THIS MACHINE KILLS SECRETS

How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information

ANDY GREENBERG

DUTTON

CONTENTS

THIS MACHINE KILLS SECRETS

CHARACTERS

(IN ORDER OF APPEARANCE)

JULIAN ASSANGE
Founder of WikiLeaks, former hacker, cypherpunk, and activist who demonstrated the power of digital, anonymous leaking by publishing record-breaking collections of secret corporate and government material.

DANIEL ELLSBERG
Military analyst who from 1969 to 1971 exfiltrated and leaked the top secret Pentagon Papers to *The New York Times* and seventeen other newspapers.

BRADLEY MANNING
Army private who, at the age of twenty-two, allegedly leaked a trove of secret military and State Department documents to WikiLeaks that would become the largest-ever public disclosure of classified materials.

ADRIAN LAMO
A former hacker and homeless wanderer to whom Manning confessed his leak. Lamo turned Manning in to army investigators.

TIM MAY
Intel physicist, libertarian, and crypto-anarchist thinker who would cofound the cypherpunks in 1991 and create a thought-experiment prototype for cryptographically anonymous leaks called BlackNet.

PHIL ZIMMERMANN
Applied cryptographer whose Pretty Good Privacy program (PGP) brought free, strong encryption to the masses. His investigation by the U.S. Justice Department from 1993 to 1996 ignited a debate over users' right to uncrackable encryption.

DAVID CHAUM
Inventor and academic whose anonymity systems, including DC-Nets and Mix Networks, would inspire the cypherpunks and lead to tools like anonymous remailers and Tor.

ERIC HUGHES
Mathematician, cryptographer, and cofounder of the cypherpunks who ran one of the Internet's first anonymous remailers.

JOHN GILMORE
Former Sun Microsystems programmer who would cofound the cypherpunks as well as the Electronic Frontier Foundation.

JOHN YOUNG
Architect, activist, and cypherpunk who founded Cryptome.org in 1996, a leak-focused site that has published thousands of names of intelligence agents and their sources, along with hundreds of secret encryption- and security-related documents.

JULF HELSINGIUS
Finnish systems administrator and privacy advocate, Helsingius created the Penet anonymous remailer and faced legal pressure from the

Church of Scientology that demanded he turn over the identity of one of his users.

JIM BELL
Engineer and libertarian whose 1997 essay "Assassination Politics" described a system of using encryption to facilitate anonymous, untraceable, and crowd-funded contract killings.

JACOB APPELBAUM
Activist, hacker, and developer for the Tor anonymity network who befriended Julian Assange and became the WikiLeaks' primary American associate.

PAUL SYVERSON
Logician and cryptographer in the Naval Research Laboratory who is credited with inventing the anonymous communications protocol known as "onion routing."

NICK MATHEWSON AND ROGER DINGLEDINE
Two MIT researchers who worked with Syverson to develop onion routing into a usable tool and then a nonprofit known as the Tor Project.

PEITER "MUDGE" ZATKO
Former "gray hat hacker" who served as a spokesperson for the hacker group the L0pht. Now leads the cybersecurity division of the Pentagon's Defense Advanced Research Projects Agency, including its program to find a method of rooting out rogue insiders known as CINDER or Cyber Insider Threat.

AARON BARR
Former chief executive of HBGary Federal, a small D.C. security firm that touted his methods for unmasking anonymous hackers and leakers.

THOMAS DRAKE
National Security Agency whistleblower who was threatened with prosecution under the Espionage Act for communicating with a reporter regarding alleged financial fraud and waste at the agency.

BIRGITTA JÓNSDÓTTIR
Icelandic member of parliament, poet, and activist who worked with WikiLeaks and is pushing a collection of radical transparency bills through Iceland's legislature known as the Icelandic Modern Media Initiative.

DANIEL DOMSCHEIT-BERG
German former WikiLeaks associate who worked closely with Assange but was pushed out of the group in the fall of 2010. He has since engaged in a bitter feud with Assange and founded his own digital whistleblower group known as OpenLeaks.

ATANAS TCHOBANOV AND ASSEN YORDANOV
Two Bulgarian investigative reporters who founded the independent media outlet Bivol and were inspired by WikiLeaks to create the Bulgaria-focused leak site BalkanLeaks.

ANDY MÜLLER-MAGUHN
Former member of the board of the German hacker group the Chaos Computer Club. Müller-Maguhn worked with WikiLeaks and served as an intermediary in the dispute between Assange and Domscheit-Berg.

THE ARCHITECT
Secretive and pseudonymous engineer who worked with Assange and Domscheit-Berg to set up a revamped submission system for WikiLeaks in late 2009 and 2010. After a falling-out with Assange, he joined Domscheit-Berg at OpenLeaks.

PROLOGUE

THE MEGALEAK

On a rainy November day in a garden flat in London, Julian Assange is giving me a lecture on the economics of leaking.

"To put it simply, in order for there to be a market, there has to be information. A perfect market requires perfect information," he says, settling his six-foot-two-inch body, clothed in a sleek navy suit, into the couch, a coffee mug in hand. His voice is a hoarse, Aussie-tinged baritone. As a teenage hacker in Melbourne its pitch helped him impersonate IT staff to trick companies' employees into revealing their passwords over the phone, and today it's deeper still after a recent bout of flu. His once-shaggy white hair, recently dyed brown, has been cropped to a sandy leopard print of blond and tan. (He's said he colors it when he's "being tracked.")

"There's the famous lemon example in the used car market. It's hard for buyers to tell lemons from good cars, and sellers can't get a good price, even when they have a good car," he says in a professorial tone. "We identify the lemons."

Assange, today, has a particular lemon in mind. He's just told me that WikiLeaks plans to release tens of thousands of internal e-mails from a major American bank in early 2011, just a few months away from our meeting. He won't say which bank, or exactly what the e-mails will reveal, but

he promises they will expose corporate malfeasance on a massive scale, enough to "take down a bank or two."

"You could call it the ecosystem of corruption," he says. "But it's also all the regular decision making that turns a blind eye to and supports unethical practices: the oversight that's not done, the priorities of executives, how they think they're fulfilling their own self-interest."

This is Assange at the height of his power. When I report his words later that month in *Forbes* magazine, speculation that WikiLeaks' target would be Bank of America shaves off $3.5 billion from the company's stock market value in a matter of hours. The thirty-nine-year-old WikiLeaks founder had gotten accustomed to the feeling of his thumb on the eject button for the world's institutional information. In the last four months, his group had already spilled 76,000 secret documents from the Afghan War and another 391,000 from the war in Iraq, entire shadow histories of the two wars, the largest public classified data breaches of all time. "These big package releases. There should be a cute name for them," he says with a stern look.

"Megaleaks?" I offer tentatively.

"Megaleaks. That's good," he says. "These megaleaks . . . they're an important phenomenon, and they're only going to increase."

A few hours later, after I've turned my recorder off, Assange has donned his gray parka and he and his assistant are packing up to leave. That's when he lets slip that WikiLeaks is planning another megaleak in the near future, speaking about it as if it were an embarrassing technicality he mentions only out of necessity.

A big one? I ask, sweating a little. He responds that it's seven times the size of the Iraq War document dump.

"Does it affect the private sector or a government?" I try to subdue the panicked feeling that after three hours of talking to a man who dispenses secrets to reporters like Christmas gifts, I'm somehow only now getting the real story.

"Both," he says.

"Which industries?" I ask, thinking of my editors' interests at the business magazine I work for.

That's when Assange's professional dispassion seems to crack, and he allows an unrestrained, full schoolboy grin to spread across his face, complete with his usually hidden overbite. "All of them," he says.

A minute later, he's out the door and disappeared down the rain-shined sidewalks of London.

-- --- -- ---. -. -.-- .--. .--. .. ... --- .. ..-- .--. -.

Cablegate changed the world. Three weeks after my meeting with Assange, 251,000 once-secret State Department Cables began flowing out of WikiLeaks and would continue for the next year. The documents had too many connections to too many world affairs to draw straight lines between cause and effect. But when a sidewalk vendor named Mohamed Bouazizi set himself on fire in front of the governor's office in the Tunisian town of Sidi Bouzid, the country's citizens responded by taking to the streets to overthrow their government. Many of them cited WikiLeaks' revelations about the U.S. State Department's disdain for Tunisian president Ben Ali as giving them the courage to oppose their dictator of the prior two-and-a-half decades. If they stood up to him, it was now clear, America wasn't coming to his aid.

As populist anger spread to Egypt, Libya, Syria, and elsewhere, Muammar Qaddafi warned Libyans in a televised speech not to read "WikiLeaks, which publishes information written by lying ambassadors in order to create chaos." Nine months later, that revolutionary chaos had overwhelmed his military, ousted him from power, and killed him.

When President Obama announced that all American troops would be leaving Iraq by the end of 2011, CNN reported that WikiLeaks had cratered negotiations that might have kept them there longer. U.S. generals had asked for guarantees of legal protection for any remaining soldiers in the country. But thanks to leaked cables that revealed a massacre of Iraqi civilians and a subsequent cover-up, the Iraqi government had refused, and sent the American forces on their way.

But even as Assange's ultrascoop percolated around the globe, the bank leak he had foretold to me failed to appear. For the next year, the Australian

carefully dodged all questions about the nonleak, offering veiled excuses and eventually seeming to pin the blame on a rogue staffer who WikiLeaks would claim deleted the files. Assange's brash vows to "take down a bank or two" only contributed to the banks' vicious retaliation against WikiLeaks: Bank of America joined an informal coalition of payment firms including Visa, MasterCard, PayPal, Western Union, and others who refused to process donations to the world's most controversial website, choking it to the point of paralysis.

Today, WikiLeaks is on life support. Assange faces questioning for alleged sex crimes in Sweden, with more American legal foes waiting in the wings. Revelations by the prosecutors of WikiLeaks' alleged source Bradley Manning suggest Assange may have actively coached the young army private, potential grounds for his own indictment. His organization's work has stalled as it struggles to raise cash. Some of its most ardent supporters have become its most bitter critics, and its releases have dropped sharply in frequency and impact. Assange seems more interested in hosting a TV talk show on the Russian government–funded network RT than in rebuilding his organization, and WikiLeaks-watchers from Evgeny Morozov to Richard Stallman argue that the group's fate holds dark lessons. With WikiLeaks, they say, the Web turned out to be less the free, anarchic realm we once imagined than a restrictive platform tightly controlled by corporations and governments.

But it would be a mistake to focus only on how WikiLeaks has been contained, muzzled, punished, and sabotaged while ignoring a larger lesson: how the group has inspired an entire generation of political hackers and digital whistleblowers. That story didn't begin or end with Julian Assange, or even with his institution-eviscerating group. Instead, it tracks the ideals, the means, and the movement that WikiLeaks represents, extending from its predecessors decades earlier to the ideological descendants it has radically mobilized.

Since my meeting with Assange that rainy day in London, that thread has taken me from one edge of the Western world to the other as I sought out the history and future of an idea: digital, untraceable, anonymous leaking. And the line of thought I followed remains stronger in many ways than

ever before. The activists and fellow travelers I've met have no illusions about WikiLeaks' and Assange's weaknesses and failures. But they share the same spirit that drove Assange: to build a better secret-spilling machine than the last one.

This Machine Kills Secrets is a book about the forces that coalesced to make WikiLeaks happen. And it's also about how those forces are working to make it happen again.

The insider's drive to expose institutional secrets—to conscientiously blow the whistle or vindictively dump a superior's dirty laundry—has always existed. But the technology that enables the spillers of secrets has been accelerating its evolution since the invention of computing. With the dawn of the Internet, the apparatus of disclosure entered a Cambrian explosion, replicating its effective features, excising its failed components, and honing its methods faster than ever before.

The state of the world's information favors the leaker now more than ever. In 2002, the amount of digitally recorded data in the world finally matched the amount of analog recorded information, according to a study by the University of Southern California's Annenberg School for Communication and Journalism. Just five years later in 2007, the most recent year the study included, digital information already accounted for 94 percent of the world's recorded information. And all of that information is *liquid*: infinitely reproducible, frictionlessly mobile—fundamentally leakable.

Just what fraction of that vast digital swamp remains secret is tough to gauge. But Harvard science historian Peter Galison, taking printed files as a proxy, estimates that there are five times as many pages being added to the world's classified libraries as to its unclassified ones. Despite Barack Obama's promises of a more transparent government, 76.7 million documents were classified in 2010, compared with 8.6 million in 2001 and 23.4 million in 2008, the first and last years of George W. Bush's administration.

The numbers of people who have access to that material are just as unfathomable. Four million Americans have some form of clearance to read classified information. Of those, about 1.2 million have top secret clearance.

But the abundance of widely shared secrets is hardly the only factor pushing the leaking movement forward. Anonymous whistleblowing remains a game of skirting surveillance, and WikiLeaks' key advancement in the science of spilling information has been in separating the leaker from the leaked information. Cutting the data trail to a leak's source was the crucial trick that emboldened ever-greater disclosures from whistleblowers leading up to the Cablegate blowout.

That's why the story of leaked secrets, from the days of Daniel Ellsberg and the Pentagon Papers to the growing brood of sites hoping to reproduce WikiLeaks' work, has not been driven merely by digital disclosure, but by digital anonymity. And true digital anonymity requires cryptography.

The craft of cryptographic leaking that WikiLeaks brought to light seems like a paradox: A movement focused on divulging secrets depends on a technology invented to keep them. But anonymity technologies represent a special kind of encryption: They reveal data itself while hiding certain metadata *about* the data. Specifically, anonymity tools hide that one metadatum that counts most, the IP address that can be linked immediately to a user's location and device. Protecting that one fact is a harder trick than it sounds: In the end, strong anonymity tools have taken more than a decade longer than mere strong encryption to make their way into the hands of the average Internet user. But that strong anonymity, as it slowly matured over the course of two decades, was the lever WikiLeaks used to upend the world.

Today, a schizoid hive-mind of Internet pundits and social media theorists claims, simultaneously, that everyone knows no anonymity exists on the Internet ("These Days the Web Unmasks Everyone," states a *New York Times* headline from 2011) and that everyone knows no *identity* exists on the Internet—that "no one knows you're a dog," as the *New Yorker* cartoon caption reads. Half of security gurus preach about the Internet's invasion of privacy, while the other half bemoan the Internet's lack of authentication, which they say makes the task of identifying bad actors—what they call the "attribution problem"—nearly impossible.

Forget these conflicting parallel realities. The Internet is neither fundamentally private nor fundamentally public, anonymous or onymous. Those who behave a certain way online and use certain services will have no privacy, while those who behave another way and use other services can be very, very hard to identify—harder to identify now, in many ways, than ever in communication's history.

The public and private paths on the Internet have been diverging. Today users have the option to use a service like Facebook, which is designed to learn your real name and attach it to all your actions, preferences, locations, and even thoughts. Or they can use a service like WikiLeaks' now-defunct submission system, which was designed to learn absolutely nothing about them—in fact, to provably demonstrate to users, by using modern anonymity software like Tor, that it *can't* learn anything about them.

All of which is to say that WikiLeaks wasn't a one-off fluke, a brilliant hacker's lucky break, or, as digital pundit Clay Shirky has characterized the press's image of WikiLeaks, a "series of unfortunate events." It was the *inevitable* outcome of the changing nature of information and advancements in cryptographic anonymity, catalyzed to an explosion by Assange's actions.

The first two parts of this book will tell the story of how leaking has been transformed over the last forty years by generations of cryptographers and revolutionary activists of all stripes. The third part tours the post-WikiLeaks world, following the same movement of radical hacktivists as they seek to systematize, replicate, and evolve the craft of disclosure.

As I traveled from San Francisco to Iceland to Berlin to Bulgaria to report this story, I was searching not so much for WikiLeaks' methods, its influences, or its sequels as I was trying to write the story of an ideal that drove this hidden movement. It was on a street in my own neighborhood in Gowanus, Brooklyn, that I saw a busker sitting on a curb, strumming a guitar with the same words scrawled across it that once were written across the one Woody Guthrie played: *This Machine Kills Fascists*. That sentence, to me, brought to mind the ideological arrow I see from Ellsberg to Assange and beyond: a revolutionary protest movement bent not on stealing information, but on building a tool that inexorably coaxes it out, a technology

that slips inside of institutions and levels their defenses against the free flow of data like a Trojan horse of cryptographic software and silicon.

But the machine that kills secrets isn't merely WikiLeaks, or the photocopier that duplicated the Pentagon Papers, or the anonymity network Tor, or even the Internet. It's a living idea—one that continues to evolve in the minds of all those who aim to obliterate the world's institutional secrecy.

PART ONE

LEAKER PRESENT, LEAKER PAST

"The mice will win in the end. But in the meantime, the cats will be well fed."

