equally "the extent to which organizations use the same (open) standard" (Baarsma, 2004, p.49). At the societal level, significant welfare gains can be achieved but two difficulties arise. First, the (considerable) estimated benefits lie in the future, whereas most expenses have to be made

on the short term (Baarsma, 2004, p.49). Because of the delayed benefits, issues such as the evaluation of time and interest rates can be relevant to decision makers.

Second, costs and benefits are not equally distributed among the parties involved (p.49, p.82). In many cases, the cost of introducing open standards is initially borne by public authorities, whereas the main benefits may accrue to citizens and businesses (e.g., improved quality of service). These benefits may be indirect and unpriced.¹³ The Baarsma report further mentions two redistribution effects:

- Redistribution effects between suppliers and consumers. The profit from closed standards and closed source software often ends up with suppliers; when making the transition to OS and OSS, a portion of the profits will shift from suppliers to end users / consumers.
- International distribution of effects. Market power leads to higher prices and often to less product innovation. A switch to OS and OSS can stimulate the local economy and innovation.

ISO Methodology: More recently, the International Standardization Organization (ISO, 2010a, 2010b, 2011) developed a methodology to measure the benefits of open standards for companies. The ISO Methodology focuses in particular on standards that contribute to the core value of a company. Measuring occurs in retrospect and consists of four steps. First, the value chain (Porter, 1985) of a company is analyzed. Second, the effects of standards on main business activities are identified. To support this process, a list of 81 possible effects of standards has been drawn up. Third, the value drivers and key operational indicators are identified (e.g., saving time, decrease of the number of rejects and cost reduction). Finally, based on the selected indicators information is collected and effects are measured.

The ISO methodology has been applied in eleven case studies, most of which concern the introduction of compliance standards (i.e., environmental, health and safety management standards such as the ISO 9000 and 14000 series). Analysis of these cases shows that the main quantitative benefits are cost savings for businesses, that is, reduced information transaction costs (easy access to information) and economies of scale effects (fewer suppliers and less raw material). According to Yang (2012), application of the methodology to interoperability standards seems possible.

The sequence of steps in the ISO Methodology resembles that of a verification process, and is in this sense vulnerable to methodological criticism. For example, it does not indicate how to isolate the impact of standards from that of other factors, such as the ability of companies to implement standards and contextual factors such as regulation. However, the methodology's elaborate specification of possible effects of open standards may provide a valuable input for developing measurement methods in the field of government IT.

Intermediate Conclusion: Yang's initial inventory (2012) suggests that little quantitative research has been done internationally on the benefits of open standards¹⁴. While the discussed methodologies do contribute elements that are relevant for measuring the consequences of a move to open standards, no comprehensive, ready-made methodologies exist to quantify possible savings for government IT.

While the lack of quantitative government data was held to be a major stumbling block for the Dutch Court of Audit (2011a), one might question whether data on transitions from closed to open standards would have helped to answer the motion Gerkens. (This is challenged in the next section.) Moreover, the Court leaves unspecified which data it would have needed.

The economic framework introduced earlier points to several (market) effects relevant for measuring the benefits of open standards that are still missing. In the next section, we examine more closely what it would mean to measure one of the effects of interoperability, namely reduced switching costs and vendor dependence¹⁵. The motion Gerkens states that in the long run by using open standards the costs of switching IT supplier can be significantly reduced, which will increase competition in the IT market and lower prices.

Types of Switching Costs	Switch between proprietary products (closed standards)	Switch between open standard-based products
Search cost, i.e. the time, effort and expenses needed to find a product or supplier (if these are very high the switch may not be made)	High	Low/ Moderate
Transaction costs, i.e. the costs that must be made to reach an agreement, including forging a new trade relationship and writing off investments in earlier ones	High	Moderate
Learning costs, i.e. the costs (time, money, effort) consumers incur to familiarize themselves with the new product/supplier; these costs are non-transferable	High	Low
Complementary investments, i.e. expenses made to buy complementary products (e.g. DVD and DVD player)	High	Very Low
Costs related to network effects and compatibility; some products exhibit network effects that arise when a user desires compatibility with other users or where increased consumption of addition units of the same good creates additional value. Users then benefit from adopting products with most users.	High	Very Low
Contractual switching costs, i.e. financial incentives for customers to make repeat purchases from same vendors (e.g. frequent flyer program or penalty for early withdrawal of deposit banking)	High	High

Table 2: The implications of using closed and open standards for different types of switching costs.

Switching costs: In the economic literature the term switching costs is most often used for switching from one closed standard to another (von Weizsacker, 1982). Competing incompatible technologies are concerned (Shapiro and Varian, 1999) such as HD-DVD and Blu Ray. Whether a switch is made, depends on previous investments in time, effort and money and complementary products; the additional functionality provided; the speed at which new network externalities can be realized (i.e., the benefits attached to being connected to a network with other users); and so on. If the costs are too high, this is termed 'vendor lock-in'. Especially if there only seems to be room in the market for one of the two competing technologies (a 'winner takes all' situation) the height of the switching costs may lead consumers and producers of complementary products to postpone choosing a technology. In these cases switching costs inhibit the functioning of the market. In the

field of IT various switching costs can be discerned (Chen and Hitt, 2006). Table 2 column 1 lists a number of them.

Switching costs do not exclusively apply to closed standards (i.e., switching from one closed to another closed standard). Each switch to another supplier involves costs. But their height may vary strongly. Thus, the switching costs between suppliers of products that comply with the same open standard are usually much lower. Table 2 roughly indicates the switching costs for closed and open standards. For example, when switching to another closed standard (incompatible technology) one will have to write off investments in complementary products and transaction and learning costs, whereas this is typically not the case when switching to a supplier who sells products that comply with the same open standard. Because they ease such a switch, open standards help to avoid lock-in (Farrell and Saloner, 1985). By doing so they increase consumer choice and stimulate the market.

Back to the motion Gerken. In its report, the Court of Audit interprets the Parliament's request as concerning the costs of switching from closed to open standards (DCA, 2011a, p.49). The report focuses on the (short term) costs of such a transition. However, these data, had they been available, would hardly have thrown light on the (mid-and long-term) market effects of open standards. To clarify our point, we outline three transition scenarios:

1. From a closed to an open standard
2. From a closed to another closed standard
3. From an open standard-based product to another based on the same standard

The line of reasoning in the Court of Audit report is based on scenario 1. Broadly speaking, in this scenario the short term costs are high and the short term benefits low. On the short term, the cost of scenario 1 hardly differs from that of scenario 2 (for example, switching from Video2000 to VHS). But in the long run the benefits of these two scenarios do differ. The expected long-term benefits in scenario 1 are high. In scenario 3, however, the switching costs already make a difference on the short term. For, the switching costs are low and the market benefits are felt immediately (lower prices, vendor independence). See Table 3. Perhaps needless to say, the switch from closed to open standards in scenario 1 is a precondition for switching vendors more easily in the future (i.e., under the regime of scenario 3).

Scenarios for switching to new supplier	Costs	Short-term benefits	Long-term benefits
1. from closed to open standard*	High	Low	High
2. from closed to other closed standard	High	Low	Low
3. from open to same open standard	Low	High	High

*Table 3: Scenarios for the cost of switching to a new supplier. (*The switch focused on by the Dutch Court of Audit)*

According to our interpretation of the motion Gerken, the Parliament is foremost interested in the difference between the switching costs in scenario 2 and 3, whereas the Court's report focuses on scenario 1. The difference between scenarios 2 and 3 reflects the societal costs of vendor-dependent government IT and measures the effect of open standards on the market.