BRUCE SCHNEIER

CHAPTER 1

THE WHISTLEBLOWERS

When Dr. Daniel Ellsberg decided to violate thirteen years' worth of security clearances, embark on the largest public breach of top secret documents in the twentieth century, and likely spend the rest of his life in prison, he faced a problem: how to duplicate seven thousand pieces of paper many times over using 1969 technology.

RAND, the California military think tank where Ellsberg held a position two steps removed from the president of the United States, didn't have a Xerox machine. The technology was twenty years old, but still not widely used. And it presented some obvious security issues for an agency dealing with ultraclassified materials. So Ellsberg, a thin, thirty-eight-year-old man with wiry dark hair and features that resembled a more Semitic Paul Newman, needed help. He contacted Tony Russo, a mildly subversive Virginian co worker, and Russo soon became the only other analyst at RAND who knew about and sympathized with Ellsberg's leaking plans.

Russo found one of the newfangled photocopiers in the advertising agency of a friend who shared their antiwar agenda. Over the next year, Ellsberg would spend countless nights hauling RAND's papers out of the building in an inconspicuous briefcase, then standing in front of that

primitive copier in a dark office reproducing a secret history of America's involvement in Vietnam: the Pentagon Papers.

It was tedious work. At first Ellsberg tried to copy two pages at a time from one of the forty-seven bound volumes. But he found that the words near the spine were faded and distorted. So he resorted to disassembling the binder and photocopying the pages one by one. "I tried to program my motions," he wrote in his memoir, *Secrets*:

> One hand picked up a page, the other fit it on the glass, top down, push the button, wait . . . lift, move the original to the right while picking another page from the pile. . . . This is all very familiar now, but it was a new technology then. It took a little extra time to put the top down and up, and I didn't know why it had to be done. Did it have to do with the copying quality, or was the light bad for the eyes? Was it dangerously bright? How did it work, anyway? Was that peculiar green color some kind of radiation?

There were complications: Ellsberg intended to give portions of the papers to several senators, and if necessary, the news media too. To make multiple copies, he would have to hand the papers over to a professional copying office, where they'd be subjected to the curious eyes of who-knew-how-many clerks. Inconveniently, the papers were marked with glaring "Top Secret" stamps across their tops and bottoms, with more classified signifiers peppered throughout the margins of the monstrous classified tomes.

So at first Ellsberg cut off the heads and feet of the pages with scissors, later upgrading to a paper cutter. Then Russo suggested he tape strips of cardboard over the top and bottom of the photocopier's glass face, what Ellsberg would later refer to as "declassifiers." Even then, some words were cut off by the declassifiers, and small, randomly interspersed "Top Secret" markings lingered on the edges of the pages. Ellsberg had to comb through the encyclopedia-size pile to excise them. When he thought he was ready to hand the first briefcase-size fraction of the stack over to a New York

copy shop months into his project, he riffled through the papers one last time and was startled to immediately find another page with an obvious, unsheared "Top Secret" marking. He left the copy shop and retreated to a lunch counter where he surreptitiously pruned more "Top Secret" remnants out of the papers while attempting to nonchalantly consume a sweet roll and a cup of coffee over the course of several hours.

The process was punctuated by Ellsberg's periodic visits by the local police. Russo's friend in advertising wasn't particularly skilled at manipulating her office's security system, and the result was multiple silent alarms—an average of three a week—that brought in bored policemen to check on the distinguished-looking man who always seemed to be photocopying late at night. Ellsberg would casually cover the classified documents on the desk beside the copy machine, greet the policemen politely, and carry on his work as soon as they left.

Ellsberg recruited Russo to help with the endless task, along with Russo's advertising friend, Ellsberg's second wife Patricia, even his two thirteen- and ten-year-old children from his first marriage. (Why did Ellsberg involve his children? He writes that he expected to spend the next decades talking to them only through a pane of glass in a federal prison, and he wanted them to at least understand exactly what he had done, and why.)

Even with his ragtag team's help, it took the Harvard- and Cambridge-educated analyst more than a year of on-and-off grunt work to create a full set of the papers and duplicate them at commercial copy centers, eventually creating an eight-foot-tall stack of breached classified documents. At ten cents a page in those shops, the process also required Ellsberg to spend several thousand dollars. (The equivalent of more than twenty thousand dollars today, accounting for inflation.) Once, when he sent a batch of papers off to Senator William Fulbright, Fulbright's aide politely offered to reimburse him. But when Ellsberg named the price—$345 including postage—the aide hastily rescinded the offer. Fulbright, who had told Ellsberg he would launch congressional hearings based on the documents, would later rescind that offer too.

The data leaks that would earn army private first class Bradley Manning the alleged title of the world's most prolific whistleblower weren't merely orders of magnitude larger than Ellsberg's Pentagon Papers. Compared to photocopying seven thousand pages several times over, Manning's leaks were also phenomenally easier—the difference between spending months harvesting a season of crops and playing a few hours of FarmVille on Facebook.

In the midst of his work as a low-level intelligence analyst in Iraq, Manning slipped a rewritable CD marked with "Lady Gaga" into the tray of his work machine, a PC connected only to the military's high-security Secret Internet Protocol Router Network, or SIPRNet. The SIPRNet was "air-gapped": It wasn't connected to the Internet through any plug or wireless signal. But Manning could simply copy the CD's music to the computer, delete it from the rewritable disc, burn whatever top secret data he wanted to the piece of plastic, and walk away with it minutes later. "[I] listened and lip-synced to Lady Gaga's 'Telephone' while exfiltrating possibly the largest data spillage in American history," Manning would write a few months later. "Pretty simple and unglamorous."

The data caches that Manning replicated, allegedly, included 91,000 files from the war in Afghanistan, 392,000 from the Iraq War, 779 files of inmates in the Pentagon's Guantánamo prison, and a quarter of a million memoranda from the U.S. State Department, which also shared its data with troops via SIPRNet.

If the Ellsberg of 1969 could have seen the size of those leaks and the ease with which Manning extracted them, he might have cried at the unfairness of technological progress. One of Manning's Lady Gaga CDs offered enough capacity to have stored the Pentagon Papers about fifty times over, and the laser head that wrote to those discs could have accomplished in a minute or two what required a year of off-and-on work for Ellsberg and his photocopier.

To turn that comparison around, how long would it have taken Ellsberg to copy a leak the size of Manning's using only his 1969 technology? On a modern copier, I found I could only achieve a pace of around eight pages a minute. Assume that Ellsberg was able to photocopy for eight uninterrupted

hours out of every twenty-four—say, from nine at night to five in the morning to avoid suspicion and keep his demanding job at RAND. At that rate, and even with a 2011 photocopier magically transported to 1969, it would have taken Ellsberg six months of straight work to reproduce just one copy of the 261 million words included in the State Department Cables—not even considering the Afghan or Iraqi files—that Manning effortlessly transported onto his Lady Gaga CD.

In fact, Ellsberg never worked steadily at that eight-pages-a-minute pace. If he had, he would have finished copying the Pentagon Papers in a week or less. But at the more realistic pace that Ellsberg set, factoring in the need for sleep, fear of being caught, his much slower copier, distractions, a high-level military job that often required late nights and travel, breaks to maintain his sanity, the need to make secondary copies, and the niggling task of manually scissoring out any evidence of the files' classification before turning them over to a professional copying service, he didn't finish his photocopier work for close to three months of solid work interspersed over a year.

Adding in the textual data that filled the smaller but still massive files from two data-flooded wars and Ellsberg's need to make multiple copies, and it's possible to roughly extrapolate how long a Manning-size leak would have realistically taken at Ellsberg's rate: about eighteen years. Suffice it to say that by then, his revelations would have belonged in a history book rather than *The New York Times*. And therein lies the clearest of so many differences between the act of leaking in the twentieth century and the twenty-first.

--- -.- - .... -.. -.-- .... .--- --. .--- --- -.-. -...

Daniel Ellsberg was born into an upper-middle-class Chicago family in 1931, in the depths of the Great Depression. Though his parents were Russian-born Jews, they had converted and raised Ellsberg as a strict Christian Scientist. Ellsberg's father was trained as an engineer but, like many men in that decade, spent years without work. Although Ellsberg would later come to admire his father, the rosy-cheeked boy with a dark, wiry coif first found a different hero: his father's brother, Ned Ellsberg, the navy admiral and writer. Admiral Ellsberg had risen to fame as a member

of the navy's submarine salvage team, invented an underwater torch for cutting through the steel of sunken ships' hulls, and wrote a dozen fiction and nonfiction books with titles like *Men Under the Sea*, *Ocean Gold*, and *I Have Just Begun to Fight!* The young Ellsberg devoured the books and looked up to their author.

Ellsberg's father found work first in Springfield, Illinois, and later in Detroit in 1937, and the family moved to the middle-class Highland Park suburbs. Ellsberg, an intensely intelligent child with few friends, won a scholarship to attend the prestigious Cranbrook private school, just as World War II began to rage in Europe. Despite his reverence for his military uncle, Ellsberg's early memories of war itself were of a vague and evil specter. One of his elementary schoolteachers passed around a model of a magnesium bomb of the kind capable of penetrating buildings and remaining alight continuously no matter how much water was poured on it. "A particle . . . , we were told, would burn through flesh to the bone and wouldn't stop burning even then," he wrote. "It was hard for me to understand people who were willing to burn children like that. It still is."

Ellsberg was a top student in his classes. But his mother wanted her son to be the next Vladimir Horowitz or Arthur Rubinstein, and it was to the piano that she committed nearly all his time. He was expected to practice for six to seven hours a day. Reading was considered a vice and a distraction, and Ellsberg remembers his mother quietly hiding his books to keep him at the keyboard.

As obediently as Ellsberg followed his mother's ambitions, he was less willing to blindly accept the religion that his parents lived by. At Sunday school, he peppered his teacher with tough theological questions. Later, in his teens, he read and deeply absorbed an exposé of plagiarism in the works of Mary Baker Eddy, Christian Science's founder, that shook the faith his parents had tried to instill in him.

One summer day in 1946, much of the influence that Ellsberg's family held over his life suddenly, violently vanished. On a road trip to a party in Denver, Ellsberg's father fell asleep at the wheel of the family's sedan. He awoke just seconds before the car plowed into the concrete structure of an

overpass, demolishing the right side of the vehicle. Ellsberg's mother was killed instantly. Though the details were initially kept from him, Ellsberg later learned she was beheaded. His father received facial injuries but survived. Ellsberg awoke thirty-six hours later. His sister never did.

When Ellsberg gained consciousness, his father had gone back to Michigan, leaving him in a Denver hospital with his mother's family. For months after the accident, the elder Ellsberg felt too guilty to face his son. Daniel, for his part, was overcome with a strange emotional numbness. He once said that his first thought after his mother's death was simply "I guess I don't have to play the piano anymore."

When Ellsberg did return to Michigan, he was suddenly freed from piano practice and instead began to hungrily consume books. He dramatically accelerated his progress as a student and, two years later, won a scholarship from the Pepsi-Cola Corporation to attend Harvard. One evening early in his time at the university, while sitting on a bench with a beer and a Hemingway novel, he had an epiphany. "It felt so strange, I couldn't figure out what it was," he told a biographer. "Then I realized: I felt *free*, for the first time in my life."

Ellsberg married his college girlfriend, Carol Cummings, graduated from Harvard, and won a Woodrow Wilson fellowship to spend a year studying at Cambridge University. When he returned, he was more than ready to join the war in Korea, a conflict he saw through the simple Cold War lens of a Communist aggressor pushing into a would-be democratic state. He enlisted in the Marines, prepared to fight alongside his brothers at the forty-ninth parallel. But instead, he spent the next two years in officer's training in Quantico, Virginia, long enough that when he emerged, the war was over. He had graduated, again, at the top of his class of a thousand soldiers.

Just months into that military career, Ellsberg was handed his first top-secret security clearances.

Many years and many layers of privileged knowledge later, Ellsberg would have a conversation about that rite of passage with Secretary of State Henry Kissinger, one that he documented in his memoir. Kissinger was about to receive his own high level clearances, and Ellsberg wanted to

prepare him for the heady effects of that rarified information. So he described for Kissinger the experience of entering a world of secrets.

At first, Ellsberg said, he'd felt exhilarated at the enormous bounty of incredible facts that flooded into his intelligence. But that initial feeling soon gave way, and instead he felt like a fool for having worked for so long without those secrets, under such a veil of illusions and ignorance. A couple weeks later, he began to see everyone *else* as fools, watching them labor under that same malformed knowledge he had suffered from for years.

It would take years more, Ellsberg recounted, before he finally began to see the limits of his top secret information, the ways that it blinded him and led him astray with the sense of omniscience it offered. In the intervening time, he says, those secrets often prevented him and other secret keepers from learning anything from anyone who didn't have their clearances. Knowing secrets, Ellsberg told Kissinger, requires a person to lie to and distrust everyone who advises him.

"I ended by saying that I'd long thought of this kind of secret information as something like the potion Circe gave to the wanderers and shipwrecked men who happened on her island, which turned them into swine," Ellsberg wrote of his warning to Kissinger. "They became incapable of human speech and couldn't help one another to find their way home."

.- ...- .... -.- .- ...- ... .- -.-. ...- -.. .--- -. ... ...- .-

If Ellsberg's path to becoming the most prolific leaker of his age began with a steep upward trajectory fueled by Ivy League ambition, Bradley Manning set out from far more common circumstances: destitute, middle-American aimlessness.

Manning grew up in Crescent, Oklahoma, a tiny conservative town that had one stop sign and fifteen churches, "more pews than people," as Manning would later write. He was a bright child who could read at three, built his first website at ten, and won the top prize at his school's science fair three times. He also had a rebellious streak that led him to ask hard questions of religious neighbors, argue with Sunday school teachers, and even remain silent during the Pledge of Allegiance in school to avoid its

"under God" doctrine. But those from his hometown described him to the local magazine *This Land* as a quiet, good-natured boy, small for his age, who studied hard, played saxophone in the school band, loved video games like the military simulation *Command and Conquer*, and talked sometimes of joining the army one day.

Manning's father, Brian, had a more mixed reputation in the neighborhood where Manning grew up. A gruff former navy computer analyst who worked as an IT manager for Hertz car rentals, he was also a strict and unforgiving father. One neighbor has described him as "demeaning," another as simply "a dick." Brian Manning would leave on business, sometimes for months at a time. His wife, a woman named Susan Fox, whom Manning had met while stationed in the United Kingdom in the late seventies, couldn't drive, and they lived four miles from town. So the older Manning would stock up the house with food and supplies and leave them largely isolated. Fox filled the void of her loneliness with alcohol, starting with vodka in her morning tea.

When Manning was thirteen, his father announced one evening that he was separating from Manning's mother. Fox would bring Manning back to her hometown, the Welsh village of Haverfordwest, not much larger than Crescent.

If growing up as the only American in a small British community hadn't been alienating enough, Manning now faced another new emotional challenge: Just before leaving Oklahoma, he had announced to friends that he was gay.

Manning never publicized his homosexuality in Wales, but he was treated as an outsider nonetheless, teased for his accent, his effeminate mannerisms, his small size—even as an adult, Manning would only measure five feet two and 105 pounds. Manning's inability to fit in wasn't helped by a fierce sense of American patriotism that he inherited from his father. One friend from Crescent described him as "basically really into America," particularly Americans' sense of political and economic liberty—not often an outlook shared by the residents of parochial ends of the United Kingdom.

Alienated from most of his peers, Manning turned to the outlet of so many other young men: computers and the Internet. He spent his lunch

periods in the school's computer lab, coding a website that functioned like a primitive version of Facebook, allowing users to create communities and find local news. In the process, he learned about the basics of Web servers and Internet routing.

When he graduated from high school, Manning's strong connection to the United States brought him back to Oklahoma to live with his father and now two stepbrothers in Oklahoma City. He put his computer skills to use at a software start-up called Zoto. The tech firm was a more politically liberal setting than Manning had ever been exposed to, and co-workers remember him speaking out loudly against the deteriorating war in Iraq and criticizing President Bush. In his work, he was a competent coder, but his loneliness and angst sometimes hampered his productivity: One manager, Kord Campbell, has recalled Manning's "thousand mile stare" and described him as "quirky as hell." Manning developed a reputation as odd and unreliable. After a shouting match with his boss, he was fired.

At the same time, the young man's relationship with his restrictive father and new family was fraying quickly. Manning would say years later that he was kicked out of his home because he was gay. But his father told a PBS *Frontline* reporter that he had always accepted his son's sexuality. And a 911 recording of a call from Manning's father's second wife describes Manning throwing objects and threatening her with a knife. "I have been telling him he needs to get a job and he won't get a job!" Manning's stepmother says frantically in the recording. "He said he thinks he should just be able to take money from us." Manning wasn't arrested, but he was escorted from the house by police. Days later, he left in his Toyota pickup truck and drove to Tulsa, homeless, directionless, and largely alone in the world.