This conclusion is in line with earlier criticism that in its calculations of government IT expenditure the Court's report does not take long term consequences into account such as (a) exit costs, i.e., the costs made when switching suppliers, which should be depreciated (an issue embedded in questions posed by the Dutch Parliament, see DCA, 2011b), and (b) the indirect consequences of working with closed systems, that is, producing data which later may have to be converted and migrated to open formats. As Sleurink (2011b) puts it in his letter, "when it comes to a cost estimate one should not only study the life cycle of the software in question, but also that of everything produced with the software."

Discussion: The report of the Dutch Court of Audit confuses open standards and open source software. It hardly addresses open standards and fully omits addressing their effect on the market. It does not answer the question posed by the motion Gerken's about the savings that can be achieved by reducing the use of closed standards. The report does, however, draw conclusions about this issue¹⁶. These conclusions re-surface in the English summary and are referred to in international policy discussions, in which the Dutch Court of Audit is – in this instance undeservedly – regarded as an authoritative source. We therefore recommend the full report to be translated in English so that those who refer to the summary can acquaint themselves with its content and limited scope.

Internationally, no appropriate methodologies exist that quantify in a systematic way the benefits of open standards for government IT. With this article, we offer a possible stepping stone for a developing such a methodology. Summarizing our steps:

- We introduced a (revised) economic framework that identifies functions of open IT standards and their possible effect on the market. For the motion Gerken's, particularly the interoperability function and its effects were argued to be relevant.
- We analyzed the results of a preliminary inventory of methodologies internationally. The existing methodologies focus foremost on making a business case for introducing standards. While they do not solve the problem of determining the benefits of dismantling closed systems, elements therein (i.e., variables and indicators) offer useful input for further research.
- We illustrated what it might entail to measure the benefits of open standards. We focused on various switching costs in three transition scenarios, and showed which data would have been required to respond to the motion Gerken's, i.e.: *not* data about the costs of switching from a closed to an open standard, which the Court of Audit sought, but the *difference* between (a) the cost of switching from closed to closed standards (scenario 2) and (b) the cost of switching between open standard-compliant suppliers (scenario 3).
- With the rising cost of government IT, the Dutch Parliament has good reasons to seek quantitative data on savings by reducing the use of closed standards. The required research poses a methodological challenge to which we have tried to make a modest contribution. However, we fully realize that we have not even touched on the problem of quantifying other possible benefits of open IT standards, such as increased ease of IT use, increased security, long-term digital preservation, and greener IT.

To conclude, what if the Dutch Court of Audit had done a better job and their scientists had managed to provide the required information to the Dutch Parliament? There would have been the danger that politicians would have mistakenly expected, first, that the costs and (financial) benefits accrue to the same government authority; and, second, that OSOSS activities can be initiated and benefits reaped in the same (political) time frame (see also Baarsma, 2004). This is a recurrent dilemma in policy research: if scientists do sound research, will politicians be able to draw the right conclusions and political consequences?

References:

- Akerlof, G.A. The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics*, 84(3), 1970, pp. 488–500.
- Baarsma, B. *Kosten en baten van open standaarden en open source software in de Nederlandse publieke sector- ene analyse op meso- en macroniveau*. Stichting Economisch Onderzoek, SEO-rapport 755. Amsterdam: Universiteit van Amsterdam, September 2004.
- Beld, J.W. van den Technische normen niet altijd commercieel gewenst. *Elektrotechniek-Elektronica*, 2, 1991, pp.22-24.
- Blind, K. *The economics of standards: theory, evidence, policy*. Cheltenham, UK: Edward Elgar, 2004.
- Chen, P.Y. and L.M. Hitt, Information technology and switching costs. *Handbooks in information systems* 1, 2006, pp.437-470.
- CIPPM *Open standards in government IT: A review of the evidence*. Bournemouth University, Centre for Intellectual Property Policy & Management, <http://www.cippm.org.uk/publications.html> – final draft 10 September 2012, consulted 20 September 2012.
- David, P.A. and W.E. Steinmueller, Economics of compatibility standards and competition in telecommunication networks. *Information Economics and Policy* 6(3), 1994, pp.217-241.
- DCA, Dutch Court of Audit (Algemene Rekenkamer), [Open standaarden en opensourcesoftware bij de rijksoverheid](#). Tweede Kamer, vergaderjaar 2010-2011, 32679, nr. 2. 's-Gravenhage: Sdu, 15 maart 2011, 2011a.
- DCA, Dutch Court of Audit (Algemene Rekenkamer), *Beantwoording vragen Tweede Kamer bij rapport Open standaarden en opensourcesoftware bij de rijksoverheid*. Brief aan de voorzitter van de Tweede Kamer, Den Haag, 15 juni 2011, 2011b.
- DTI, *The Empirical Economics of Standards*. UK, London: Department of Trade and Industry, 2005.
- Dussel, H. and B. Vos, *Leveranciers Lock-in*. PIANOo congres 2012, <http://www.pianoo.nl/sites/default/files/documents/documents/vendorlockinenopenstandaardenbijictaanbestedingen.pdf>, consulted 3 October 2012.
- Ecorys *Handreiking voor kosten-batenanalyse voor ICT projecten*. Actieprogramma maatschappelijke sectoren & ICT, opdrachtgever ministerie van Economische Zaken, Rotterdam, December 2007.
- Eijgenraam, C.J.J., C.C. Koopmans, P.J.G. Tang and A.C.P. Verster, *Evaluation of Infrastructural projects: Guide for Cost-Benefit Analysis, Sections I and II*. The Hague, CPB Netherlands Bureau for Economic Policy Analysis, 2000.
- EZ, *Nederland Open in Verbinding: Een actieplan voor het gebruik van Open Standaarden en Open Source Software bij de (semi-)publieke sector*. 's-Gravenhage: Ministerie van Economische Zaken, 2007.
- Farrell, J. and P. Klemperer, Coordination and lock-in: Competition with switching costs and network effects. *Handbook of industrial organization* 3, 2007, pp.1967-2072.
- Farrell, J. and G. Saloner, Standardization, compatibility, and innovation. *RAND Journal of Economics*, 1985, pp. 70-83.
- Forum Standaardisatie, <http://forumstandaardisatie.nl/open-standaarden/>, consulted 20 September 2012.
- Gerkens c.s., see Tweede Kamer (House of Parliament) 2010.
- Ghosh, R. *Free/Libre/OpenSource Software: Policy Support; An Economic Basis for Open Standards*. Maastricht: MERIT, University of Maastricht, FLOSSPOLs project, 2005
- ISO, *Economic Benefits of Standards- Methodology Guide*, Version 1, Geneva,Switzerland: ISO, 2010a.
- ISO, *Economic benefits of consensus-based standards: the ISO Methodology*. Geneva,Switzerland: ISO, 2010b.
- ISO, *Economic benefits of standards - International case studies*. Geneva,Switzerland: ISO, 2011.

- Jones, P. and J. Hudson, Standardization and the Cost of Assessing Quality. *European Journal of Political Economy* 12, 1996, pp.355-361.
- Kindleberger, C.P. Standards as Public, Collective and Private Goods. *Kyklos* 36, 1983, pp.377-396.
- Krechmer, K. (2006). Open Standards Requirements. *The International Journal of IT Standards and Standardization Research*, 4(1), January - June 2006.
- NOiV, *De derde voortgangsrapportage Nederland Open in Verbinding*, <http://www.rijksoverheid.nl/onderwerpen/digitale-overheid/documenten-en-publicaties/rapporten/2011/12/13/de-derde-voortgangsrapportage-nederland-open-in-verbinding.html> of 30-12-2011, consulted 5 October 2012
- Paapst, M.H. *Barrières en doorwerking, een onderzoek naar de invloed van het open source en open standaarden beleid op de Nederlandse aanbestedingspraktijk*. Dissertation, Groningen: Rijksuniversiteit Groningen, 2012.
- Porter, M.E. *Competitive Advantage, Creating, and Sustaining Superior Performance*. New York: The Free Press, 1985.
- Raymond, E.S. *The Cathedral and the Bazaar*, Sebastopol, CA: O'Reilly, 1999.
- Reddy, N.M. Product of Self-Regulation. A Paradox of Technology Policy. *Technological Forecasting and Social Change* 38, 1990, pp.43-63.
- Shapiro, C. and H.L. Varian, *Information rules: a strategic guide to the network economy*. Boston, Harvard Business School Press, 1999.
- Sherif, M.H., K. Jakobs and T.M. Egyedi, Standards of quality and quality of standards for Telecommunications and Information Technologies. In: M. Hörlesberger, M. El-nawawi, T. Khalil (eds.). *Challenges in the Management of New Technologies*. Singapore: World Scientific Publishing Company, 2007, pp. 427-447.
- Sleurink, H. *Open brief aan de het College Algemene Rekenkamer*. 23 March 2011a, [English translation:] http://www.opentrends.nl/wp-content/uploads/2011/03/PublicLetter1_Sleurink.pdf, consulted 28 April 2013.
- Sleurink, H. *Open brief aan de het College Algemene Rekenkamer*. 2 September 2011b, [English translation] http://www.opentrends.nl/wp-content/uploads/2011/09/PublicLetter2_Sleurink.pdf, consulted 28 April 2013.
- Stedehouder, J. *Reactie op rapport OS/OSS Algemene Rekenkamer*. 22 March 2011, <http://www.slideshare.net/janstedehouder/reactie-op-rapport-ososs-algemene-rekenkamer>, consulted 1 October 2012
- Swann GMP (2000). *The Economics of Standardization*. London: Department of Trade and Industry, Standards and Technical Regulations Directorate.
- Swann, G.M.P. *International standards and trade: a review of the empirical literature*. OECD Trade Policy Working Papers, no. 97, OECD Publishing, 2010.
- Tweede Kamer (House of Parliament), *Motie van het lid Vendrik c.s..* Vergaderjaar 2002-2003, 28600 XIII, nr. 30. 's-Gravenhage: Sdu, 2002, <https://zoek.officielebekendmakingen.nl/kst-28600-XIII-30.html> .
- Tweede Kamer (House of Parliament), *Motie van het lid Gerken c.s..* Vergaderjaar 2009-2010, 26643, nr. 156. 's-Gravenhage: Sdu, 2010, <https://zoek.officielebekendmakingen.nl/kst-26643-156.html> .
- Updegrove, A., 'Openness and Legitimacy in Standards Development', *Consortiuminfo.org*, feature article, <http://www.consortiuminfo.org/bulletins/nov12.php#feature>
- Vendrik c.s. see Tweede Kamer (House of Parliament) 2002.
- Weizsacker, C.C. von *Staatliche Regulierung - positive und normative Theorie*. Schweizerische Zeitschrift für Volkswirtschaft und Statistik, 2, 1982, pp. 325-243.
- Yang, X. *Methodologies for assessing the benefits of open standards; The implications for the public IT procurement*. Thesis for master of science in Engineering and Policy Analysis. Delft: Delft University of Technology, July 2012.

Endnotes:

¹ The term 'open' is used to indicate that different stakeholders (can) participate in the standardization process, that the documented standards are readily available, and that

there are no obstacles to use them (see also Standardisation Forum, 2012). For a more detailed discussion on open standards see Krechmer (2006) and Updegrove (2012).

²That is, one can read the source code (and look, as it were, under the hood of the car) and change and reuse the source code depending on the accompanying license.

³The motion Gerkens (formally: Gerkens cum suis) was proposed by the members of Parliament Gerkens (socialist party), Heijnen (liberal party) and Vendrik (green party).

⁴ See Stedehouder (2011) for a compilation of reactions to the report.

⁵This is referred to in DCA (2011b).

⁶As part of an internal evaluation the Dutch Court of Audit invited one of the authors, Tineke Egyedi, to comment on the report. This conversation took place February 20, 2012 in the presence of four representatives. Some of her comments are provided here.

⁷In answer to a parliamentary question the Court responds that, although an earlier report (Baarsma, 2004) concludes that "probably net societal benefits can be achieved if the public sector as a whole switches (...) to open standards", this conclusion "is quantified nowhere" and therefore the Court does not take it into account (question 51, DCA, 2011b). The Court does not apply the same degree of criticism to its own research.

⁸ The report is referred to as an authoritative source, for example, during a meeting on European ICT public procurement (Brussels, 12 December 2011), http://cordis.europa.eu/fp7/ict/ssai/action23workshop-nov2011_en.html, accessed 5 December 2011. It is also referred to in the study of Bournemouth University (CCIPM, 2012).

⁹ As far as we know, no studies exist that specifically address the costs saved by patent-free standards. This may deserve further investigation.

¹⁰<https://www.ictu.nl/archief/noiv.nl/service/english/index.html>

¹¹Xiuyun Yang's research was done as part of his master thesis (TU Delft, EPA). For the inventory of methodologies, he searched the Internet using different (combinations of) terms and interviewed a number of experts (face-to-face, via email and phone). See Yang (2012). We warmly thank him for consenting to using some of his work.

Given the focus of this article, we do not discuss macro-economic research on the impact of open standards on economic growth (DTI, 2005) and international trade (Swann, 2010).

¹²These are: INSPIRE, 'Welstand Transparant' and 'Stelsel van basisregistraties'.

¹³The Baarsma report concludes that in particular indirect (often unpriced) benefits will be decisive when choosing between closed and open software (Baarsma, 2004, p.80), such as fewer disadvantages of network effects and the emergence of new markets.

¹⁴ To our knowledge, there are still no TCO studies on the use of open standards (see also Baarsma, 2004, p.23).

¹⁵ The Court has not examined the "cost effects associated with vendor-dependence" (the Court's answer to Parliamentary letter, question 11, DCA, 2011b).

¹⁶ The Court of Audit concludes, for example, that competition law and regulation are more appropriate means to address the functioning of the market than standards are (DCA, 2011a, p.52) - without having examined this.

CASE WATCH:

Judge Robart's Opinion in Motorola vs. Microsoft and the Future of FRAND

Andrew Updegrove



Perhaps the most important term in any standards organization's Intellectual Property Policy (IPR) policy is the acronym "RAND," standing for "reasonable and non-discriminatory" (in Europe, they add an "F" – for "fair" – at the front end, yielding "FRAND," but the meaning is the same). Virtually every other term in such a policy will appear in one of many variations from policy to policy, and these definitions can be quite lengthy and precise. But the definition of F/RAND is always word for word the same – never is a different term used. And only rarely is there any elaboration to explain exactly what "fair" or "reasonable" are intended to mean.

The result is that when two parties – the owner of a patent claim that an implementer of a standard can't avoid infringing (an "Essential Claim") and a party that wants to implement the standard – can't agree on what the permissible range of terms bounded by these words should be, a third party is needed to settle the dispute.

Until recently, surprisingly few such disagreements found their way into the courts, meaning that there were not many judicial opinions to turn to for guidance on exactly what FRAND might mean. Because licensing terms are usually kept confidential, this also means that there are few public reference points for licensors and licensees to refer to when they are having trouble reaching agreement.

With the advent of the mobile platform wars, this state of affairs has changed, leading to uncertainties in the marketplace and attracting the attention of regulators on both sides of the Atlantic. They are urging standards organizations to become involved in facilitating resolution of such disputes (e.g., by including voluntary or mandatory arbitration clauses in IPR policies), so that the court system is not clogged with these typically complex, lengthy and difficult contests.