For the next months, Manning slept first in his truck and then later in the room of a friend from Crescent, Jordan Davis, hiding in the bedroom from Davis's father until he could find a bare-bones apartment in town. He flitted between menial jobs, working first in a Chucky Cheese–style entertainment center called Incredible Pizza as a waiter, later at a music and video game store. He drifted to Chicago and then to Maryland, working retail jobs at Guitar Center, Starbucks, and Abercrombie & Fitch before

finally moving in with his aunt near Rockville and enrolling in a local community college.

Manning had learned the exhaustion of life without a degree. He writes that he was "in desperation to get somewhere in life." But he couldn't afford a four-year university. When he turned to his father for help, the elder Manning told him to take a well-worn path for resourceless and lost young men: the military. Despite Manning's patriotism and admiration of the armed forces years earlier, his opposition to the war in Iraq left him conflicted. Brian Manning, years later, would say of his son that he "twisted his arm."

"He didn't want to join," Manning's father would tell the PBS show *Frontline*. "But he needed structure in his life, he was aimless. I knew in my own life that joining the navy was the only thing that gave me structure."

The army, as promised, swiftly imposed direction on Manning's career. After Manning enlisted in August 2007, he spent the next year in basic training and then, when his superiors recognized his computer skills, specialized education in intelligence analysis. In October 2009, he shipped out to Iraq, a twenty-two-year-old soldier—slight of frame and short on experience—inducted suddenly into wartime's wealth of secrets.

Daniel Ellsberg read as much paperwork on the war in Vietnam as practically any Pentagon analyst. For one stretch in his first years at the Department of Defense, he requested that all new documents on the war be sent to his in-box, and he spent practically every waking moment digesting thousands of pages. But his real education on the war would come later: in the passenger's seat of a jeep, traveling the roads of the countryside around Saigon with a rifle in his hand and a grenade in his lap.

In 1962, Ellsberg had completed a doctorate at Harvard in economics, focusing on decision theory. His dissertation honed in on what would come to be known as the Ellsberg Paradox, a strange glitch in the way that humans make choices: Show someone two opaque jars with ten stones in each, one with five black stones and five white ones and one with an unknown number of white and black stones. Then tell the test subject he'll

be rewarded for picking a white stone. Experiments show that he'll tend to choose from the jar with a known, equal number of black and white stones. But tell him a second later that he'll be rewarded for choosing a black stone, and he'll *again* choose the jar with known numbers of black and white stones. In both cases, human brains make the assumption that the uncertain jar is less likely to have a favorable ratio of stones, even when those assumptions contradict each other from one second to the next.

When Ellsberg arrived at RAND as an analyst, the White House was already making its choice about which opaque jar it would rather gamble on: armed conflict in Vietnam, or the seemingly riskier idea of letting it fall to Communism and increase the red blotch spreading across half the world map.

Ellsberg spent years at the Pentagon-tied think tank RAND and then as a military analyst in the Pentagon itself, inhaling war files and occasionally digging up documents to justify President Lyndon Johnson's moves to slowly widen the war in Vietnam. But he sensed that the paperwork he was sifting through wasn't the real war, and in 1965 he took a new job at the State Department. Soon he shipped out as a boots-on-the-ground analyst, eager to see the war for himself. He was entrusted with go-anywhere-see-everything status on the irregular banana-shaped landmass known as South Vietnam, and within weeks he was in the field, accompanying troops on operations.

Ellsberg found that he was considered a liability if he didn't carry a firearm or even if he hesitated to use it in combat situations. So despite his State Department civilian observer status, he started carrying a Swedish K submachine gun alongside the soldiers he accompanied, even as he took notes and photographs as an analyst.

The former soldier was soon adopted by John Vann, a seasoned retired lieutenant colonel in the army who had also come to Vietnam as a civilian observer. Vann became Ellsberg's roving guide, mentor, and driver. That was no common privilege: Wheels were a risky way to see the country, and most officers didn't even dare to drive the roads through the swamps and jungles that Vann frequented, instead flying between bases by helicopter. At one point, the utility vehicle that Ellsberg and Vann traveled in momentarily

broke down in the same spot where, three months later, Vann's assistant would be captured by Vietcong and kept as a POW in a cramped bamboo cage for the next seven years.

But Vann believed that driving was the only way for an officer to understand the real truths of the war, and he had learned that a single, nimble jeep could evade Vietcong mines. He taught Ellsberg the roadside clues that the VC firmly controlled certain areas, despite official reports to the contrary. Ellsberg learned to see freshly cut barbed wire fences, dug-up roads, and destroyed buildings just a few feet away from outposts supposedly held by U.S.-friendly Vietnamese.

As Ellsberg interviewed more advisers on the ground, he found more wishful thinking on the part of the U.S. forces: American bureaucrats were told, for instance, that pro-U.S. militias patrolled their territory at night. In reality, much of South Vietnam was handed over to the Vietcong from sundown to sunrise.

When Ellsberg stayed at a base in the town of Long An on Christmas Eve 1966, a very drunk South Vietnamese major began ranting about American arrogance and stupidity. Later, outside, he took several shots with a pistol at Ellsberg and his companions, missing them in the dark before other soldiers could restrain the enraged major. When Ellsberg quizzed a Vietnamese lieutenant about the incident later, the younger man reluctantly admitted that the resentment against American intervention wasn't unique. In fact, many of the other officers felt the same way.

But Ellsberg's notion that Vietnam was an unwinnable war wasn't confirmed for him until New Year's Day 1967, the day he first came face-to-face with Vietcong soldiers. Or rather, face to back. As Ellsberg and three other soldiers walked ahead of a platoon of troops, they suddenly heard firing behind them. Three Vietnamese boys in black shorts had hidden in the grass just feet from where the four men's boots passed, popping up to fire their AK-47s at the troops behind Ellsberg's group. The four Americans didn't dare fire back toward their own men, and instead had to take cover from the hail of bullets sent back from the American platoon.

The three Vietcong boys disappeared into the jungle brush, only to hide

and jump up fifty meters behind Ellsberg's forward group and pull the same trick again before vanishing. Three half-naked kids had shown a kind of fearlessness, cunning, and mastery of the terrain that an entire platoon couldn't counter. Later in the day, a pair of Vietcong outfits performed an even more wily maneuver against Ellsberg's platoon, alternately firing on the Americans and then fading into the jungle, first from the left, then from the right, then from the left again. Each burst dragged the platoon toward their imagined attackers to counterattack, and they found themselves moving in a futile zigzag shape as they sought an efficient and ghostly enemy. "I was very, very impressed," wrote Ellsberg in *Secrets*. The "morning's work had sown in my guts a thought that had been only in my head before: These opponents were going to be very hard to beat. Or to put it another way, we were not going to defeat them."

Over the next months, Ellsberg's feelings were reinforced with impossible missions, disappointing interviews with officers, and repeated glimpses of corruption among the military regime the United States supported. When he returned to RAND in the middle of 1967, he had decided: He would work within the system to end this futile war.

Ellsberg became a hard-nosed critic against the war effort within the think tank's walls. But his arguments merely convinced most colleagues that his experiences had destroyed his objectivity. Despite now working under Special Assistant for National Security Kissinger and others at that near-presidential level, he found that his pessimistic comments regarding Vietnam fell on deaf ears.

Still, his time in Vietnam served a purpose beyond grim education: It made him one of the few RAND analysts chosen to work on a landmark study on the evolution of America's involvement in the country, a classified history that would trace the story of Vietnam's endless wars back to the French occupation and the Japanese invasion that preceded it. At the time, it was known as the McNamara study, named for Secretary of Defense Robert McNamara, who launched it before leaving government to become president of the World Bank. Today, that report is known as the Pentagon Papers.

Ellsberg agreed to help write a portion of the study because he knew

that the assignment would also provide him the access to read the entire report, a multivolume, comprehensive effort with the full analytic weight of RAND's brains behind it. And what he found, as he dug into historical documents and then got his hands on the first volumes of the papers in the following months, put his antipathy toward the war in a new light: The American quagmire in Vietnam wasn't an honest mistake, or even a mistake at all. It was the result of a decades-long policy, the tip of an ugly iceberg older and more trenchant than the Cold War itself.

To summarize seven thousand pages in a few words, the United States had controlled and incited the war in Vietnam—and it was a single war, not a series of wars against different regimes—for nearly twenty-five years. And its motives had always been those of geopolitical empire, never the democratic well-being of Vietnamese citizens.

It started in the mid-forties, when the United States had financially and militarily supported France's control of Vietnam as a colony, and then backed its bloody reconquest of the country after French forces were temporarily interned and pushed aside by Japanese invaders. Despite pleas from Vietnamese president Ho Chi Minh to recognize Vietnamese independence, America's motivation was always, simply, to support its Western ally as a colonial power.

Only after the rise of McCarthyism and the Maoist takeover of China did any question of Communism versus democracy in Vietnam arise. And by then it was too politically painful for any president to retreat from the country and allow the Communist hemisphere of the globe to grow one sliver larger. Meanwhile, as every president from Truman to Kennedy to Johnson to Nixon sank deeper into the widening war, they had *known* that the conflict was inherently imperial from the start, and even seen State Department reports that showed that Ho Chi Minh had the majority support of the population.

Vietnam had never been a true civil war. It was a war of conquest, initiated and perpetuated for more than two decades by the United States, fueled by presidential secrecy and lies. It was no catastrophic accident. As Ellsberg wrote, it was simply "a crime."

After his time on the ground, Ellsberg didn't need much convincing of the war's folly. But the Pentagon Papers put the stamp of historical confirmation on his determination to end it. And in 1969, that education as a leaker would be capped by a fateful trip he took to a Haverford College peace conference.

For Ellsberg, simply attending a meeting full of peaceniks was a radical step. After the first day at the small Quaker school, he found himself on the sidewalk in nearby Philadelphia handing out antiwar pamphlets to passersby, a tactic that at first felt awkward and ridiculous for a high-level insider who had vowed to end the war through his influence in Washington's power structure.

The second day on Haverford's campus, a young man named Randy Kehler stood up to speak to the crowd. Like Ellsberg, he had attended Harvard, then graduated from Stanford. Ellsberg was impressed with his poise and levelheaded intellect, and remembers thinking that Kehler was "the best that we've got" as a country.

In a strong and steady tone, Kehler explained that he had become the last remaining male member of the War Resisters League in San Francisco. All the others had been imprisoned for violating the draft. As Kehler's voice cracked onstage, he told the audience how proud and happy he was that he would soon be joining his friends in prison.

The crowd at first seemed stunned at the thought that the young man in front of them was about to be treated as a criminal. Then thunderous applause broke out.

But Ellsberg couldn't stand. He was emotionally devastated. The senior military analyst stumbled out of the auditorium and into an empty bathroom, where he collapsed and sobbed for an hour. "It was as though an ax had split my head, and my heart broke open," he writes. "But what had really happened was that my life had split in two."

When Ellsberg recovered, he made a promise to himself: He would do whatever he could to end the war. Even if it meant going to prison.

Two essential traits of a leaker are an abundance of knowledge and a lack of power. And Bradley Manning both had access to far more information and wielded far less power than Ellsberg ever did. As the young soldier would later write, he was "smart enough to know what's going on, but helpless to do anything."

Manning's army career would quickly become as troubled as his premilitary life. By the middle of 2010, he had been demoted for hitting another soldier and shouting down a superior, assigned to hauling around boxes in the supply closet and working at events like a sparsely attended barbecue for a visiting team of cheerleaders. On one occasion, an officer found him curled in a fetal position on the floor. On another, he was found sitting alone with a knife, the two words *I want* carved into a wooden chair. Fear for his safety and his mental state had led a superior to remove the bolt from his rifle. Even then, he retained his secret classification privileges.

Manning's demotion may have also been linked to the fact that he now made little effort to conceal his homosexuality, even attending demonstrations against California's anti-gay-marriage Proposition 8 while stationed in upstate New York. He told a reporter that he had been kicked out of his home and lost a job because of his sexual orientation. He said that the military's don't-ask-don't-tell policy was forcing him to live "a double life."

His Facebook statuses referred to a Boston boyfriend, Tyler Watkins, whom he had met while on leave there prior to shipping out to Iraq. "Bradley Manning is glad he is working and active again, yet heartbroken being so far away from hubby," read one status update. And another: "Bradley Manning is in the barracks, alone. I miss you, Tyler!" Manning would write later of his decision to "transition" to becoming a female named Breanna Manning. On one of his leaves, he spent days dressed as a female in public, and had begun planning for electrolysis and other sex change procedures after his discharge.

But the moment that Manning would cite as setting him on the path to become his era's most prolific leaker didn't come during his social struggle in the army's ranks. It occurred during his work as an analyst, one of the hundreds of thousands with access to the army's endless classified troves

of information. And it happened far more quickly than Ellsberg's long-burning transformation from hawk to dove.

Fifteen detainees had been taken in by the Iraqi Federal Police for printing "anti-Iraqi literature," and Manning was assigned to investigate the situation. He soon determined that the prisoners hadn't advocated violence, but had simply written what Manning described as a "scholarly critique" of Prime Minister Nouri al-Maliki, looking into possible corruption in the prime minister's cabinet. "I immediately took that information and *ran* to the officer to explain what was going on," Manning would later write. "He didn't want to hear any of it . . . he told me to shut up and explain how we could assist the [police] in finding *more* detainees. . . ."

"I had always questioned the way things worked, and investigated to find the truth. But that was a point where I was a *part* of something. I was actively involved in something that I was completely against," he wrote. "Everything started slipping after that. . . . I saw things differently."

Manning dug deeper, browsing the State Department database he would later be accused of spilling to WikiLeaks: 251,000 memoranda describing the intimate dealings of the world's leaders in candid terms. He described "crazy, almost criminal political back dealings, the non-PR versions of world events and crises, all kinds of stuff like everything from the buildup to the Iraq War during Powell, to what the actual content of "aid packages" is.

"There's so much . . . it affects everybody on Earth. Everywhere there's a US post, there's a diplomatic scandal that will be revealed. . . . Iceland, the Vatican, Spain, Brazil, Madagascar, if it's a country, and it's recognized by the US as a country, it's got dirt on it," Manning wrote. "It's open diplomacy . . . world-wide anarchy in CSV format. It's beautiful, and horrifying."

Finally, he writes of a video shot from the cockpit of an Apache helicopter, showing a group of men being killed by the aircraft's heavy weaponry. "At first glance, it was just a bunch of guys getting shot up by a helicopter. No big deal, about two dozen more where that came from," wrote Manning. But the video was being stored in the file of the Judge Advocate General, implying that it was being used in some sort of military justice proceeding.

So Manning tracked down the video's date—a day in July 2007—and its coordinates, a Baghdad suburb called New Baghdad. And he linked those facts with a story in *The New York Times* that revealed two Reuters journalists had been killed in the helicopter airstrike, along with nine insurgents on the ground and in a black van, who the military said had been firing on U.S. soldiers.

Manning knew that the men on the ground hadn't, in fact, been firing on anyone. The Apache helicopter had mowed down the group from above without any evidence that they were insurgents. And the black van that had pulled up beside the wounded and dying men to help them had similarly been mere civilians, a family hoping to save the lives of a group of strangers who lay dying on the street and sidewalk. But the helicopter had rained down bullets on the van, too, wounding two children and killing their parents. "Well it's their fault for bringing their kids into a battle," one soldier quipped in the clip's audio track.

"I kept that in my mind for weeks . . . probably a month and a half," says Manning. Then he decided: He would hand it over to WikiLeaks, where it would become the prologue for a classified exposé to dwarf all others in history.

--- ---- -- .... ---- ---- -- --- ---- ---- ---- --- --- . ...

Adrian Lamo seems to have fallen asleep. His head hangs suspended over his lunch, a plate of salmon, plantains, and vegetables next to a cup of coffee that he has filled to the brim with cream and five packets of sugar.

We're sitting in a restaurant that serves Colombian food, a few blocks from his home in a dreary town that he's requested I not name. Instead, the thirty-year-old hacker has asked me to write only that we met on "an island," a taunting clue to the legions of angry supporters of WikiLeaks and Bradley Manning who would like to locate Lamo and harass or harm him. Those pursuers aren't a figment of Lamo's imagination. Just days before, a news crew from Al Jazeera posted a TV interview of Lamo that included a momentary shot of his computer. One of his many online stalkers quickly spotted an Internet protocol address on the screen, performed a Whois lookup to find a

registered location in Carmichael, California, and posted screenshots of the information online. Luckily for Lamo, it was an old address.