In late April, the task of defining FRAND became incrementally easier, with the handing down by Justice James Robart of a 207 page opinion in a closely-watched dispute between Motorola and Microsoft, involving several patents that Google later acquired (along with the rights under the law suit) when it purchased Motorola Mobility. In that opinion, Robart sought to determine what, under all relevant circumstances, Google could fairly and reasonably charge Microsoft to infringe upon the Essential Claims in question when (for example) it builds and sells an Xbox.

The question at the heart of the case was how individual Essential Claims should be valued. For example, should a patent claim become be worth more when it achieves monopoly status by inclusion in a standard, or the same, or perhaps even less, since the volume of licenses the owner of the claim would enter into would presumably rise dramatically? And what if a single device (such as a mobile phone) includes dozens, or even hundreds of Essential Claims? Should the value of each Essential Claim be devalued, lest the aggregate licensing fees exceed the maximum that the market could bear?

A number of clear summaries of Judge Robart's complete opinion can be found on the Web (a good example, by Jorge Contreras, can be found [here](#)). For current purposes, however,

suffice it to say that a busy judge and his clerks spent an inordinate amount of time poring over the extensively briefed and argued record placed before them by the highly paid legal teams of two very large companies and sought to divine the true economic boundaries of FRAND.

The result is a closely reasoned opinion that is based in part on pre-existing rulings, but in several significant aspects breaks new ground. It is these new aspects that offer the greatest value, because they provide one clearly explained methodology that can be used as a reference by future parties seeking to reach agreement on FRAND terms, and by judges when the parties cannot.

The fact that the opinion provides such a methodology, however, begs the questions of whether the novel aspects of Judge Robart's opinion will in fact be followed, and also whether they even should be.

The question at the heart of the case was how individual Essential Claims should be valued.

Regarding the first query, there are hundreds of independent legal jurisdictions in the U.S. and abroad, none of which are obligated to follow the rulings in the Motorola case (although they may be influenced by it if they so choose).

Instead, Judge Robart's opinion, assuming that it is not reversed in relevant aspects on any appeal that may follow, will only be binding in those courts in the same jurisdiction that are presented with similar situations. And that's a very small slice of the global litigation pie.

Regarding the second question, it remains to be seen whether the concepts that Judge Robart developed will be adopted by future finders of law (e.g., whether the societal benefits of standards should be reflected in permissible royalty rates, and if so, whether the somewhat arbitrary multiplier that Robart chose is appropriate).

Similarly, other judges may disagree that the comparables that Robart used for determining the market value of Essential Claims should in fact be used at all, or at least not in all circumstances.

For example, Judge Robart concluded that the prices charged in standards-related patent pools should be relevant to the pricing of licenses in Essential Claims in one-on-one negotiations as well. A patent pool is most often formed when there are many holders of Essential Claims. When this situation arises, there can be two resulting negative impacts that can potentially prevent a new standard from becoming widely adopted. The first concern is that the simple act of negotiating license terms with scores of different parties may add up to more effort than seems to be worthwhile. The second is that the combined price to be paid may make the standard too expensive to implement at all.

With a patent pool, the owners of the Essential Claims in question agree on several things. First, they agree on how much they think the market will bear for the pool of Essential Claims. Next, they agree on a mechanism (usually involving a third party) to determine whether each patent claim they assert is essential really is, and if it is, what percentage of the combined license fee that patent claim should be entitled to receive. (You can read more about how a patent pool works in the standards context [here](#)).

Inherent in Judge Robart's turning to patent pools for comparable pricing is a concern with so-called "patent stacking," or the potential for a given standard to be priced out of the market if one or more owners of Essential Claims are unreasonable in its demands.

But in fact, such situations are likely to occur in only a very small number of circumstances involving either very complex technology (e.g., Wi-Fi) and/or market niches where gaining

the right to charge royalties is very much part of the reason why companies join standards organizations. And, in fact, standards-related patent pools are only very rarely formed, due to the time and expense (not to mention extensive wrangling among patent owners) required to form them. In other words, the marketplace has only very rarely found that royalty stacking was a serious enough concern to warrant the formation of a patent pool at all.

While not completely unknown, patent pools are particularly rare in the case of software standards. As a result, using a patent pool as a reference in such a case arguably should not be of much relevance at all. Judge Robart would presumably agree with that conclusion. But other judges might not make that distinction, and in any event, once patent pools are removed as a reference, a hole opens up in the Robart analysis that would need to be filled through some other means.

In the software (and many other) domains, the marketplace may therefore be only incrementally better off after the issuance of Judge Robart's opinion than it was before. As a result, courts and judges will still be taxed with adjudicating extremely complex situations, and litigants will still face highly speculative outcomes.

How speculative? In the case of Motorola/Google, Motorola initially requested a royalty rate that Microsoft claimed would require it to pay as much as \$4 billion a year for the use of the Essential Claims (a number that seemed absurd to me, as well as to many others). By the time litigation ensued, the demand had been lowered to \$400 million – an order of magnitude reduction. The final number determined by Judge Robart to be consistent with a FRAND commitment was a mere \$1.8 million per year.

Whether you pick \$4 billion/\$1.8 million or \$400 million/\$1.8 million as the range of legitimate dispute, that's still an enormous disparity of expectation. Normally, businesses hate uncertainty, and are often willing to pay more in order to protect themselves from expensive litigation or the prospect of becoming subject to a wildcard judgment.

So why don't companies simply agree on a definition for FRAND when they form a standards setting organization (SSO), the way they do with so many other complex elements of a typical IPR policy?

For the last twenty-five years, I have tried to interest my consortium clients in addressing this issue head on, and have only rarely been successful in persuading them to even incrementally add to the definition of what FRAND should mean. Here are two examples that clients of mine have included, and which might profitably be considered by other organizations as well:

Reasonable: License terms relating to an Essential Claim included in a Standard that are not more onerous (including as to price) than could be obtained by the owner of such Essential Claim in the open market absent its inclusion in a Standard. It is acknowledged that Reasonableness cannot be established with precision.

Non-Discriminatory: Available to all Implementers under terms that are substantially identical to the terms made available to others under similar circumstances.

To be fair, these definitions would not resolve all sources of disagreement. But they would substantially narrow the range, and could considerably decrease the likelihood of a dispute arising at all.

Despite the fact that U.S. regulators have asked SSOs to consider providing more guidance on what they mean by "FRAND," I am unaware of any SSOs that are taking up this challenge. This seems quite unusual, given that quite a few SSOs and committees in other organizations (e.g., the American Bar Association) are now discussing other suggestions made by the same regulators, such how an arbitration clause in an IPR policy could best be drafted, and then implemented in the marketplace. And it also seems strange that companies are content to allow courts to come up with, almost inevitably, a variety of different rule sets which may take many years to coalesce into a definition that industry could then use as a consistent guide.

It would seem that there would be obvious value in reaching voluntary – as compared to court-imposed – consensus on a definition, or alternative available definitions, of FRAND that any given SSO could include in its IPR policy. These definitions could also include, or reference, specific valuation methods taken from a list developed for that purpose (Judge Robart's methodology providing an appropriate first entry on such a list). Where an SSO decides to follow this path, its members could debate which formulation of FRAND and mechanism they wish to use, just as they already spar with great energy over which variations on other significant terms to employ. In this way, they would get the results that they agree upon, rather than one that some future judge ultimately deems in retrospect to be most appropriate.

The result should be a win-win for all concerned. Licensors and licensees could come to terms faster, and with far less likelihood of ending up in court. Moreover, they would also avoid replacing one long, expensive process (legal action) with another process than be almost as long and expensive, at least in its first act (arbitration). The burden of courts would also be significantly reduced.

Perhaps most significantly of all, SSO members could get back to the important work of developing the hundreds (and even thousands) of new standards that are needed each year in order to allow new products and services to reach the market, to permit the benefits of technology to reach farther and faster into the Third World, and for more and better jobs to be created.

That seems like a very fair and reasonable goal to pursue.

Bookmark [the Standards Blog](http://www.consortiuminfo.org/standardsblog/) at <http://www.consortiuminfo.org/standardsblog/> or set up an RSS feed at: <http://www.consortiuminfo.org/rss/>

Copyright 2013 Andrew Updegrave

Sign up for a free [subscription](http://www.consortiuminfo.org/subscribe/2.php?addentry=1) to **Standards Today** at

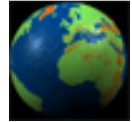
<http://www.consortiuminfo.org/subscribe/2.php?addentry=1>

The Problem with Patents: Operating with Blunt Instruments

Andrew Updegrave



On June 4, the Obama administration announced a new effort to curb the baseless patent that it believes are stifling innovation and economic activity. The new initiative would take five actions under the President's Executive authority, and also makes seven legislative As anyone who watches technology even casually will be aware, the assertion of patents has played a dominating role in the mobile sector press of late. It's not often that a new platform takes over, and as a result, both the stakes as well as the opportunity to unseat incumbents are high. recommendations intended, "to protect innovators from frivolous litigation and ensure the highest-quality patents in our system."



In such a situation, the dominant players have an incentive to pull out all the stops, and indeed they have. The resulting suits have been particularly troublesome where infringement is unavoidable, as is the case with so-called "standards essential patents."

But the high level head bashing between technology leviathans like Apple, Samsung, Google and Microsoft has partially obscured a more troubling and ongoing crisis in the technology sector, which is the misuse of patents by companies referred to as "Patent Assertion Entities" (PAEs), "non-practicing entities" (NPEs), or simply as "trolls."

PAEs are entities that own (or control) and assert patents, but do not themselves offer products or services that implement them. PAEs come in several flavors, including universities that develop technology (often with public funding), entities formed solely for the purpose of owning, licensing, and asserting patents, and shell companies, sometimes formed by actual vendors to indirectly assert patents against their competitors without the plaintiffs knowing who is really behind the attack.

The entities that have incurred the greatest public wrath are those whose business it is to threaten implementers – and even simply users – with litigation unless they pay up. Often, the patents such PAEs assert may be weak or improperly issued, or may not in fact be infringed at all by the target of their attention. But patent litigation is extremely expensive, so many of those contacted (and particularly small companies) simply pay up rather than fight.

Ironically, the uptick in market activity that is now raising the patent issue to the forefront of the President's busy agenda was partly the result of an action taken by Congress to lessen the woes of those attracting the attention of trolls. Previously, a PAE could sue multiple defendants in a single law suit. But as a result of the America Invents Act recently enacted by Congress, trolls must now sue each defendant individually. The result? A dramatic rise in patent assertion suits clogging up federal courts.

President Obama has been harsh in his criticism of PAEs, describing them in February of this year as entities that, "don't actually produce anything themselves...[but instead] essentially leverage and hijack somebody else's idea and see if they can extort some money out of them." He went on to say that the patent reforms achieved in the America Invents Act,

which he signed into law in 2011, did not go far enough: “our efforts at patent reform only went about halfway to where we need to go.”

What the President did yesterday was to try to bridge that gap. You can find his announcement [here](#), and the Fact Sheet containing those actions and recommendations is here. A [related report](#) by the President’s Council of Economic Advisors, the National Economic Council, and the Office of Science and Technology can be found here.

The Report acknowledges that not all innovators (such as universities or skunk works) wish to productize or police their patents, and that intermediaries may therefore have a place in an effective innovation economy. But the Report also recognizes that an increasing number of PAEs embark upon “overly aggressive” litigation and threats of suit against “thousands of companies” based on patents “without specific evidence of infringement” (especially in the case of software). It also gives specific examples of documented negative impacts:

A range of studies have documented the cost of PAE activity to innovation and economic growth. For example:

- One study found that during the years they were being sued for patent infringement by a PAE, health information technology companies ceased all innovation in that technology, causing sales to fall by one-third compared to the same firm’s sales of similar products not subject to the PAE-owned patent.
- Another study found that the financial reward received by winning PAEs amounted to less than 10% of the share value lost by defendant firms, suggesting that the suits result in considerable lost value to society from forgone technology transfer and commercialization of patented technology.

The goal, the Report asserts, should be to employ the types of actions that have historically been taken to curb abuses while preserving innovation, concluding that:

...fostering clearer patents with a high standard of novelty and non-obviousness; reducing disparity in the costs of litigation for patent owners and technology users; and increasing the adaptability of the innovation system to challenges posed by new technologies and new business models; would likely have a similar effect today.

It’s hard to fault the President for once again taking action to plug the gaps left by inadequate Congressional action. But, as the phrase goes, the President’s plan “Says easy, does hard.” The reason? Because patents, by their nature, are blunt instruments that are too easily granted and too often wielded like cudgels.

Consider just the following by way of example:

- A patent gives monopoly rights for over 20 years, and the same invention can underlie an increasing cascade of products and services, even though the level of overlying innovation may soon dwarf the invention in question.
- A pharmaceutical product can be based on a single patent, but a mobile device can implement thousands.
- A successful drug can cost hundreds of millions of dollars to develop and test, and can follow on the heels of multiple failed, but equally costly efforts, while a

software patent can be based on an idea an engineer has in the shower one morning.

- Some inventions are based upon years of complex work and vast investments leading to unique results, while others can be simple and independently conceived by multiple inventors in the same narrow time frame.
- Different courts vary widely in their willingness to enforce patents, leading to domestic and international “forum shopping” to gain the most desired result.
- Patent litigation is highly expensive and interpretive, allowing both plaintiffs and defendants to honestly believe that they are in the right.
- Practicing as well as non-practicing entities use the same legal tools to assert their rights.

It is hardly surprising then that many people feel that even legally valid patents actually adjudicated in courts can cause real problems, especially in areas such as software. But even leaving that concern aside, how does one differentiate “overly aggressive” litigation from permissible assertion of legal rights, or PAEs that serve a useful purpose by conservatively assisting universities from “trolls” asserting shaky patents obtained by the same source non-infringing end-users?

Taken as a whole, the actions and recommendations have the potential to dramatically improve the situation. Unfortunately, many of the actions would require Congressional action, meaning that with a few exceptions the initiatives to be pursued under Executive Authority can make only incremental progress (e.g., by providing educational materials to help “main street” businesses defend themselves if they are sued by trolls). More meaningfully, the administration will be stepping up training of patent examiners, which will hopefully result from fewer inappropriate patents being granted to begin with.

Almost all of the forceful actions, sadly, would require Congressional action. Those recommended practices include allowing courts to force losing patent plaintiffs to pay the legal costs of successful defendants, requiring PAEs to disclose the entities that may ultimately control them, and changing the rules for gaining an injunction in the International Trade Commission.

It’s hard to imagine that such action will follow any time soon. Meantime, perhaps the brightest hope may, as often is the case, arise at the state level. Recently, Vermont enacted a law allowing defendants to recover not only costs from trolls, but damages as well. Such a law can provide a significant disincentive for any owner or licensor of a patent to assert it unfairly. If such laws proliferate, perhaps we’ll see a decline in blunt force assertion of invalidly issued and irrelevant patents against innocent vendors and users sooner than later.

Of course, passing similar laws in 50 states would be a slow and tedious process. But state action is better than no action, so hopefully more states will follow Vermont’s lead. Until they do, as usual, only the trolls (and lawyers) will benefit from the status quo.