Still, Lamo hasn't shaken his paranoid compulsions, partly residual from his years as a hacker and homeless drifter. When we sit down at the restaurant, he insists on switching seats "to face the door," despite the fact that both of our seats are perpendicular to the exit.

The question that seems, a few minutes into our meal, to have had such a soporific effect on Lamo is this one: Now that Bradley Manning has been placed in an isolated cell in a Quantico, Virginia, brig awaiting trial, largely deprived of exercise and visitors and forced to strip and wear nothing but a coarse smock every night to prevent him from committing suicide with his underwear's elastic band, does Lamo regret having turned Manning over to authorities? Looking back, would he still have drawn him out in online conversations that stretched over days as Manning confessed every detail of his leaks, and then turned those incriminating logs over to the authorities?

Lamo has responded by closing his eyes and allowing his head to bob and sink slowly for several seconds. I consider reaching over to tap him on the shoulder. Before I do, he suddenly looks up and answers me.

"The man is the equivalent of a spy. He's our next Aldrich Ames or Robert Hanssen," Lamo says, naming two convicted double agents who sold information to the USSR over several decades. Lamo's speech is a robotic slur, a result of the cocktail of psychoactive prescription drugs he takes daily. But his hazel eyes have opened wide and he's now staring at me with surprising lucidity. "The only difference is that instead of giving information to the Soviets, he's giving it to an antisecrecy organization. In another country, he'd get a bullet in the head. Here, he gets donations and approbation."

Lamo's hair is slicked back away from a pudgy, almost feminine baby face. In his pierced left earlobe is a small screw he wears as an earring. He wears a blue shirt tucked into his jeans over a potbelly that's likely another side effect of his medical regimen. Earlier, Lamo listed five names of drugs he says he takes to treat his Asperger's syndrome, a form of autism. But when I consult with a doctor after our meeting, I learn that the drugs are

generally used for treating chronic pain, depression, and schizophrenia. There is no prescription drug for the treatment of Asperger's.

Lamo goes on to argue that the story of Manning's mistreatment comes from just the few supporters that have managed to visit him: Manning's friend David House and his lawyer, David Coombs. "Manning is being treated as any maximum security detainee would be treated," Lamo slurs. "It's being played up as a sideshow to garner sympathy."

But House and Coombs aren't the only ones to point out Manning's mistreatment. Just the week before, P. J. Crowley, the State Department public affairs official, called Manning's treatment by the military "ridiculous, counterproductive, and stupid" before resigning his government post. Later, a UN torture investigator would also speak out after being barred from visiting Manning.

The waitress comes over, and Lamo, who spent part of his childhood in Colombia, makes her laugh with a few words in slurred Spanish. Then he takes a sip of coffee, but his mouth doesn't seem to function properly, and he moves the liquid around in his cheeks for several seconds before swallowing.

I continue: Doesn't it open Lamo to charges of hypocrisy that he turned Manning in for the same information-wants-to-be-free attitude that Lamo himself preached during his years as an illegal hacker?

Lamo looks down into his plate, closes his eyes, and his neck muscles seem to relax. After a few seconds I fear again that he's finally passed out in his chair. When he looks up suddenly, this time I twitch in surprise. "I know that saying this isn't going to make me very many friends," Lamo says. "But had Manning released just that video and nothing else, I wouldn't have told anyone about it. I would have even exfiltrated it myself if I were him." Lamo pauses, as if to let this sink in.

"He should have gone through the files," he continues. "Instead, he said, 'There are a million documents. I've read one millionth of a percent of them, but I've established there's no harm in releasing them.'"

Lamo goes through a convoluted arithmetic he says he used to make his decision, first weighing the good of the victims of the helicopter strike and their families versus the good of the soldiers who carried out that strike

and then the good of Manning versus that of the secrecy of the entire United States military and State Department. And since the moment that he committed to handing over his instant messenger chat logs to the authorities, Lamo says he hasn't doubted the conclusions of his moral calculus.

Lamo's lids fall to half-mast. "He wanted to make the world a better place. He just didn't know what he was doing," he intones flatly. "I wish there could have been some other resolution. I actually suggested to the agents that they keep him around and feed him disinformation. Instead, they chose to grab him."

This is the stranger, of all possible strangers, to whom Bradley Manning chose to confess a leak that may put him in prison for the rest of his life.

When Manning sought out Lamo as a confessor and friend, he had some reason to believe that the older hacker was a kindred spirit. For several years at the beginning of the last decade, Lamo was one of the media's favorite digital deviants: the so-called "homeless hacker." Traveling back and forth across the United States by Greyhound, fueled by amphetamines and painkillers, sleeping in abandoned buildings and on friends' floors, Lamo would stop into twenty-four-hour Kinko's to use their computers for marathon hacking sessions.

Lamo avoided traditional network intrusion, which uses unpatched vulnerabilities in the victim's software. Instead, he often exploited misconfigured proxy servers, meant for use by outsourcing firms and other corporate partners, as hidden gaps in corporate firewalls. Using Internet Explorer as his only tool, Lamo would pry open those gaps and enter forbidden networks.

Once, he tells me, he could have transferred the entire cash pool set aside for bonuses at the telecom giant MCI WorldCom to any account he chose. On another occasion, he found a bug in AOL's network that allowed hackers to hijack users' instant messenger accounts, and he later hacked a Yahoo! website to insert a dig at President Bush into a news story. He carried a stun gun on his travels and used it for electrocuting various objects like electronic locks and vending machines, which sometimes responded by spitting out change or food.

In 2002, Lamo dug up a flaw in *The New York Times*' corporate password system, and exploited it to add his name to the paper's list of op-ed

contributors beside the former head of the NSA, Robert Redford, and Rush Limbaugh. On that same field trip inside the *Times*' network, he also used the paper's account to run the equivalent of three hundred thousand dollars in searches on the paid research service Lexis-Nexis.

Lamo made a point of minimizing the damage from his hacks and alerting the administrators of the systems he exploited, going so far as to walk them through the necessary steps to close their security holes. But in the case of the *Times* adventure, Lamo's victim didn't see his intrusion as a favor. The company turned his case over to the FBI, which put out a warrant for his arrest and tracked the twenty-two-year-old's itinerant wandering for five days before he surrendered himself to police in Sacramento. After a year-long trial, Lamo pled guilty and was sentenced to pay sixty-five thousand dollars in fines and spend six months under house arrest at his parents' home.

After the *New York Times* case, Lamo became a poster boy for the well-intentioned hacker misunderstood by society. He starred as the central character in a documentary film titled *Hackers Wanted* that focused on his mistreatment at the hands of federal law enforcement. In the final message of that film, Lamo gives a soliloquy on digital ethics that transcend what's legal or illegal, delivered at fast-forward pace that sounds nothing like his drug-swamped speech today:

> I hoped and believed that I could [hack systems] in a way that would set a precedent that would allow people to come forward in good faith to try to do the right thing, to let them believe that maybe motives did matter, that it wasn't all black-and-white. I think this is symptomatic of something we're seeing in the government today. In many ways they're eliminating shades of gray. They want to polarize people. It's important to our national agenda today to see good guys and bad guys. Because as soon as we start to believe that maybe it's not all black-and-white, that someone can do wrong for a good reason, that not every action of law is inherently infallible, it strikes a very dangerous precedent for the government the way it wants to operate today.

After the documentary's filming was completed in 2003, *Hackers Wanted* went unreleased for seven years until it was finally leaked in May of 2010 onto copyright-flouting BitTorrent file-sharing networks, where it became a modest hit in the world of hackers and information security. Lamo insists he wasn't the source of the leak.

When fans wrote to Lamo and the film's director, Sam Bozzo, asking how they could support the film with donations, Lamo wrote on his Twitter feed on May 20 that donors should give their money instead to WikiLeaks, the whistleblower organization that one month before had released Manning's Apache helicopter video to an explosive response.

For a young, conscience-stricken soldier who had just completed a massive leak of secret documents, everything would have pointed to Lamo as a sympathetic confidant.

Just a day later, Lamo says he began receiving e-mails from Bradley Manning. The text of the messages was encrypted, and the public key encryption Manning had used was designed so that only Lamo could decrypt it. But Lamo couldn't find the key that would unlock those messages, so they remained hopelessly scrambled. Lamo wrote back suggesting they simply chat over instant messenger.

On May 21, Lamo received the following message, this time encrypted using the Off-the-Record chat protocol:

"Hi. How are you? I'm an army intelligence analyst, deployed to Eastern Baghdad, pending discharge for 'adjustment disorder' . . . I'm sure you're pretty busy," the message from a user named Bradass87 read. And then before even waiting for a response, it continued: "If you had unprecedented access to classified networks fourteen hours a day seven days a week for eight plus months, what would you do?"

--- -. - .... ---- --- ---- .... -.-. .... --- -. .... .-. .. ----

After a year of shuttling briefcases of documents out of RAND and standing over photocopiers for nights on end, Ellsberg was ready to spill the Pentagon Papers. His next problem: finding someone to take them.

Ellsberg's Plan A was to have a legislator read the papers into the *Congressional Record* or hold a hearing based on them, an avenue to the public that still played within Washington's rules. But Ellsberg's first choice in the Senate, William Fulbright, balked. After some initial enthusiasm, Fulbright read a portion of the documents and performed a swift about-face after he realized just what kind of political maelstrom might surround the report's release. "Isn't it after all only history?" he asked Ellsberg dismissively when they next met in his office.

Ellsberg moved on to the Democratic presidential hopeful Senator George McGovern, who at first seemed even more gung-ho about airing the papers. McGovern offered to read the study on the Senate floor as filibustering material, which would make it fair game for the media. "I want to do it. I will do it," Ellsberg remembers the Democratic legislator declaring in their meeting.

A week later, he called Ellsberg on the phone. "I'm sorry, I can't do it," McGovern said. His campaign for the presidency, it seemed, would have been hamstrung by the controversy of a political pipe-bomb like Ellsberg's leak.

So Ellsberg turned to Plan B, a whistleblowing outlet he felt was almost sure to result in his spending many years in prison: the press. A few years earlier, Ellsberg had experimented with several single-document leaks to *The New York Times* aimed at chipping away at Vietnam policy. So he knew a political reporter there, Neil Sheehan. Ellsberg had moved to Cambridge after resigning from RAND to protect his former colleagues from whatever backlash might follow the papers' leak. And in his apartment near Harvard Square, he showed Sheehan a copy of his stolen bounty. Sheehan took a portion with him, but told Ellsberg his editors still hadn't decided whether to go ahead with publication.

In fact, Sheehan's pretense of dallying over the study was designed to prevent the *Times* from being scooped by another publication. A few weeks later, Sheehan used a key Ellsberg had loaned him to sneak into the Cambridge apartment, have the papers photocopied in a nearby shop, and return them. The newspaper had already rented out a portion of the New York Hilton and begun frantically, secretly, building its story on the study.

On June 13, 1971, the story splashed across the front page of the *Times*: VIETNAM ARCHIVE: PENTAGON STUDY TRACES 3 DECADES OF GROWING U.S. INVOLVEMENT.

And how long did it take for the leak to be traced to Ellsberg? In fact, some RAND analysts already suspected him even before the *Times*' presses started rolling. The newspaper had called RAND executive Leslie Gelb to give him a chance to comment on the story, and according to Ellsberg biographer Tom Wells, Gelb immediately fixated on Ellsberg as the source. How many high-level analysts, after all, had both access to the papers and such a fierce opposition to the war?

The White House didn't take long to finger Ellsberg either. In archived White House recordings, Nixon names Ellsberg and RAND executives Mort Halperin and Leslie Gelb as the only three analysts who had access to the study. Within days, Ellsberg—or "Ellstein" as Nixon called him with crude anti-Semitic humor—was being discussed as the assumed perpetrator of the leak.

When the *Times* hit newsstands, it immediately launched a free-speech battle that would redefine the First Amendment. The White House, arguing that the *Times* had violated the Espionage Act, successfully convinced a federal court to file an injunction against the newspaper to prevent it from publishing any articles on the study. But Ellsberg had already given another copy to *The Washington Post,* which picked up where the *Times* left off.

The *Post* was injuncted too. But Ellsberg stayed a step ahead of the government's censors, distributing copies of the study to *The Boston Globe,* the *L.A. Times, The Christian Science Monitor,* the *St. Louis Post-Dispatch,* and others, avoiding wiretapped phones and staying in friends' houses to dodge arrest until all the papers could be distributed. Faced with an endless game of injunction Whac-A-Mole, the White House would eventually give up on preventing the papers' publication.

Meanwhile, any illusion Ellsberg may have had of remaining anonymous quickly collapsed. A legislative aide to McGovern and Senator Pete McCloskey—another senator who had rebuffed Ellsberg's leak offer—both told *Newsweek* that Ellsberg had offered them classified documents. The FBI soon extracted an affidavit from Ellsberg's ex-wife, whom he'd told about the leak to prepare her for the possibility that he would soon be in prison and unable to pay alimony. In exchange for a grant of immunity, Tony Russo's advertising friend—the one who had offered Ellsberg her photocopier—testified to the bureau's agents too.

Every element of Ellsberg's leak—from his access to narrowly shared information to that information's copying to its distribution to countless reporters—had left fingerprints for the feds. The press certainly had no doubts: By the time that Ellsberg turned himself in to federal authorities in Boston, *Time* magazine had already put his face on its cover below the words "The War Exposed."

With no anonymity tools or cryptographic protections at his disposal, the whistleblower had also exposed himself.

In Baghdad's forward operating base, Hammer, where Manning was stationed as an intelligence analyst, security was shockingly lax—"physically, technically, and culturally," as Manning would tell Lamo. He sat among rows of other young analysts watching car chases, music videos, clips of buildings exploding, and often writing data to CDs and DVDs. Even the locks on the doors weren't properly implemented. Though they were secured with electronic codes, soldiers would simply knock and be let in. "The culture fed opportunities," he wrote.

And then there were the networks. Although SIPRNet wasn't connected to the Internet, it lacked sophisticated monitoring. Manning would tell Lamo that he once asked an NSA agent at the base if the network was capable of detecting local suspicious activity. Manning says the agent responded that it "wasn't a priority" and returned to watching the Shia LaBeouf film *Eagle Eye* and eating Girl Scout cookies. On another occasion, Manning says he asked the agent specifically about a hypothetical mass internal leak. Manning says the agent responded that he doubted "anyone could figure it out. . . . Resources are strained."

"Weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis," Manning listed to Lamo. It was, all told, a "perfect example of how not to do infosec."

In a Senate hearing in early 2011, Senator Susan Collins would grill military and State Department officials over those exact vulnerabilities. "How could it be that a low-level member of the military could download such a volume of documents without it being detected for so long?" she asks in a slow, exasperated tone. "That truly baffles me."

Thomas Ferguson, the deputy undersecretary of defense for intelligence, answers her, sounding distinctly like the teacher's pet who finds himself in the assistant principal's office. "The situation in the theater was such that we took a risk," the gray-goateed official responds flatly, trying to get his confessional over with as quickly as possible. "We took a risk that by putting information out there . . . to provide agility and flexibility of the military forces there, they would be able to reach into any database on SIPRNet, download that information, and move that information using removable media."

And why weren't there at least network forensics to catch Manning after his epic data dump? Here the heat can almost be felt building under Ferguson's collar. "A lot of the systems there are, for lack of a technical term, cobbled together," he continues with a tight chest. "It's not just like Bank of America where it's one homogeneous system and they can insert things and take them out. They have multiple systems and putting in new intrusion software or monitoring tools, you have to approach each system differently."

The military, he adds, "took on the risk. . . . These people are cleared, they go through background investigations."

And then finally, the remarkably honest kicker: "Frankly, most of our focus was on the outside intruder threat, not the inside threat."

Manning, by all indications, was the quintessential insider threat, and he fluidly negotiated the network's vulnerabilities. In fact, until he sent his fateful, encrypted missive to Adrian Lamo, he performed most of his epic data breach as if he were following a leaker's best practices handbook.

As Manning told Lamo, the two SIPRNet machines that linked to troves of classified information lacked most of the forensic monitoring tools that

might have detected his abnormal searches and his repeated copying of that data to his camouflaged rewritable disks. But even after collecting that contraband, Manning didn't dare leak it over Internet-connected military networks to WikiLeaks. The timing of his leaks suggests he waited until he was able to return to the United States on leave, and upload it from his MacBook's connection to a nonmilitary network—perhaps from his aunt's house in Rockville, Maryland. Like Ellsberg, in other words, he walked his leak out through the Pentagon's front door.