Copyright 2013 Andrew Updegrove

Sign up for a free [subscription](#) to **Standards Today** at

<http://www.consortiuminfo.org/subscribe/2.php?addentry=1>

CONSIDER THIS:

#68 The Devil's in the Cloud: It's Time to Stop our Headlong Rush into Cyber Insecurity

Andrew Updegrove



There appears to be consensus in many quarters that migrating to the Cloud is highly desirable – indeed, that mass migration is already inevitable now that the technology as well as the bandwidth finally exists to make remote hosting viable.

And why not? Multinational IT vendors view this transition as the next great market opportunity; governments see in it a chance at long last to rationalize their Byzantine legacy systems without incurring massive up front capital costs; and enterprise users find the value proposition increasingly compelling as their locally-based systems become more complex, expensive and difficult to maintain.

Meanwhile, an ever increasing torrent of data, records, photos and social relations of everyday individuals leap with the tap of a key from hard drives and back up devices under the control of their owners to servers located who knows where, owned by who knows who, and vulnerable to who knows what?

As this process continues, all-too predictable market forces will drive cloud services towards commoditization, and with commoditization will come consolidation – again, in response to classic market dynamics.

As the share of global electric power consumed by data farms and networks approaches an incredible 10%, concerns over climate change and rising energy prices continues to drive the data farms that receive all this data to cluster around the lowest-cost energy sources – wind farms, hydroelectric dams and, someday, perhaps solar and geothermal sources as well. Already there are millions of servers humming in data farms adjacent (for example) to the Columbia River in Washington state that dwarf the agricultural farms that they have replaced.

Ten years from now, what percentage of all that matters will be hosted by an increasingly smaller number of ever more enormous data complexes? Not just the transactional wherewithal to enable transportation, finance, government, food production, power transmission, manufacturing and education to function, but – far more consequentially – what percentage of all data: technical, financial, civic, cultural, commercial, indeed, all human knowledge? No longer will any of this data be archived in non-electronic form (i.e., on paper). It will, of course, be backed up electronically – to other data farms.

Let us add one final trend: as the First World becomes more networked and Cloud dependent, its asymmetric vulnerability to less network-reliant enemies will increase exponentially. After all, when the United States has a military budget equal to that of the next 17 most militarily committed nations combined, what incentive can there be for a lesser country that wishes to tweak the lion's tail to spend a Rial or a Won on traditional weaponry?

This last trend has been well-recognized as a reason to take electronic cyber security seriously. But this realization masks a far more serious vulnerability entirely, because

systems that are the victim of a cyberattack can usually be restored again – often within hours. But the data hosted at a facility that has been transformed into a smoking ruin by kinetic weapons of war or a terrorist attack will never be brought back on line again if its back up site is in ashes as well.

As we will explore below, in a cloud-based world, it will be remarkably simple for any nation – indeed for the entire First World – to be reduced to a state of societal collapse by an enemy whose identity may never be learned, much less determined while the nation is still capable of retaliating.

The moral of the story is that equal attention will need to be paid to developing and mandating adherence to standards ensuring physical as well as electronic security for our increasingly Internet-dependent modern society. To do otherwise will be to render ourselves vulnerable to a degree of societal destruction that would rival that produced by a nuclear war, and which will soon be within the technical capabilities of dozens of nations throughout the world.

Ten years from now, what percentage of all that matters will be hosted by an increasingly smaller number of ever more enormous data complexes?

Does that sound improbable and alarmist? Let me suggest that you consider the following scenario before drawing a conclusion.

New Year's Day, 2023



As the sun set on New Year's Eve, 2022, a dozen anonymous container ships are decreasing speed a few miles outside major American and European ports. Like many carriers nearing the end of their useful lives, their histories are mongrel in nature; some had been commissioned by shipping magnates in Greece, while others had been ordered from points around the world. Each had passed through multiple hands and now sailed under Panamanian registry or one of the other common flags of convenience; and each had been chartered three years ago by one of an equal number of shell companies formed in third world countries scattered around the globe.

The terms of each contract made the charter party responsible for the upkeep of the ship it had leased, and therefore in due course each ship had undergone repairs in small ship yards in the Indian Ocean and in Southeast Asia before returning to ply its trade in the various shipping lanes of the world.

Over the two years that followed, the ships loaded and unloaded tens of thousands of anonymous containers. As one might expect, they contained almost anything a container could hold – phonebooks from printers in Calcutta destined for telecommunications carriers in France; timber transshipped at the mouth of the Amazon consigned to furniture companies in South Carolina; consumer electronics from Taiwan bound for Southampton; plywood shipped from Kyoto to Seattle made from trees that had been cut in Oregon and shipped from Portland to Kyoto only a few months before. All of the infinitely varied stuff of global commerce that passes from point A to point B before being transferred to trucks and trains for forwarding to points C and D.

Frequently, the ships traded cargoes in ports in Africa, India, Indonesia, Bangladesh and other parts of the Indian Ocean and South Pacific.

There was therefore nothing to remark upon as the members of the aging fleet neared their current destinations: some were closing on Seattle, Los Angeles, New Orleans, Newport News and Boston. One had steamed up the St. Laurence Seaway, through the lakes and locks and onto the broad waters of Lake Michigan. Others were nearing ports in the English Channel, the Baltic, and the Mediterranean. The papers of each ship were in order, and a pilot was already scheduled to guide each to the dock that had been reserved to accept its cargo.

To the practiced eyes of the pilots, each ship would be different, although all were of approximately the same tonnage and design. But any pilot would swiftly note two aspects of each ship that would stand out. The first was that its hull had been modified to install large doors in its stern, ostensibly to allow roll on/roll off handling of cargo. That would be curious, because each ship had also been configured to carry containers, which would most often be loaded from above.

The only indication that something unusual was afoot was the low hum of the propeller-driven drones – hundreds of drones

They might also wonder what port each ship visited that was configured to load from the bow, rather than from the side. But with 70,000 commercial vessels plying the seas, they would have seen almost everything before.

The second aspect was that each ship was riding unusually high, showing more bottom paint and Plimsol lines than one would assume for a ship carrying a profitable cargo of tightly packed containers.

In the dark of the night, though, none of these peculiarities would be visible. Nor was anyone near enough to notice as the doors in the sterns of the ships swung open, because all lights had been extinguished inside. The only indication that something unusual was afoot was the low hum of the propeller-driven drones – hundreds of drones with muffled engines – emerging in rapid succession from each ship before pursuing its unerring course towards its target. They flew only a few hundred feet above the water, and then over the land.

Some of those targets were only a few score miles away, while others were many times more distant. It hardly mattered, though, because the United States and Europe had been secure within their borders for many decades. In the modern world, only the United States, with its ten carrier fleets, could project real military muscle against distant enemies. Why, then, would any First World nation need the types of coastal anti-aircraft defenses they had constructed before the advent of the nuclear age? These fortifications had long ago been abandoned and fallen into ruin.

Needless to say, confusion reigned as the first drones began striking their targets. The small night time staffs working at the targets had no way of knowing what was hitting them – Truck bombs crashing through the chain link fences that surrounded the installations? Missiles? And from where?

Only after the destruction was complete did the realization spread that the nations were under a coordinated attack. Their governments and militaries struggled to understand what had happened, and to react. But the drones had all been destroyed, leaving few clues. And still under cover of darkness, the ships that had launched the attacks had sunk quietly beneath the waves as their crews raced out to sea in speedboats, there to be taken aboard by other ships that had left the same ports the night before. These vessels were equally anonymous, except for the hoists that allowed them to swing up the speedboats without

deviating from their courses or decreasing their speed, and then to lower them in a matter of minutes through the open hatches that rapidly closed once more.