From there, Manning described to Lamo how he used a combination of security tools to cover every link in the leaking chain that led from WikiLeaks to his MacBook. He connected to WikiLeaks' Web servers that deployed Secure Sockets Layer, or SSL, the Web encryption commonly used to hide e-commerce or banking sites' data from any network snoops looking for passwords or credit card numbers. Then he used Secure Shell File Transfer Protocol, or SSH FTP, a method of creating a tunnel of encryption between two remote systems to allow them to securely share files. Finally, and most significantly, he ran Tor, an anonymity tool that took his path to WikiLeaks' drop site through a series of hops around the Internet, each new address in the series encrypted to prevent anyone from piecing together his final destination and his origin. With that hidden, trace-resistant connection set up, Manning proceeded to siphon out the military's secrets, through Tor's tangle of obfuscating blind alleys around the world, and out to the WikiLeaks server at a data center in Stockholm, Sweden.

A year later, after Manning's loose lips had led military investigators to his name, they confiscated every machine that might have been involved in his leak, from the SIPRNet computers to the MacBook that had by then been shipped back to his aunt's home in Maryland. With access to those specific computers, the game was over. Investigators found plenty of evidence stored on his hard drives to tie Manning to the leak: He had attempted to expunge all the evidence on his MacBook by overwriting the files with junk data, but his laptop had somehow aborted the process. There were Guantánamo detainee files, ten thousand State Department Cables, and—significantly—chat logs between Manning and Julian Assange in which

Assange seemed to help Manning crack into an administrator's account to access the military network while covering his tracks. (Assange had wanted to know as little about Manning as possible, and their communications likely remained pseudonymous. "Lie to me," he had told Manning.)

Investigators even found a "readme" file on Manning's MacBook that he had submitted to WikiLeaks along with his megaleak. "This is possibly one of the more significant documents of our time, removing the fog of war, revealing the true nature of 21st century asymmetric warfare," it read. "Have a good day."

But it's important to remember that none of those fingerprints initially led the investigators to Manning's name. Adrian Lamo, not digital detective work, put the army on Manning's scent: All appearances indicate a forensic trail from WikiLeaks to Manning's identity was never found. Before Lamo handed the investigators Manning's name on a platter, they could hardly have confiscated every machine on SIPRNet—not to mention every possible laptop used by every intelligence officer on leave in every home in America. Manning, after all, was just another of the 1.2 million Americans with a top-secret security clearance, a well-concealed needle in the towering military-industrial haystack.

All of which means that if the young army private hadn't detailed his entire leaking process to a stranger he had met online just minutes before, step by incriminating step, he might never have been found out.

.... .--- --.- ..-. --- -.. - .--- .. -.-- -- .--- ..- .--- ..- . .

Ellsberg's leak was such a blow to President Nixon's ego and sense of executive power that the White House overreacted in spectacular fashion. "Goddammit, someone has to go to jail!" Nixon was recorded saying, pounding on his desk with a fist. "That's all there is to it!"

Later, the administration's attack methods broadened: "We've got to get him," the president said to Kissinger and Attorney General John Mitchell, referring to Ellsberg. "Don't worry about his trial. Just get everything out. Try him in the press. . . . We want to destroy him in the press. Is that clear?"

What came next must be considered some of the most absurd and

shameful tactics in presidential history. One group of Nixon's operatives followed Ellsberg's psychotherapist, Lewis Fielding, disguised with wigs, pipes, and, for one agent, a shoe insert to create a fake limp. Later they broke into Fielding's office to dig up Ellsberg's records. The burglars hoped to find dirt on his personal life, or even a connection to a foreign government or subversive group. They found nothing: Fielding hadn't stored any notes on Ellsberg in his office.

The break-in was followed by an attempt to drug Ellsberg with LSD before a speech he planned to give in Washington. Cuban hotel workers in Miami were recruited by a team led by G. Gordon Liddy to infiltrate the event, spike Ellsberg's soup with acid to "befuddle" him, and "make him appear to be a near burnt-out drug case." But by the time it was all approved, the Miami waiters couldn't be flown to Washington in time. The plan was scrapped.

In the Watergate trial, prosecutors would find that a team of twelve Cuban men had also been hired to assault and "totally incapacitate" Ellsberg at a peace rally. Members of that team later said their mission had been variously to punch Ellsberg in the face or break his legs. But the crowd around the newly famous whistleblower had been too thick, and the twelve goons decided to instead beat up random, unlucky protesters at the event's edges.

Much of that criminal behavior didn't become public until after Ellsberg's trial. But in the meantime, Ellsberg's defense team found that investigators had illegally wiretapped Ellsberg and RAND's Mort Halperin without a court order and, even worse, neglected to share those files with the defense. Finally, the judge in the case, William Byrne, revealed that he had been approached by a Nixon aide and offered nothing less than the directorship of the FBI in exchange for influence in the Ellsberg trial.

That mountain of improprieties added up to a mistrial. "The totality of the circumstances of this case . . . offend a sense of justice," wrote Byrne in his decision. "The bizarre events have incurably infected the prosecution of this case."

Ellsberg was free. The same day, newspapers reported that Nixon's attorney general, John Mitchell, who had indicted Ellsberg, had himself been indicted on charges of conspiracy, obstruction of justice, and perjury.

It was the beginning of the end of the Nixon presidency—and, eventually, the war in Vietnam.

. ... .. -.. --- .. --- --- .--. . .. -- .--. . -.. .

When Manning and Lamo first began their exchange of encrypted messages, Lamo made two promises of confidentiality. "I'm a journalist and a minister," he told Manning. "You can pick either, and treat this as a confession or an interview (never to be published) and enjoy a modicum of legal protection."

In fact, within forty-eight hours of first contact with Bradley Manning, Lamo says he was already mulling the possibility of turning his newfound friend in to authorities. He contacted Tim Webster, a former army counterintelligence agent and friend, and later Chet Uber, an ex-intelligence contractor who worked with Lamo in a volunteer cybersecurity research group called Project Vigilant.

Webster put Lamo in contact with army counterintelligence officers who soon telephoned him at his home. They were skeptical, and asked for proof of Lamo's claims. It hardly seemed credible that a private first class had accessed and stolen gigabytes of some of the world's most sensitive information and then confessed it casually over instant messenger to a stranger. Lamo says he responded by referring to a code-named secret project that Manning had mentioned to him. There was a long silence. Then one of the agents asked Lamo never to repeat that code name. "They told me to forget that I'd ever even heard the word," he says. The feds didn't question Lamo's credibility again.

The call with the Criminal Investigation Division (CID) led to a meeting with FBI agents. Uber would remember that at this point Lamo was conflicted and even called Uber in the middle of his sit-down with the G-men. "I'm in a meeting with five guys and I don't want to do this," Uber says Lamo told him. The older man says he responded, "You don't have any choice, you've got to do this."

For the next two days, Lamo continued to chat with Manning, now with the knowledge that federal agents would be looking over his shoulder at their conversation. They discussed religion, Lamo's legal history, and the

"crazy white-haired Australian" Julian Assange, with whom Manning had been communicating. At one point, Manning began to wax lyrical about the victims and perpetrators of the Apache helicopter video he had helped to expose, which WikiLeaks had used to send shock waves around the world just a month before. Manning mentioned that he'd recently added several of the people involved as friends on Facebook. Those individuals included thirty-three-year-old ex-soldier Ethan McCord, who had been racked with guilt over his involvement in the highly publicized Apache helicopter attack and would later speak out against the war. "They touch my life, I touch their life, they touch my life again . . . full circle," Manning wrote.

"Life's funny," Lamo responded.

Then Lamo abruptly changed the subject. "*random* Are you concerned about [army counterintelligence] looking into your Wiki stuff?" he asked. "I was always paranoid."

Manning responded that there was "no open investigation," a sign that he had likely been doing some investigations of his own—counter-counterintelligence. In later conversations, Manning went on to describe how all records of his leak had been "zerofilled"—irreversibly deleted—and to describe the arsenal of anonymity and privacy tools he had used. Lamo asked him what he would do if his cover was blown anyway. "Try and figure out how I could get my side of the story out . . . before everything was twisted around to make me look like Nidal Hasan," Manning replied, referring to the army major who quietly became a radical Islamist and went on a shooting spree at Texas's Fort Hood in 2009, killing thirteen and wounding twenty-nine.

"I don't think it's going to happen," Manning added. "I mean, I was never noticed."

Near the end of their series of chats, Manning seems to be contemplating more existential questions: "I'm not sure whether I'd be considered: A type of 'hacker,' 'cracker,' 'hacktivist,' 'leaker' or what . . ." he mused. "I'm just me . . . really."

"Or a spy," Lamo wrote back, adding a smiling emoticon.

On May 26, less than a week into his chats with Lamo, Manning was arrested by army criminal investigators. He was charged with more than

two dozen crimes, including violating the Espionage Act and aiding the enemy. The second of those crimes is punishable in the military justice system with death. But Manning's prosecutors have stated that they don't plan to argue for Manning's execution. Only a life sentence in a military prison.

In March 2011, ten months after Manning's arrest, Daniel Ellsberg stood in front of the White House wearing a navy blue suit and tie, along with hundreds of others protesting Manning's inhumane confinement in a Quantico, Virginia, military jail.

In July, Manning had been moved from a brig in Kuwait to the Quantico base, where he was kept with virtually no contact with other prisoners, allowed an hour of walking exercise a day and just a few hours of visits a week. One of the few friends who managed to see him on a regular basis, a researcher at MIT named David House, describes Manning's deteriorating mental condition over the next months, as a bright twenty-three-year-old eager to discuss physics and sociology slowly devolved into a medicated, near-"catatonic" state. When House saw Manning in February, he says it was as if Manning "had been sleeping hard for days, and needed hours to fully wake up."

At the March protest, the seventy-nine-year-old Ellsberg was asked by police to leave the street in front of the White House, as protesters chanted, "This is what hypocrisy looks like!" He politely declined to leave and was put in handcuffs and taken away in a police van. When he and the other 112 arrested protesters were released later, he promptly traveled to Quantico, where he had trained as an officer in the Marines decades earlier. Outside the base there, he staged another sit-in and was arrested again.

In interviews with reporters around that time, Ellsberg said that he identifies with Manning "more than anyone else I've seen in the last forty years."

"I was that young man," he told a CNN reporter. "I was Bradley Manning."

President Barack Obama disagrees. After a fund-raising event a month later, the president was confronted by a protester doggedly asking him about Manning's confinement. Obama didn't shrink from offering his views, which were caught on camera and soon posted to YouTube. "We're a

nation of laws," the president says with a smile to the Manning supporter questioning him. "We don't let individuals make their own decisions about how the laws operate. He broke the law."

"Isn't that just the same thing as what Daniel Ellsberg did?" Obama's interlocutor asks.

"No, it wasn't the same thing," Obama responds dismissively. "Ellsberg's material wasn't classified in the same way." The president turns away, and the conversation is over.

Obama is right, of course. It wasn't the same thing. The materials that Ellsberg leaked were actually of a *higher* top-secret classification. But the president was right on a deeper level too. Ellsberg, despite his sympathy for Manning, is not "that young man."

Daniel Ellsberg's story is that ultrarare conversion of an elite military leader into a radical dissident. Only a handful of officials had the authorization to read the Pentagon Papers. For Ellsberg to both have had the privileged access to the documents that he leaked and to actually have leaked them required a unique combination: a highly distinguished career that brought him to the pinnacle of Pentagon secrecy and a complexity of conscience that allowed him to execute a 180-degree turn in his loyalties near the peak of that career.

Manning, by contrast, was one of the millions of Americans with lower-level security clearances. He fitted the profile of a leaker from the moment he entered the Pentagon's employ: disaffected, powerless, strong-willed, and antiauthority.

In comparing Manning to himself, Ellsberg cites Manning's statement in his chats with Lamo that he "wouldn't mind going to prison or being executed." "I never thought, for the rest of my life, I would ever hear anyone willing to do that, to risk their life, so that horrible, awful secrets could be known," Ellsberg told the CNN reporter. "Then I read those logs and learned Bradley was willing to go to prison. I can't tell you how much that affected me."

But Ellsberg generously overlooks the fact that although Manning says he was *willing* to go to prison, he never *expected* to. Everything in Manning's conversations with Lamo indicates he felt that the anonymity and

privacy tools he had used—along with the army's negligent lack of security precautions—had rendered him immune from punishment. Ellsberg, by contrast, assumed he would spend much if not the entire rest of his life in prison, and even made practical preparations for the day when he would be separated by bars and razor wire from his wife and children.

The conclusion to this story, that today Ellsberg is free while Manning is shuttled between jail cells and courtrooms to potentially face a life behind bars, might be misleading. In fact, while the technical play-by-play of each leak shows the evolution of leaking technology and methods, the outcome of those cases is a counterintuitive fluke. If not for his ill-fated conversation with Adrian Lamo, Manning's high-tech leak would likely have gone unpunished. And if not for Nixon's flubbed attacks on Ellsberg, the older man might still be in prison even four decades later.

The barriers to modern megaleakers like Manning have crumbled: They needn't spend a year photocopying. They needn't be Eagle Scouts or war heroes who penetrate the government's most elite layer only to go rogue—just one of the millions of Americans with access to secret government documents or the many, many uncountable millions more with access to secret corporate information. And perhaps most important, they needn't risk reprisal by exposing their identities to the journalists they hope will amplify their whistleblowing.

The forces that caught Manning are real and significant: The greatest vulnerability for any leaker remains his or her human connections. But the lesson of Manning's story for a generation of digital natives will be, above all else, that *he nearly got away with it.* Use the right cryptographic tools, keep your mouth shut, and you, too, can anonymously, frictionlessly, eviscerate an entire institution's information.

There may not be many Daniel Ellbergs in the world, ready to push through the twentieth century's stubborn barriers to leaking. But the twenty-first century would be wise to expect more Bradley Mannings.

PART TWO

THE EVOLUTION OF LEAKING

"Insiders know where the bodies are."

JULIAN ASSANGE

CHAPTER 3

THE CYPHERPUNKS

The forty-first issue of the Melbourne University Mathematics and Statistics Society's quarterly magazine, *Paradox*, contains a short but telling anecdote about the society's most well-known former vice president.

One day during his three-year career as an undergraduate student of math and physics, Julian Assange was walking through Melbourne University's campus when he spotted a mysterious valve protruding from the University Chemistry Building's brick wall. He decided, spontaneously, to open it. When he did, the metal sphincter let out a deafening noise and a cloud of smoke. And for a few delightfully chaotic moments, as Assange told a fellow student later that day, the man who would advance the evolution of leaking more than anyone in the twenty-first century "was in heaven."

A lanky, six-foot-two-inch, very pale, white-haired thirty-two-year-old, Assange cut a strange figure among the tanned teens and twentysomethings at the University of Melbourne. He was known to work at his computer for days on end with no sleep and little food. He spent much of his time camped out in the university's Mathematics Society meeting room, usually wearing a dark gray trench coat over a T-shirt and his corn-silk hair in a

ponytail. Sometimes he would stand up from his computer and perform a set of twenty or so jumping jacks, explaining to anyone present that short bouts of physical activity served a certain neurobiological function that made stimulant drugs unnecessary.

He spoke rarely about his past, and few asked. He was often accompanied by an entourage of strangers whom he declined to introduce to anyone in the room. And he mysteriously refused to let the society put his photo on its website, citing "security" reasons and insisting that it be replaced with an image of an alien.

Assange no doubt felt like an extraterrestrial among the university's more traditional students. He described the academic physicists at one conference as "snivelling fearful conformists of woefully, woefully inferior character" and wrote that "for every Feynman or Lorentz, [there are] 100 pen-pushing wretches scratching each other's eyes out in academic committees or building better bombs for the DSTO (Defence Science & Technology Organisation), who had provided everyone with a bag, embossed with their logo, which most physicists pathetically lugged about with pride and ignorance."

At the time, as Assange later recounted to *The Age*, the Applied Maths program at the university had received funding from the U.S. Defense Advanced Research Projects Agency (known as DARPA). Assange believed (inaccurately, according to the department's staff) that money would ultimately go toward improving the design of the Grizzly Plow, a military bulldozer used in the first Iraq War and designed to sweep away barbed wire and sand at more than thirty-five miles per hour. The plow, as Assange described it, filled the trenches inhabited by enemy troops, rolling over them and burying them alive like an accelerated version of Tim May's father's bunker-burying bulldozer from World War II.

Assange was disgusted by what he saw as the military's influence on campus and bored by formal education. If his classmates had asked about his past, they would have realized how little he had in common with them: In his three decades, he had already gone toe-to-toe with major corporations and the Pentagon as one of the world's top pseudonymous hackers, been

convicted of digital felonies, wandered Australia as a homeless vagrant, traveled to dozens of countries, run a business on the early Internet, co-written a memoir, devised an innovative crypto-system, and, perhaps most significantly, received an education as valuable as any degree: nearly a decade of close reading, writing, and debate on the Cypherpunks Mailing List.

So, perhaps chiefly to entertain himself during his time in college, Assange invented a game: The Puzzle Hunt. Following a model invented by MIT for its venerable Mystery Hunt, the Puzzle Hunt was an elaborate campus-wide scavenger hunt punctuated with dozens of math and logic problems that drew in hundreds of students and still takes place annually on the University of Melbourne's campus.

One of the puzzles Assange generated for that competition—and he created more of them in his first year than any other student—involved a long quote from Shakespeare's *Julius Caesar,* with each letter written backward. Seemingly random gaps appeared throughout the chunk of text, and collecting the letters following those anomalies revealed a clue for the next puzzle. Another conundrum involved factoring large numbers into primes—a procedure that would have seemed natural for anyone familiar with RSA's public key encryption tricks.

Each set of puzzles in the hunt began with a quote. One, from the Koranic figure Ja'far as-Sadiq, captured Assange's playful love of obscurity: "Our cause is a secret within a secret, a secret that only another secret can explain; it is a secret about a secret that is veiled by a secret."

A year after Assange left the university—he's described quitting as a "forced move," as in chess, "when you have to do something or you'll lose the game"—he sent an e-mail to many of his former colleagues in the Melbourne University Math and Statistics Society asking for their participation in a new project as exciting and intellectually challenging as the Puzzle Hunt.

It was called WikiLeaks.

"Are you interested in being involved with a courageous project to reform every political system on earth—and through that reform move the world to a more humane state?" he wrote to his old classmates. "We have only 22 people trying to usher in the start of a world-wide movement. We don't have time to reply to most reporters' emails, let alone the interview requests—and I leave for Africa in under a week! We need help in every area, admining, coding, sys admining, legal research, analysis, writing, proofing, manning the phone, standing around looking pretty, even making tea."

A year later, he would write to his university math colleagues again, this time posing his project directly as an offshoot of the Puzzle Hunt's whimsical mind games.

> Hello Puzzle Hunters.
>
> I am looking for good people, courageous people, intelligent people to help develop and run an international leaked document analysis & essay competition.
>
> Wikileaks is only new, but we have already broken major stories in the international press that have achieved significant reforms likely to save tens of thousands of lives. Our problem? We're drowning in leaked documents.
>
> Across the world there are other notable analytical, mooting and essay competitions. Competition in most of these cases is what we might describe as 'mere competition'; the motivational elements extend to social and professional standing, competition camaraderie and the pleasure of discovery and creation, but together we can create a much more interesting competition; a competition where teams of bright people form an engine for justice, a competition where:
>
> 1. The basis is of real substance and interest in the form of never before released leaked documents of potentially significant political importance.
>
> 2. Discovery and creation are augmented by the nature of the material and its moral calling. These are real puzzles with real discoveries to be found.

3. In addition to traditional or academic honors, there is the ultimate honor: to have a positive impact on civilization through one's labours and for this to be internationally recognised.

Each team will receive a previously unanalyzed leaked document or series of leaked documents. . . . Proposed awards: over-all winner, lightning (24 hour), best analysis, best critical analysis, best news story. Where 'best' is defined as 'whose insights contribute most to humanity.'

"I think it would be fair to say that he saw Wikileaks, in some ways, at some times, as a political version of the Puzzle Hunt, with great social implications," Daniel Mathews, one of Assange's college friends and an early volunteer for WikiLeaks, would tell an editor of *Paradox*. Like the hackers and code rebels playing games of Crypto Anarchy with nested envelopes on Eric Hughes's living room floor, Assange approached WikiLeaks as a great game, an elaborate cypherpunk puzzle of leakers, friends, and adversaries playing by rules laid out in the landscape of cryptography.

But for all his talk of "an engine of justice" and "reforms likely to save tens of thousands of lives," the other goal in WikiLeaks' game—or perhaps just a bonus perk for a fire-starter like Assange—was its potential for explosive chaos. The rebellious young Australian felt the same yearning to outsmart and tear down the corrupt establishment as Tim May expressed in his earliest crypto-anarchist dreams.

Four years later, after the firestorms of Bradley Manning's alleged record-breaking, world-shaking releases, the science fiction writer Bruce Sterling wrote of WikiLeaks: "At last—at long last—the homemade nitroglycerin in the old cypherpunks blast shack has gone off."

The denizens of the Cypherpunk Mailing List drew the blueprints for that massive improvised explosive device, refining the recipe not just with theory but with years of trial and error, testing the limits of anonymity and antigovernment provocation. And it was Assange who watched the experiments, studiously mixed the chemicals from their notes, and then opened the fateful valve.

. ---- ... . -.-. ... .. -.-. -- ... .---- -.-. ---- -.. .. -

John Young knows something about how to stage a dramatic rendezvous. On an April afternoon, he's asked me to come to Carl Schurz Park on the Upper East Side of Manhattan and wait for him in front of Gracie Mansion. With the precision of his architectural training, he's sent me an aerial still from Google Maps that shows a semicircular bulge in the promenade where I'm to stand, overlooking the East River with a view of the Roosevelt Island lighthouse and the Robert F. Kennedy Bridge.

It's raining, and Young has not been as precise with time as he is with location. So I'm left alone in the eerily empty park, standing under an umbrella by the guardrail holding a briefcase and feeling like a character out of a John Grisham or Tom Clancy novel, which I imagine is exactly what Young had in mind.

Ten minutes later he walks out from behind a row of bushes, a stooped figure with his head down, wearing large black galoshes and holding a closed umbrella at his side while the rain pours down onto a limp fishing hat. He shakes my hand gravely, and as we walk out of the park I ask him why he doesn't carry a cell phone, which makes a useful tool for changing meeting locations from outdoors to indoors on rainy days. "Horrendous spying machines," he answers simply.

Young brightens as we reach East End Avenue. "How about we go find someplace warm and dry to talk," he says. Then, just as quickly, his eyes narrow and he gazes ruefully down the street. "This neighborhood is full of *shitty* restaurants."

Sitting in one of those shitty restaurants a few minutes later, Young lays down some ground rules: "You're interviewing me, but I'm interviewing you too," he says in a grumbled voice so low that I have to lean forward to hear him. "This interview goes both ways."

Fair enough, I agree. But a few questions in, it's clear that his idea of this bidirectional interview is significantly more adversarial than mine. "Where are you from originally?" I ask genially. Young pauses, and seems for a moment to be holding his breath.

"I take umbrage at that question. That is a stupid question, and it's the kind of question asked by stupid people," he says in the same whisper, so soft that I can't tell if he's inhumanly calm or holding back enormous anger. "And it shows me that you're not serious. So let me tell you that if you ask another question like that I will walk out that door."

I must appear so flabbergasted by this response that Young seems to feel the need to explain. "We need more friction in this interview."

Young's strange style of conversation shouldn't come as a surprise; it's no stranger than the equally conspiratorial tone of his singularly strange website, Cryptome.org. In his sixteen years of running Cryptome, Young has become a kind of paranoid twenty-first-century newspaperman, a collector of leaks, curios, raw data, and clues to mysteries that often only he and perhaps his less visible partner, Deborah Natsios, understand.

In the days before our meeting in Manhattan, for instance, Cryptome published archival footage of Hiroshima in the days after its bombing: dazed survivors walking around makeshift shelters and children collecting stones amid the rubble. Another post shows the immigration papers for Barack Obama Sr., perhaps a clue related to Obama's birthplace conspiracy theories. A third shows the finances for WikiLeaks over the year 2010, as collected by the German Wau Holland Foundation. Few of the half a dozen documents that Young and Natsios put online daily are accompanied by any analysis or even an explanation as to why the reclusive couple chose to publish them.

"My mentor, Jean-Paul Sartre, said that imagination is the only thing you can trust," says Young, after I've smoothed out some of our friction. "Facts are not a trustworthy source of knowledge. Cryptome is not an authoritative source. It's a source of imaginatory material. Don't trust Cryptome, we lie to you helplessly. Don't believe anything you see there."

But as much as John Young tries to give the impression that Cryptome is a schizoid lunatic's collage, it's nothing so simple. Since launching the site fifteen years ago, Young has published the names of 2,619 CIA sources, 276 British intelligence agents, 600 Japanese intelligence agents, and internal documents from every company from Microsoft to Cisco to AT&T

revealing their policies for secretly handing users' data over to law enforcement.

Many were leaked to Young by unknown sources. And despite threats, legal attacks, and even maneuvers by Microsoft to remove his site from the Internet in 2010 after he published what he calls the company's "spying guide," Young has never—with a few exceptions to protect private individuals—taken down a document.

The FBI first visited Young in 2003—he describes the pair of agents in typically precise fashion as having "trim haircuts and dark suits, healthy-looking young Caucasians, no facial hair, shined shoes, clean teeth, no noticeable mouth or body odor"—and offered a polite warning about "threats to the nation" that might result from Cryptome's postings of intelligence names and sources. Later, when he extended his repertoire to posting selections from databases of aerial photography, the Department of Homeland Security began calling him and politely asking him to stop. Young ignored all of them.

When Cryptome subsequently published detailed maps of Dick Cheney's secret bunker in March 2005, the site was featured in a *Reader's Digest* section called "That's Outrageous!" The article was titled "Let's Shut Them Down: These Sites Are an Invitation to Terrorists." The interviewer asked Young if there was anything he wouldn't publish—say, a security flaw in the president's Secret Service detail. "Well, I'm actually looking for that information right now," Young answered.

Four years later, when Yahoo! asked Young to unpublish a manual that showed how it complied with law enforcement requests for users' private information like search history and e-mail content, Young referred the company's lawyer to the same *Reader's Digest* story, which includes the words of former NSA counsel Stewart Baker. "If material is leaked to you, you can probably publish that," Baker is quoted saying. "Unfortunately, it's not illegal to be a jerk."

And how did Cryptome obtain those leaks? Not through any promises of high-tech security. The website includes an e-mail address along with a PGP public key. There's also a postal address, as well as a number to a telephone that no one answers.

The site's privacy policy, as far as it even has one, promises that Cryptome doesn't collect user data and deletes its logs several times a day. But its protections for the privacy of its leakers end there. The policy reads:

"As you know there are many, many ways to snoop on traffic, so much that Cryptome asserts there is no trustworthy privacy policy, not for Cryptome, not for anybody else. . . . Those who promise the most protection are out to skin you alive, those who promise the most privacy are selling your most private possessions. Cryptome is not trustworthy, and lies. It's a free site, what else could it be but up to no good?"

Young doesn't recommend that his secret-spillers use Anonymous remailers, like Tim May's BlackNet, or Tor, like WikiLeaks. Cryptome doesn't endorse any specific anonymity technologies, or make promises about safeguarding any identity information it does receive: The leaker's anonymity is wholly his or her own problem. "Do not identify yourself, jerk," says Young. "That's our policy. Don't send us stuff and think that we'll protect you."

But since the days of the cypherpunk remailers, tools for anonymous leaking have been in the hands of leakers, and the submissions have kept coming. When WikiLeaks launched in 2006, the site included a reference to John Young as the "spiritual godfather of online leaking." In fact, his influence is more than spiritual; in the earliest days of WikiLeaks, it was Young's name listed on the registration of the site's domain. And aside from Assange himself, he is perhaps the strongest tie that the secret-spilling site has to its ideological roots in the cypherpunks.

After our lunch, the rain has let up and I walk with Young to the Eighty-Sixth Street subway entrance. I start to thank him for meeting me and ask when we can talk again, so that I can hear the rest of his story. He answers with one final point of friction. "I'll talk to you. But until you publish something that puts you in prison, I won't fully respect you," he says, his face blank.

I tell him I'll do my best. Then we shake hands, and he walks away.

- ---.- - ... .--. -- --.. ---. .- --- -.. -- .--. ....

In 1988, as Julian Assange tells it, a sixteen-year-old version of himself sat in a quiet room of a temporary refuge house for families in the Australian

town of Emerald, on the eastern edge of Melbourne. He turned on the television news. Then he removed the cover from his Commodore MPS 801 printer and set it printing a long document, with its exposed mechanics emitting a noisy clacking rhythm. And then he started reading passages in *Macbeth* out loud from a Shakespeare anthology. Occasionally he would alter the pitch of his voice, ask himself random questions, pause, and answer them, all while periodically stomping around the room. To anyone watching, he would no doubt have appeared in need of antipsychotic medication.

Every epic hacker story has its Great Hack, when the teenage upstart first gains access to a powerful, faraway machine that opens up vast new possibilities. In 1983's *WarGames*, Matthew Broderick unwittingly hacks the WOPR supercomputer, a vast engine of nuclear war analysis. In 1995's *Hackers*, Angelina Jolie and Jonny Lee Miller breach the Gibson mainframe. And in *Underground*, the 1997 nonfiction book written by Julian Assange and Australian journalist Suelette Dreyfus that sketches the early Australian hacker subculture, that digital golden fleece was Minerva, a system of mainframes run by Australia's Overseas Telecommunications Commission in Sydney.

The protagonist of that story? A hacker named Mendax, who only years later Assange would reveal was none other than Assange himself, using the handle that defined his hacker persona for many of his teen years. The name referred to *splendide mendax*, the "nobly untruthful" in Horace's Odes.

Assange was determined to access Minerva, both for bragging rights and to exploit the mainframes' capabilities to run scanning and cracking programs for other netherworld adventures. But he needed a password. And the only way he knew to get one was through what hackers call "social engineering," simply calling up a human being and conning him or her into divulging secrets.

Hence the noisy layers of Shakespearean tragedy, television, and printer that the altogether sane young man was producing. Assange's sound show was for the benefit of his cassette recorder, the better to simulate the background chaos of a busy office. A few minutes later, he had found a valid number within an OTC branch office in Perth. And using his uncannily

deep sixteen-year-old's voice while the noise-tape played behind him, he became "John Keller," a trustworthy operator in the Sydney office trying to check a few data points corrupted by a crashed storage drive.

He dialed and a man picked up. Assange introduced himself and began the game. "The backup tape is two days old, so we want to check your information is up-to-date so your service is not interrupted," he casually told the man who answered the phone, not missing a beat.

"Oh, dear. Yes. Let's check it," Assange's mark responded in a concerned tone.

Assange read out a list of easily accessible information for Minerva staff users that he had downloaded, carefully inserting an error into one user's fax number. The voice on the other end interrupted him helpfully.

"Oh, no, that's wrong, our fax number is definitely wrong," he said.

So Assange tried to match his victim's worried tone and explained that they would need to confirm all the user's information. "Let's see. We have your account number, but we had better check your password . . . what was it?"

"Yes, it's L-U-R-C-H—full stop."

Lurch. Assange was in. He politely ended the conversation, gave his target a callback number that rang eternally busy, and hung up, victorious in the greatest hack of his young life.

Assange was born in Queensland, Australia, on July 3, 1971, less than one month after the first publication of the Pentagon Papers. From as early as he could remember, his family was on the move, as Assange's mother, a free-spirited costume and makeup artist, traveled with his bohemian stepfather from town to town. For a time they lived on Magnetic Island, a tropical paradise off the eastern coast of Australia where Assange's mother remembers "living in a bikini" and "going native." She wore a sarong and would trek around the island with Assange on her back, often leaving him to sleep in the shade of a boulder by the sea while she sketched. The young Australian was dazzled by the phosphorescent phytoplankton that emitted an aqua flash as the ocean's waves broke on the shore, and he swung from giant fig tree roots. His mother would slash a path to the front door with a machete and kept rifle cartridges for shooting snakes. On some occasions, opossums ran across their beds in the dark.

One evening, while the Assanges were out having dinner, their house mysteriously caught fire and burned to the ground, with their snake-shooting ammunition combusting like a series of firecrackers in the night. After losing most of their possessions, they lived with near-ascetic simplicity. "You didn't have to have a lot of money to live a privileged lifestyle," Assange's mother told the local news outlet, the *Magnetic Times*. "It was so beautiful . . . at night, when the ferries stopped, we felt cut off from the world and its troubles. There was a sense of safety and security."

Despite that idyllic setting, Assange made few friends in his "itinerant minstrel childhood," as he called it. "I was quick to anger and brutal statements such as 'You're a bunch of mindless apes out of *Lord of the Flies*' when faced with standover tactics were enough to ensure I got into a series of extreme fights," he wrote in 2006. "I wasn't sorry to leave when presented with the dental bills of my tormentors."

Assange's birth father, whom his mother met at an anti-Vietnam rally, was gone before he was a year old. His next father figure, an alcoholic, was divorced from his mother when he was nine. His second pseudo-stepfather, whom Assange's mother has described as a manipulative and abusive character, had fathered Assange's younger half-brother, and when Assange's mother left him, the man and a powerful cult to which he belonged searched persistently for Assange's family. They stayed on the move, now out of fear rather than the innocent wanderlust of Assange's earliest years. In all, Assange moved through fifteen different towns and at least as many schools, when he attended school at all.