The countries that had been struck launched no counterattacks, because there was no way to know who to attack without weeks of investigative work. Even after the identity of some of the scuttled ships was established, it was laborious to work through the tangle of seemingly endless layers of holding companies controlling them. And the drones could have been loaded in any of the hundreds of ports the ships had visited over the preceding years.

The civil and military leaders of the target countries never did completely understand what had hit them. To do so would require sophisticated networks to gather and analyze data of all kinds.

And that was now impossible. Because, of course, the targets the drones had destroyed were the data farms.

The New Dark Ages



When the New Year's Day sun rose in Europe and the United States, the reality of what had happened was hidden to almost all. Only a hundred or so targets had been struck, and the smoke from the devastated facilities was already dissipating. What people did realize immediately was that a great many things that they were used to working now did not.

What no longer functioned included anything that relied on electricity or the Internet. Which was, of course, virtually everything except automobiles and hand tools. This was necessarily the case, because all of the elements that coordinated and controlled the power grid had been destroyed. Even many battery powered devices were silent – the cell phones had no dial tones, and the radios generated only static, because the management software and servers that enabled telecommunications had also been annihilated. Perhaps most discomfiting of all, there was no Internet, nor any of the services that relied upon the Internet.

For the first few hours, the effect was unusually peaceful, the way a power outage can sometimes be. Neighbors in the Deep South of the U.S. remarked upon how nice it was to simply sit on the porch and talk, just like the old days.

But by mid-day, the novelty was replaced with consternation, because there was virtually no information available about what had happened, and how it would be made right. True, some emergency broadcast radio channels were operating, but because the authorities that controlled them had so little knowledge about what had happened, or the extent of the damage, there was little they could say. Worse, if they had shared what information they did have – that those ostensibly in control had no idea how they would go about restoring the power grid, let alone the Internet, in any reasonable amount of time – mass panic would certainly ensue.

There was little to prevent the arrival of that state of affairs in any event. For those that were fortunate, it was a matter of days. For others, it arrived before the night of the first day had fallen. Riots and looting broke out in many cities, fueled in part by fear and in part by opportunism.

By the second day, the true severity of the situation began to penetrate the consciousness of more and more people. The gas in the tanks of their cars was the last gas they would have until who knew when, because gas stations had no generators. Even if they had, there

would be no more deliveries of new fuel to the stations, because there was no more Internet to support inventory and shipping controls to monitor supply or demand, or to restart the refineries, all of which had immediately shut down and could no longer be controlled.

Needless to say, the banks did not open. Nor did ATMs operate, although in truth the relevance of paper money was rapidly becoming less and less obvious. The capital markets stayed closed as well, as did almost every element of the transportation system, dependent as they were on computerized management, and as workers became less and less willing to use precious gasoline driving to work.

As the fuel ran out in cars and trucks, the delivery of even locally available essential items – food, heating oil, medicines, clothing, replacement parts – speedily came to an end.

As had always been the case in the past when a natural or man-made disaster had struck, police, firemen, EMTs and other first responders sprang into action. But this time, everything was different. For one thing, they lacked reliable communications. For another, they lacked information.

What no longer functioned included anything that relied on electricity or the Internet. Which was, of course, virtually everything

Databases that used to live on local servers had long ago been moved to the distant data farms. Information as basic as the addresses and phone numbers of a police department's own personnel was suddenly unavailable. Desk sergeants were reduced to rummaging through desk drawers, hoping that someone had printed out a copy of one piece of information or another for temporary reference.

The same crisis developed quickly in almost every other setting. Hospitals relied on power from backup generators, but only for a few days until their fuel supplies gave out. Their patients no long had a medical history to consult, because paper records had all been replaced with electronic medical records. All of those records – of course – were remotely hosted, or at least had been, prior to the attack. Now they had ceased to exist. Nor could doctors order medical tests, because the servers that hosted the diagnostic software also no longer existed. Only the oldest doctors had ever been trained to diagnose through personal observation. The younger ones found that suddenly they were scarcely more competent to treat their patients than were the patients themselves.

So also at airports, where suddenly air traffic controllers and pilots were reduced to line of sight, visual navigation; pilots with rapidly emptying fuel tanks circled nervously over airports waiting for clearance to land. Once down, they did not take off again, because every airline shut down its operations; they had no way to know who had paid for a ticket who had not, or whether planes would be full or empty, or whether there would be sufficient fuel at any given airport to refuel a plane once it had arrived.

Buses, of course, needed fuel. And soon they had none. Railways were only a little better off, because their signaling systems no longer functioned. That hardly mattered, though, because the local lines and spurs that long ago carried rail freight from main lines to factories and small towns had long ago been abandoned. There was little point to moving items from one transshipment point to another, since there were no longer any trucks to complete the delivery to its final destination.

First responders did the best they could at the local level for as long as they could. But as time went on, what they could do became less and less. They had no food to dole out, nor any way to bring heat to the emergency shelters that had always served their appointed purposes in the past. As the reality of the situation began to sink in, police, firemen and

ambulance staff did what could be expected – without fuel to commute, they returned to their families, to do what they could to protect them instead.

Meanwhile, supplies of medications at pharmacies and hospitals rapidly dwindled. When stocks of insulin and other urgently needed medications gave out, the results were both predictable and tragic.

The shock of realizing that vital information had been lost – perhaps forever - played out over and over in millions of businesses, universities and government agencies in the days that followed. The impact was numbing and immobilizing. Theoretically, over many months millions of new servers could be ordered, built, bought, shipped and installed, and those servers could theoretically be reloaded with software and that software could be reconfigured, over another very long time. But how could those servers be manufactured, much less ordered, paid for, shipped and installed without access to the data, software and computing power that had been destroyed? Over time, perhaps, yes, but how to accomplish anything at all until that had occurred? Or survive until it had?

So it was with the power grid as well. The days were long gone when every town had its own generation facility. Instead, the grid had become like an ocean of power into which producers poured electricity and from which users pumped it out, matching up accounts between buyers and sellers through highly complex software. Maintaining that grid had become an almost infinitely complex balancing act. Take down one part, and the impact could cascade through a wider and wider area. Bringing it back up was a vastly intricate job, predicated on the assumption that virtually all generating capacity would be available to once more be linked together.

True, wind turbines continued to turn and the dynamos deep inside hydroelectric dams still spun. But renewable energy constituted only a very minor part of total energy needs, and little of that could now be distributed. The coal-powered facilities that remained continued to produce, but only for a few days, until their on-site coal supplies ran out, because the transportation system was down. Gas-fired plants had already shut down when the pipeline system crashed, due to loss of the systems that controlled distribution. Naturally, all of the nuclear facilities were shut down immediately, out of fear that they could be the next targets of attack.

Every way that those in charge sought to turn, there were missing pieces – missing pieces in everything and everywhere. It was as if in an instant all of the modern infrastructure of two continents had been turned into confetti and blown to the four corners of the earth. Here there was still a bit and over there another, but too much of what should have been in between was unavailable to allow anyone to start to repair anything at all. And really, there was no place to start, because your communications were down, as your analytical tools were no longer available.

In the best of times, perhaps it could all have been put back together again. But these times were anything but fortuitous. To rebuild would require vast amounts of coordination and communication. But chaos increasingly prevailed in the streets as food and fuel ran out. Soon, only the armored vehicles of SWAT teams and the National Guard could safely move about, when they had the fuel to do so. Those charged with maintaining order and with restoring normalcy became first, demoralized, and then desperate. Finally, they became powerless, and mass desertion set in. Who could blame them?

It was both cruel and deliberate that the attack had been unleashed in midwinter. Those who relied on natural gas for heat were immediately at risk of freezing to death, while those relying on oil were able to keep the cold at bay only until their tanks ran dry – assuming they could run without electricity. Those that had full tanks stayed warm while they

starved; it did not take long to consume their last canned goods. That is, if they had not been stolen by their neighbors first.