Assange's distrust of power was inculcated just as early as his rootless wandering. He remembers his mother driving through an Adelaide suburb late one night, after leaving an antinuclear protest, giving a ride to a friend who held evidence that the British had forced five thousand natives from their land to test nuclear weapons in the Maralinga region of South Australia. When Assange's mother saw that she was being tailed by a car, she dropped off the friend in a back street and continued. The tail turned out

to be a plainclothes policeman who pulled over the car, searched Assange's mother, and made a thinly veiled threat that she "get out of politics" or risk being seen as an "unfit mother."

But just as formative as that dark political lesson was his first computer, a Commodore 64 that he used in a computer shop across the street from a house his mother rented. Seeing his interest and skill, his mother bought it for him, a sacrifice that required moving into a cheaper home. Assange began simple coding and cracking software protections, and soon he was hooked on what he described as "the austerity of one's interactions with a computer." "It is like chess," he told one reporter. "Chess is very austere, in that you don't have many rules, there is no randomness, and the problem is very hard."

Not long after his Minerva hack, Assange and two Australian friends whom he met on Usenet formed the International Subversives, and began publishing a zine of hacking techniques and tales. It had a rather limited circulation: to obtain a copy, a hacker had to write an article for it. Therefore its readership remained at three.

But the International Subversives was no mere geek clubhouse. The group developed into elite hackers, and Assange soon became by some accounts the most accomplished practitioner of digital intrusion in Australia, a near-mythic figure across the burgeoning hacker subculture. He writes in *Underground* of gaining access to networks ranging from Melbourne University to Nortel to NASA to Lockheed Martin and the Los Alamos National Laboratory, and, according to comments he later made in a Swedish documentary, installed a back door in the heart of the Pentagon's systems that allowed him and his friends to come and go as they pleased for two years. "For someone who was young and relatively removed from the rest of the world, to be able to enter the depths of the Pentagon's Eighth Command at the age of seventeen was a liberating experience," he once told the art historian Hans Ulrich Obrist.

Mendax's mission was never to steal or destroy, Assange says, only to explore, and he outlined his hacker's ethic in *Underground*: "Don't damage computer systems you break into (including crashing them); don't change the information in those systems (except for altering logs to cover your tracks); and share information."

One of the two other International Subversives, known as Trax, had found enough information in Telecom Australia garbage bins to learn to spoof calls, making them appear to come from a central exchange hub or even from another person's phone. Just as cypherpunk remailers would hide the origin of e-mail in years to come, Trax taught Assange to hide his location and identity by routing his modem's phone traffic through that intermediary.

An incredibly methodical hacker, Assange didn't depend only on that redirection but also erased all logs, and generally avoided any behavior that would remotely raise suspicion. Still, there were slipups. On one occasion, he accidentally rang a thousand phones simultaneously in a Telecom Australia office building at seven A.M. And finally, on another occasion, he was caught in his tracks by a system administrator trolling the networks late one evening. The admin turned out to be so determined to catch the intruder on his network that he drove in to a Melbourne office from the suburbs in the middle of the night to gain higher network privileges.

When it became clear that he couldn't continue the cat-and-mouse game any longer, Assange sent his pursuer a note that appeared in the center of his screen, one that momentarily shocked him into inaction.

> I have finally become sentient.
> I have taken control.
> For years, I have been struggling in this greyness. But now I have finally seen the light.

Assange knew that the surprise value of a suddenly intelligent machine wouldn't last. So he pleaded for understanding.

> It's been nice playing with your system.
> We didn't do any damage and we even improved a few things. Please don't call the Australian Federal Police.

And then he logged off before the call trace could begin.

Assange left his mother's home at the age of seventeen and moved in with a girl whom he later married, and the young couple soon had a son. As he tells it, he also kept a beehive, endlessly delighting in studying the insects' society in all its complexity. To avoid their stings, he writes that he would collect his sweat in paper tissues and dissolve it into a sugar water solution that he fed the bees as nectar. The trick was meant to associate his odor with the bee-friendly taste of flowers, a clever biological hack.

But the hive also served another purpose. Assange used it as a hiding place for the floppy disks that stored his hacker's booty, data like stolen passwords and logins, and records of the open pathways and security vulnerabilities he had mapped out across the Internet. After every hacking session, he carefully secreted them away among his beloved bees.

With one exception. In October 1991, just as the Crypto Wars were beginning in the United States, his wife of three years left him, taking their young son with her. Assange was emotionally destroyed. He moped around the house for days in fits, and fell into a state of careless lethargy.

When the Australian Federal Police finally knocked on his door one night soon after and showed him a search warrant on suspicion of computer crimes, all of his incriminating disks were strewn across his desk, with one in his PC's disk drive.

Mendax's career was over.

.... --- .. .. --.. -.-- --- -.. .... --- --. -.-. .- --- -.-- .---

It was the fourth day of the Columbia University Occupation of 1968, and the one hundred radical young men and women who had seized Avery Hall were pissed. Not simply angry that their school had obliterated a huge, tree-covered patch of land in a public park to build a new gym, with its back door facing their Harlem neighbors in a reincarnation of Jim Crow. Or even about the hellish, unjust Vietnam War and the fact that their own university had been shown in newly revealed documents to be secretly tied to the military's Institute for Defense Analyses.

No, the architecture students in Avery Hall were frustrated because the student body's protest, a full-blown strike that had taken control of most of

the major buildings on campus, wasn't working. The administration showed no sympathy to their pacifist and progressive demands, and wasn't willing to bargain. Most of the Columbia faculty had refused to stand with them, choosing instead to mediate between the students and the administration. And they could sense that a police crackdown was coming. The mood was tense in Avery and sheer pessimism was threatening to crumble the students' control of the building.

Then John Young spoke up. A thirty-two-year-old widower and graduate student, Young had been so quiet in the activists' meetings until that point that some students had suspected him of being a police spy. But one of those present described the short speech he gave that night as having an easing and profound effect on the group, his Texas-tinged grumbling coming out as "a cross between a mutter and the Oracle of Delphi."

Young began by congratulating his fellow students on having created a true anarchist democracy within the walls of Avery. And then he urged the group to stop moping and push forward with its work, to reach out to the outside world to make their demands heard, and to use its architectural training to build a fairer and more democratic city.

Finally, he told everyone to quit arguing and sulking, and get to work. It was a simple statement, over in five minutes. But it had its intended effect. Thanks to Young's prophetic mumbling, as the historian Richard Rosenkranz wrote in his chronicle of the Columbia protests, "the Avery Commune was once again a functioning organism."

In the end, the Columbia protests did end in violence, with students pulled out of buildings by police who brutally beat them with blackjacks, flashlights, and batons, cracking ribs and splitting scalps.

But the Avery occupation would set Young on a course toward radical, progressive libertarianism for the next forty-odd years. "I knew it was more than a student demonstration and that something extraordinary was going on," he said a few years later. "In a few days, we had sped up our lives, approached a condition of human relationships that can usually be found only in the realm of ideas."

Young had grown up in a poor family, the son of a wandering jack-of-all-

trades, traveling around Texas with his father and occasionally to Oklahoma or New Mexico, to find jobs washing dishes, painting, canning, picking cotton, and driving trucks. He described his father's philosophy as "antiorganization, antigovernment, basically antiauthoritarianism, very pro letting the people do it for themselves." But he bristles at the idea that his bottom-rung background drove him toward radicalism. "It would be easy for you to say, 'That poor man from that disadvantaged childhood. He's just striking back because he was denied,'" Young told Columbia protest chronicler Rosenkranz. "Well, that's bullshit. I didn't suffer from being denied, and I think my childhood was just great."

At seventeen, Young shipped out to Germany with the army and spent the next three years as an engineering supply clerk in "a vast storage depot, waiting for the next war." When he returned to the United States, the GI Bill paid for a bachelor's degree at Rice, and he double-majored in architecture and philosophy, mixing Sartre with the knack for building that he'd inherited from his father. After college he worked as a construction engineer, renovating the nineteenth-century Winedale Inn for the unfortunately named grand dame of Texas, Ima Hogg. ("She cracked jokes about her name. You did not.")

The work was meant to match the pre-Civil War–era building, and Young and his workmen scoured the woods for local materials like cedar, oak, and stone. "I learned the idea of being passive in the face of a building, rather than aggressive," he says. "You let the building tell you what to do, rather than tell it what to do."

That approach to architecture wasn't en vogue among the modernist architects at Columbia, where Young enrolled in a master of science program. But the 1968 occupation was his real education. After the strike, the students formed Urban Deadline, a nonprofit that aimed to bring the sensibility of the 1968 protests to architecture, education, and politics. It had no leaders. "Even anarchism was too organized for us," says Young.

As a part of Urban Deadline's architecture group, Young renovated storefronts to turn them into sidewalk schools, an alternative to the "prison-like" school system offered to kids in poor parts of Harlem and Brooklyn.

The group fought to create historic districts and derailed the construction of highways through poor neighborhoods. And Young functioned as the city's architectural gadfly. He once took out an ad in *The New York Times* attacking one of the world's most famous architects. "I. M. Pei," it read: "Why so many bad buildings?" When Young was invited to speak at the Museum of Modern Art, he deadpanned, "I've just had a chance to look around briefly, but if you move that Rubens and the Rembrandt and store them down in the basement, we could put thirty-two units of housing in here. We're prepared to start right now."

In the meantime, Young supported his work with a for-profit architectural firm. But even there, Young says his focus was often to report wrongdoing: corner-cutting and incompetence that led to unsafe buildings. On multiple occasions, he was hired for renovations, and instead pointed out violations like blocked exits, cracked supports, fire-prone ducts meant for air-conditioning but used instead for exhaust. When he was ignored, he reported the owners, losing clients and future work. Young says he considered that watchdogging nothing more than an architect's job. The city's regulatory commission usually ignored his complaints. "Buildings are more dangerous than guns. But real estate is such a powerful interest in New York that no one wants to hear it," he says. "The owners browbeat you into submission. They're willing to fucking ruin you, so they usually win."

It would be another two decades until Young rediscovered the same spirit of excitement, activism, and uncompromising antiauthoritarianism that had swept him up in 1968. He found it, finally, in the cypherpunks.

Assange's friends hadn't been as careful as he had. The third member of the International Subversives, a hacker who went by the handle Prime Suspect, couldn't use Trax's untraceable calling method due to a difference in the telephone exchange connected to his home. And as *Underground* tells it, he had been tracked on Nortel's network on the same fateful night that the network administrator had played cat and mouse with Assange. Prime Suspect breached its firewall during the thin window of time

between when Assange had escaped but before he could call his fellow hackers to warn them that he had tipped off the telecom's security.

In the end, it didn't matter. Trax himself had called up the cops and—almost accidentally—turned himself in. The teen hacker had long been unstable, agoraphobic, and unfit for the immense pressure of illegal hacking. When he called up the police to report a death threat against him by another hacker, he found himself inexplicably confessing his own activities. And soon those of his friends.

The Australian justice system took nearly three years to bring charges against Assange, and two more before he was sentenced. The judge, in the end, was lenient, recognizing that Mendax had never intended to profit from his hacks, only to idealistically seek a world without limits on information. He was sentenced to a two-thousand-dollar fine and a five-thousand-dollar bond depending on his good behavior.

But during the intervening five years, the possibility of impending jail time meant Assange never felt safe taking a real job or making long-term plans. He fell into a deep depression, first checking himself into a mental hospital and then checking out to spend six months on an aimless walkabout, sleeping in the wilderness around Melbourne, frequently waking with his face covered by mosquito bites.

Eventually Assange returned to the city to try and reengage with the world. He created a computer security firm with Trax, but it fell apart when their lead investor faced credit problems. And he began volunteering for nonprofit organizations, lending his computer expertise. He even worked with police in the city of Victoria, helping them to track and take down child pornography rings in two separate cases. But he drew the line at helping to catch his fellow hackers. "I couldn't ethically justify that," he's quoted as saying in *Underground*. "But as for others, such as people who prey on children or corporate spies, I am not concerned about using my skills there."

Assange took a job as systems administrator at an Australian Internet service provider (ISP) called Suburbia that hosted online chats on everything

from cryptography to religion. In some ways, he later told me, Suburbia was the prototype for WikiLeaks more than any other project he worked on.

Assange says some discussion rooms on Suburbia became forums for discussions among lawyers and activists claiming corrupt practices by the Australian telecom giant Telstra. But Suburbia also hosted discussions about a topic that would become the ground zero battle for free speech in years to come: Scientology. One of the notoriously censorious religion's critics had been sued under copyright claims and had his computers seized after posting documents on the service. The leaked documents, previously only available to members of the religion who had achieved a certain expensive stature, showed that Scientologists believed in communication with plants.

When the ensuing outrage spilled over to Suburbia, American lawyers contacted Assange to question him about one of his customers who had been an outspoken critic, David Gerard. Assange, of course, refused and instead alerted Gerard. "He had titanium balls," Gerard would tell me years later.

"We were the free-speech ISP in Australia," says Assange. "People were fleeing from ISPs that would fold under legal threats, even from a cult in the U.S. That's something I saw early on, without realizing it: potentiating people to reveal their information, creating a conduit. Without having any other robust publisher in the market, people came to us."

Even as he settled into a new life beyond hacking, Assange's charges hung over him like a bitter cloud. Years later, he would compare the feeling, hyperbolically, to Russian dissident writer Alexander Solzhenitsyn's imprisonment in Stalin's gulags. "How close the parallels to my own adventures!" he wrote in a rather self-pitying 2006 blog entry. "Such prosecution in youth is a defining peak experience. To know the state for what it really is! . . . True belief only begins with a jackboot at the door."

For an information freedom advocate like Assange, the plight of Phil Zimmermann in the United States, who, like Assange, had the threat of prosecution for seemingly harmless digital crimes hang over him for three years, must have felt especially familiar. It's little wonder that he fell in with Zimmermann's most hard-core supporters, the crew who happened to

also be radical hackers and antiauthoritarian misfits like himself. Assange became a cypherpunk.

He began posting to the mail list under the nickname "Proff" in 1995. His earliest writings, like most of the conversations on the list, were snarky takedowns of fellow posters' ideas. In his third message he calls one demanding user a "dummy" and tells him to "get a life." He tells another that "some research is in order before you go shooting off your mouth," and then makes fun of a third for hosting a party that ends at ten P.M., calling it an "afterschool Tupperware get-together." Apropos of nothing, he posts a list of National Security Agency anagrams in another message, including "Your testical [sic], again Nancy?" and "National Gay Secrecy Unit."

But "Proff" was no mere cynic or jokester. He would eventually use the list to organize a Melbourne protest against Scientology in retaliation for its attempt to censor Suburbia. "To the Church the battle isn't won in the court room," he posted in his anti-Scientology manifesto. "It is won at the very moment the legal process starts unfolding, creating fear and expense in those the Church opposes. Their worst critic at the moment is not a person, or an organisation but a medium—the Internet. The Internet is, by its very nature a censorship free zone." He then called on all good cypherpunks to come make their voices heard at the Melbourne Church of Scientology building at eleven A.M. the next day. Eleven people showed up.

But more important, perhaps, than what Assange wrote on the Cypherpunk Mailing List was what he and his cohorts read. For the decade that it was active, the list chronicled the long and painful evolution of the cryptographic anonymity that Assange would later harness under WikiLeaks. And that anonymity began, in its most newborn and vulnerable form, with a Finn named Julf.

In 1992, Johan "Julf" Helsingius, a cofounder of Finland's biggest Internet service provider, had witnessed a strange conversation on a Usenet forum hosted on an academic server. Two users were arguing, and one had taken the pseudonym Jesus. The other, a pretentious academic type, was not amused by this use of a humorous handle, and tried to argue that it

was "against the rules" of the Internet to hide one's identity on a university server, and downright offensive to hide it with a disrespectful nickname.

Coming from the growing nonacademic side of the Net, the notion that one professorial user would try to declare the rules for online identity deeply riled Helsingius. As part of the Swedish-speaking minority group in Finland, Helsingius had a special concern for protecting the rights of marginalized groups and the vulnerable, and felt that anonymity was an important safeguard for those groups. So he set out to prove that technology, not pretensions, would define the nature of identity on the Internet.

The result was Penet, an anonymous remailer server that ran off a humble PC with a 386 processor in a back room of Julf's home. Users could send Penet an e-mail along with a designated final destination—in his explanation posted to the Cypherpunk Mailing List, he cites Usenet groups devoted to erotic needlework and masturbation as examples—and the message would be relayed on to those endpoints with a newly generated pseudonym. Penet would keep a database of those pseudonyms and the e-mail addresses linked to them, so that if anyone wanted to reply to that handle, it would route back through the server and find the original sender.