Except for isolated pockets of elected leaders sheltering at military bases that could do little but preserve their own safety, all federal, state and local governments had utterly collapsed. Soon, well-armed, but hardly well-ordered, militias began to spring up. In most cases, they brought more fear than safety to the territories they staked out. Incredible as it would have seemed only a few months before, much of the first world was under the control of what could only be called war lords.

It seemed incredible that the often imagined cinematic scenario of a dystopian, post-apocalyptic nightmare world had been made real so easily, and in such faithful detail. Not by means of thousands of nuclear weapons delivered by intercontinental ballistic missiles, but by squadrons of simple, but well-targeted drones bearing conventional weapons, launched from a tiny fleet of out of date cargo ships.

In the face of such enormous need, the rest of the world did what it could, which was not very much. A few nations sent relief efforts to coastal cities, but many of those efforts were met in the United States by armed mobs intent on getting as much as possible for their starving families. Soon, these efforts ceased. And indeed, with more than 800 million people in Europe and the United States in the worst need imaginable, and with no means to distribute what they so urgently required once it had arrived, what could a poor or a small nation do to make a dent, in any event?

And then, of course, there was the danger that whoever had attacked the West could also attack anyone that came to its aid.

By the time that spring had arrived, most of the population of northern Europe and the Northern United States had starved to death, been killed, or (in some cases) killed themselves. Many of those that lived farther south were not much better off. There were few seeds to plant where they were needed and there was no fuel for the tractors. They could hope to hold out until what few crops they could plant and hoe by hand had matured.

The Ghost of (Cyber) Future



It would be convenient and consoling to pretend that what I've just described is simple science fiction. But sad to say, the only thing that is doubtful about the scenario I have described is that it might be difficult for a perpetrator to build a thousand drones without Western espionage becoming aware of the plan.

But would that really be so hard? Many countries are building drones now; the technology is not complex. Indeed, Germany successfully launched V-1 drones against Britain more than seventy years ago, and they were jet powered. With the availability of GPS-guided navigation today, building and guiding sufficiently reliable drones of the primitive type needed to stage the type of surprise attack I have described is not only within the technical ability of every nation that could be imagined to be a suitably disposed enemy today, many more besides. And there are plenty of old ships to go around.

The moral of the story is that we are rapidly and willingly creating a vulnerability of astonishing severity, largely sacrificing the difference between our \$650 billion annual military budget and that of a third world nation.

And I use the word 'rapidly' advisedly. There is already an Office of Management and Budget (OMB) program in place called the Federal Data Center Consolidation Initiative

(FDCCI), under which the Federal agencies are closing 1,200 out of about 2,900 data centers. But this may only be a first step. The Department of Homeland Security has already consolidated its information much more drastically. Where once its enormous data resources were spread across 46 data centers, everything now is hosted by *just five*. As noted in a recent FCW.com article, "although having fewer data centers gives would-be attackers a smaller zone to target, the threat is offset by a smaller perimeter that has more controlled resources within it."

That may be fine if you are only worried about terrorist attacks by a few individuals. But it also dramatically increases the damage that a successful attack could do if some or all of those centers are breached. And it's abundantly clear that unless those five centers are buried deep underground, the type of scenario I've described could already have devastating effect today.

So why are we doing this?

In part, it is because it is easier and cheaper to place servers in lightweight industrial buildings. But the more honest explanation is that we live under the illusion that because we have not had a major war on Western soil since the 1940s that it cannot ever happen again. Which is, regrettably, patently absurd. Indeed, war has been intermittent in the Middle East for decades, periodically threatening to spill beyond those borders. Only two decades ago, a murderous and savage war was waged in the Balkans. How much more likely would an attack become if a drone-filled ship could replace an army, navy and air force all rolled into one, and without incurring a single casualty on the attacker's part?

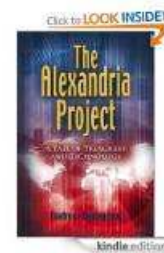
One need not look to the indefinite future to find a reason for concern. On what evidence should we assume that North Korea or Iran would never try such a gambit, and especially if it were possible that we would be unable to trace the attack to its source in time to retaliate? Even if we assume that currently known adversaries are not to be of concern, what about ten or twenty years from now, as the global population expands, and as water and other natural resources become ever scarcer?

If the picture I have painted is dreadful to comprehend, it should be. If we continue on our current course of centralizing Cloud services without housing them in appropriately protected environments, we cannot assume that a scenario such as the one described will certainly occur to one or more nations in the foreseeable future. With 5,000 years

of war-torn history to look to for precedent, we would be reckless to assume otherwise. Happily, and unlike the challenges presented by cyber attacks, addressing the threat described is not even difficult. Only expensive, although not prohibitively so. The most obvious solution is simply to mandate that critical ((broadly, and not narrowly defined) Cloud services and related infrastructure, as well as critical data be hosted underground. Indeed, the medieval solution (fortification) remains beautifully suited to the current, modern risk. There is nothing technically challenging about digging a hole in the ground, filling it with a data farm, and covering it up again with 30 feet of dirt and reinforced

Have YOU Discovered the Alexandria Project?

A Tale of Treachery and Technology



**Available Now for \$2.99 or
less**

at [Amazon](#), [iTunes](#) and [Barnes & Noble](#) (and in ePub and PDF formats at [GooglePlay](#))

concrete. It's only a matter of committing to incur the extra cost (if you're wondering what such a structure would be like, I've described one [here](#)).

While it's true that the U.S. today has a "bunker busting" bomb capable of reaching deeply buried resources, the U.S. is the only nation that has a stealth bomber capable of carrying such a 30,000 pound behemoth. It is difficult to imagine how any nation could successfully mount a concerted attack against U.S. data centers using ordinance of this nature for the foreseeable future. And unlike the drone scenario, existing defenses exist to detect and defeat such an attack, as well as to immediately determine its point of origin.

What is needed is for a thoughtful set of requirements to be set out that identifies data and critical infrastructure, and then specifies what level of protection against kinetic attack will be required to defend it. Happily, the identification of such infrastructure is already in process in the U.S. under an initiative launched by the Obama administration. Less happily, many areas of commerce are scrambling to avoid falling within the definition of "critical infrastructure" in order to avoid the costs of complying with regulations relating just to thwarting cyber attacks.

As stark as the scenario described may be, it's hardly surprising that we should find ourselves at such a pass. Realizing the promise of the Cloud has been just over the horizon for twenty years, and now, suddenly, it has come within our grasp. Moreover, technical opportunity has always beguiled us; increasingly, our society wants to enjoy the candy first, and worry about the cavities later. Stated another way, profit motives will always bring innovation to the marketplace faster than prudent rules will be devised to protect us from any undesired but nonetheless real dangers that might come along for the ride. Even when real danger becomes too obvious to ignore, lobbyists weigh in to fight new restrictions and costs, and legislators temporize and delay. Sadly, the longer we delay requiring physical protection of data farms, the greater the resistance will be, because of the investment already made in unprotected infrastructure.

What we need to ask ourselves, like Scrooge in the Dickens tale, is which future do we want to live in? History tells us clearly that we have not seen the last of war. Europe especially should resonate to the possibility of a kinetic attack.

But those in the United States should pay even greater heed, because after centuries of living safely behind our oceanic moat, we now live in an age where a handful of aging ships can truly bomb us back into the Stone Age. The time to protect ourselves from such a risk is now.

Copyright 2013 Andrew Updegrove

Read more **Consider This**... entries at: <http://www.consortiuminfo.org/blog/>

Sign up for a [free subscription](#) to **Standards Today** at

<http://www.consortiuminfo.org/subscribe/2.php?addentry=1>