Penet used none of David Chaum's crypto innovations, and Helsingius listed so many possible security vulnerabilities in his introduction to the service that it's a wonder anyone used it at all. He warned that users would have to trust him as the server's administrator, that he might be subpoenaed to give up someone's identity, and even that hackers could break in and steal the data. "It wasn't the best, the safest, or the most secure, but it was easy," says Helsingius. "That's how I pitched it, and it seems that's what people wanted."

Soon thousands of users—and eventually hundreds of thousands—were routing their secrets through Penet, enough traffic that Helsingius was paying more than ten thousand dollars a month in bandwidth. "I could have bought some expensive golf clubs instead, I suppose. But no hobbies are free, and this was something I believed in," Helsingius says.

For much of the early nineties, Penet became the best-known anonymity

service in the world, channeling discussions ranging from sexual abuse to homosexuality to religious freedom to whistleblowing, along with a load of spam, insults, and flame wars. And Helsingius became a cypherpunk regular, the Nordic king of the remailers.

And then in 1995, Helsingius received an e-mail very much like the one that was sent to Assange at Suburbia. It was from the Scientologists.

The lawyer of the Religious Technology Center, which held the copyright on Scientology founder L. Ron Hubbard's work, was requesting that Helsingius block all messages from Penet to the Usenet group on Scientology, which contained equal parts followers and critics of the movement, on the grounds that Penet users were posting copyrighted Scientology materials to the forum. Helsingius refused, of course.

A month later, he got a call. It was the Scientologists again, and this time they told him they had reported a burglary to the L.A. police and the FBI. Their copyrighted material, they argued, had been stolen via Helsingius's data laundering service by one user with the Penet pseudonym "an144108." Six days later, the Finnish police arrived with a warrant.

Helsingius fought the legal battle for more than a year. But Finnish law wasn't ready for the Internet. A postman was legally protected from having to reveal the secrets of the letters he delivered. But a virtual carrier like Helsingius still had no shield from legal orders that require he snitch on his clients. And when it became clear that he could either do just that or go to jail, Helsingius caved. He told the Helsinki court that an144108 was linked to an alumni account at Caltech. And as the Scientologists moved on to harassing Caltech's administrators for the user's name, Helsingius decided to shut down the service. Penet had gone from a symbol of freedom of speech to a honey trap for exposing exactly the people he had hoped to protect. "When the Church of Scientology won, I knew that would have opened the floodgates for anyone to try the same attack," he says. "So I pulled the plug."

Penet had stuck a toe in the water of the Anonymous Internet, and it had come back a bloody stump. Did Assange, who no doubt followed the issue on the Cypherpunk Mailing List, learn something from the saga of

Julf? "I'm sure he got a few ideas," Helsingius says cheerfully, "About exactly how not to do things."

--. -. .. - -... ... .---- -.-. .. -.. .- . .-- -.. ....- -...

> At the Village Pizza shop, as they were sitting down to consume a pepperoni, Dorothy asked Jim, "So what other inventions are you working on?" Jim replied, "I've got a new idea . . . Literally REVOLUTIONARY." "Okay, Jim, which government are you planning to overthrow?," she asked, playing along.
>
> "All of them," answered Jim.

So begins a passage in an essay by James Dalton Bell, a ten-part, sixteen-thousand-word screed that hit the Cypherpunk Mailing List in 1997 like a provocateur's glove slap across the face. It was called "Assassination Politics." And like Tim May's BlackNet, it would mix cypherpunk raw materials into an elaborate, imaginary engine that would agitate the list's conversation for years.

Unlike May, however, Bell wasn't just rehearsing a thought experiment. He hoped—and in fact, still believes—that his system would someday be implemented. Nor was "Assassination Politics" an idea that confined its intended effects to mere bits. As its name implied, it was a kind of cypherpunk political institution. And it was engineered for murder.

Assassination Politics' active ingredient was anonymity. And the cypherpunk drive for untraceable digital pseudonyms had hardly ended with Julf Helsingius and the demise of Penet. In fact, long before the Finnish server's shutdown, remailers had been evolving well beyond the simple name-for-nym swapping system that Helsingius had implemented. Instead, they had started to look more and more like the Mix Network idea outlined by David Chaum more than a decade earlier, and emulated on the floor of Eric Hughes's house with slips of paper and envelopes at the first cypherpunks meeting: multiple remailers sending messages inside nested layers of encryption to prevent anyone from knowing the identities of the sender and recipient, not even the remailers themselves.

After Eric Hughes's first stab at a cypherpunk remailer, others had soon improved on his weekend's worth of Perl coding. Hal Finney, a former video game developer who had worked on pieces of PGP, designed a version of the remailer that would integrate Zimmermann's encryption software. Now a message's destination could be encrypted with a remailer's public key. That was the first step toward Chaum's ideal: No one snooping on the sender's network could see the message's final destination. And Finney's system allowed remailers to be chained together, so that a message could be encrypted with many layers of public keys and slowly unpeeled by one remailer after another until it reached its destination. With a long enough chain of remailers, none of them would be able to connect the endpoint to the source.

Cypherpunks, as Eric Hughes had declared, wrote code: Creating was always more admired within the group than theorizing. But it was Lance Cottrell, a Ph.D. student in astrophysics at the University of California, San Diego, who actually took the time to go back to David Chaum's papers and read how a Mix Network was supposed to work. Chaum had imagined facing off against an adversary no less resourceful than the cunning NSA, so he had thought many moves ahead: If a spy could see enough of the network, for instance, Chaum realized that the spook could watch both ends of a correspondence and recognize a message going in one end and then coming out the other a few moments later. Based on the timing, those messages could be spotted as one and the same.

Worse yet, using multiple layers of encryption to route the message through multiple remailers could make a clever snoop's job easier by revealing clues about how many hops remained until the message reached its destination. If a message was wrapped in multiple layers of encryption, it would get substantially larger. And every remailer that stripped away a layer of encryption and sent the message on to its next destination would shrink it down again, providing more accidental hints to anyone trying to trace the source and destination.

So Cottrell finally built in the solutions that Chaum's genius had long ago prescribed. His remailer program, which he called Mixmaster, delayed

the transmission of messages until it had a certain number in reserve, and then sent them out in batches to fool any timing-based attacks. If a remailer didn't receive enough messages to mix them up and disguise their timing, it would even generate fake ones to surround and disguise the real one.

To prevent the trick of counting messages' apparent layers of encryption to predict how many hops until their destination, Mixmaster also relayed messages in packets of exactly the same size. If a message ended up too small after some layers of encryption were removed by the first remailers in the chain, the program padded it with junk data; too big, and it split the message up into equal chunks.

The cypherpunks appreciated the rigor of Cottrell's work, and Mixmaster was a hit. Soon it was running on around two thousand Unix machines around the world, pumping a flow of tens of thousands of anonymous e-mails a day, as close an approximation to Chaum's ideal Mix Network as ever existed.

Meanwhile, anonymous financial transactions were starting to feel like a reality too. Chaum's own company, called DigiCash, had implemented many of the ideas he outlined in his *Communications of the ACM* article. The result was eCash, a crypto-currency that would allow buyers to wire money untraceably to a seller. In the mid-nineties, DigiCash botched a series of deals and replaced Chaum with a new CEO before going bankrupt in 1998. But despite its lack of business success, no one doubted that Chaum's anonymous transactions technology worked—it had even been integrated into a Dutch toll road system that could reliably charge drivers without recording any trace of their identities.

Jim Bell, an engineer and chemist with a round face and large glasses, understood the power of Chaum's tools. He had once worked alongside Tim May at Intel, building early solid-state hard drives long before either of them had developed their interest in cryptography. Like May, he was a libertarian to his core. And for both men, in their own ways, the advent of anonymous messaging and anonymous payments represented not just the possibility, but the inevitability of crypto-anarchy. Bell's path to that end was just a bit bloodier.

Assassination Politics' plan was simple enough: Anyone could place a

"bet" with a central organization that some specific person would die at a certain time, date, and place. Gamblers would submit their encrypted guesses by e-mail, scrubbed of identifying information by anonymous remailers and linked with a payment of untraceable digital cash. When a person died, anyone could send in the key to decrypt his or her prediction, and if it turned out that the bet had nailed the exact snuff-time of a certain person, the sender collected all the digital cash on the deceased person's head via another untraceable transfer. It would be an encrypted, anonymous, digital dead pool.

Of course, Bell implied with a wink and a nudge, no one could possibly know the date, time, and place of a certain well-known person's death better than the one who caused it. And with a large enough pile of untraceable money riding on someone's head, there would be little doubt that professional killers would get in on the game.

Suddenly, Bell imagined, the minority of Americans with strong anti-government leanings would gain incredible power. "If only 0.1% of the population, or one person in a thousand, was willing to pay $1 to see some government slimeball dead, that would be, in effect, a $250,000 bounty on his head," Bell wrote.

> Further, imagine that anyone considering collecting that bounty could do so with the mathematical certainty that he could not be identified, and could collect the reward without meeting, or even talking to, anybody who could later identify him. Perfect anonymity, perfect secrecy, and perfect security. And that, combined with the ease and security with which these contributions could be collected, would make being an abusive government employee an extremely risky proposition. Chances are good that nobody above the level of county commissioner would even risk staying in office.
>
> Just how would this change politics in America? It would take far less time to answer, "What would remain the same?" No longer would we be electing people who will turn around and tax us to death, regulate us to death, or for that matter send hired thugs to kill us when we oppose their wishes.
>
> No military?

Bell described global crypto-anarchy in rosy terms: Sure, there would be no government to protect American borders or punish crime. But the military would be unnecessary in a world where no foreign government would be able to form a military, either, and all aggressive dictators would be immediately eliminated by crypto-funded assassins. "Consider how history might have changed if we'd been able to 'bump off' Lenin, Stalin, Hitler, Mussolini, Tojo, Kim Il Sung, Ho Chi Minh, Ayatollah Khomeini, Saddam Hussein, Moammar Khadafi and various others," Bell wrote. As for fighting crime, he explained, citizens could pool together money to put out anonymous hits on criminals just as easily as politicians.

"Assassination Politics" inflamed the Cypherpunk Mailing List almost as much as the defunct Clipper Chip had. "You gleefully propose to let us all in on the immoral game of murdering those who annoy us sufficiently," wrote one user through an anonymous remailer. "I'll pass."

"Others won't," Bell responded simply.

When one cypherpunk implied that Bell was a loony extremist who thought the government was out to get him, Bell corrected him: "I . . . am out to 'get' the government."

Another scolded Bell that "by resorting to violence you are no better than the ones you purport to protect us against." Bell answered that "Assassination Politics" was only responding in kind to a violation of his own rights. And he shot back the most withering possible question in a mail list populated by libertarians: "Are you a statist?"

As for cypherpunk founding father Tim May, he never criticized Bell's morals, only his methods. May, after all, was the one who had called for a "thermonuclear cauterization" of Washington, D.C., in one essay. But why bother with the silly cover story of "predictions," May thought, when anonymity tools could allow the whole assassination market to function in the open? He had predicted online "liquidation markets" ("You slay, we pay")

in the e-mail that followed his BlackNet experiment more than three years earlier.

More important, May felt, Bell lacked discretion. Even attaching his own name to "Assassination Politics" made Bell and everyone associated with him a target for the feds. "He wasn't paranoid enough in distancing himself from the project," says May. "I just stayed away from it. If I got an e-mail from Bell, I dropped it, unanswered. I didn't think he was an original thinker, and I didn't want to get involved with his lame-ass idea."

Phil Zimmermann, who had always considered the cypherpunks too radical and provocative, felt perhaps the strongest aversion of all to Bell's murderous blueprint. "He was so full of violence and anger," Zimmermann says with disgust. At one point Bell wrote to Zimmermann to ask what the inventor of PGP thought of his ideas. "I wrote him back and said that he had managed to do what no one in the U.S. government could ever do: He had made me wonder whether I never should have worked on encryption in the first place."

- .... . -.-. --- -.. - -.-- ... .. -.-- .--- ... ... -.--

John Young's eyes almost seem to mist at the thought of the cypherpunks' heyday. "My beloved cypherpunks," he says with a faraway look. "They were disputatious. Endlessly disputatious. You make a point and someone immediately attacks you unfairly, cruelly, mercilessly.

"Weakling, phony, bullshitter! Everywhere they saw authority, they attacked it."

Young and his wife, Deborah Natsios, had discovered the Internet in 1993 and marveled at the massive river of information it represented. They signed up for practically every mail list and Usenet group they could find. "We felt that we had been living in the doldrums, and suddenly we were on the cutting edge," he says.

In June 1994, he discovered the cypherpunks when Tim May, John Gilmore, Eric Hughes, and Phil Zimmermann were featured in a *New York Times* magazine story that quoted chunks of both May's "Crypto-Anarchist Manifesto" and Hughes's "Cypherpunk's Manifesto." For Young, their

cause sounded like a struggle for freedom and power as idealistic and critical as the occupation of Avery Hall had been two and a half decades before.

A fifty-seven-year-old architect among graduate students and young neorich Silicon Valley types, he didn't try to insert himself into the mail list's fierce technical debates. Instead, Young became a kind of obsessive cypherpunks news service, transcribing, scanning, summarizing, and posting articles to the list daily.

And there was plenty of news: Phil Zimmermann's battle to stay out of prison, the encroaching Clipper Chip, not to mention the rise of the World Wide Web and the security issues it introduced. Two years into his cypherpunk tenure, Young created Cryptome.org, a Web based version of the service with prolific news updates and postings. Today it might be called a blog, though the term *Weblog* wouldn't be coined for another year.

Cryptome, as its name implied, was meant to be a repository for crypto-focused materials from any source where Young could grab them. One of its first posts was a publicly available 1985 paper by the Dutch researcher Wim van Eck introducing a method of reading the electromagnetic fields around computing equipment to surreptitiously pick up the data it displayed from a distance, even through walls. With the right equipment, van Eck wrote, it would be possible to snoop on someone's computer screen in a seemingly private location from a distance of more than a kilometer. Every PC with a monitor, in other words, constantly leaked data in all directions.

Worse yet, the dreaded NSA had developed a technique, code-named TEMPEST, to read those signals. Cryptome published everything Young could find about TEMPEST, and it became a leitmotif among the paranoid cypherpunks. At one point in 1996, both Assange and Bell joined in a heated discussion of whether even the water pipes and sprinkler system around a computer might propagate its electric field and spill its data even further.

Soon after "Assassination Politics" hit the list, Young would post that essay, which he still calls a "masterful piece of fiction," to Cryptome. And amid the online shouting match that surrounded the article, it was Young who first took Bell seriously.

"It's hard to tell the difference between 'Assassination Politics' and government-sponsored provocateurism, a well-documented practice to stigmatize anarchical and antiauthoritarian ventures," he wrote. "However, it takes guts and thick skin to advocate overthrow of authority, knowing that reasonable people will think you're a nut seeking celebrity martyrdom."

"Well, it's not like I'm SEEKING martyrdom," Bell responded. "But the possibilities have certainly crossed my mind. Some people have suggested, and only partially in jest, that I may be one of the system's first victims."

In fact, Bell achieved martyrdom through a more common fate. In April 1997, his home was raided by federal agents who seized his computers, his car, three assault rifles, and a .44 Magnum handgun. It turned out Bell had pursued his agenda against the feds through more direct avenues than mere essays. In the criminal complaint filed against him, he was accused of evading taxes, falsifying his social security number, and intimidating federal agents, with "Assassination Politics" as Exhibit A. Agents dug up e-mails in which he had discussed buying the ingredients for the poison ricin, and other messages suggested he was planning to drop nickel-plated carbon fiber down the air shafts of a federal building. Bell believed that the material, which agents found in large quantities at a friend's house, would become airborne, find its way into the building's computers, and short out their wiring.

Finally, he was accused of dumping a chemical called mercaptan on the rug outside an IRS office in Vancouver, Washington. The stink bomb smelled like very potent rotten cabbage.

Despite his various stunts, Bell was charged only with tax evasion and sentenced to eleven months in prison. He was out again by the next summer, but rearrested for violating his probation. Prison darkened his outlook even further. "I once believed it's too bad that there are a lot of people who work for government who are hardworking and honest people who will get hit [because of "Assassination Politics"] and it's a shame," he told *Wired* after being released in 2000. "Well, I don't believe that anymore. They are all either crooks or they tolerate crooks or they are aware of crooks among their numbers."

Eventually he would be tried again for stalking federal agents across

state lines and sentenced to another decade in prison, where he spent his days demolishing computer monitors for forty-six cents an hour.

For some cypherpunks, Bell came to represent the first real victim of the Crypto Wars, and Cryptome became a resource for those following the case: It documented every step of Bell's legal ordeals more closely than any newspaper. Young collected media clippings, court documents, even anonymized messages from friends who had received word from Bell during his time in prison. He became so closely involved in the case that in Bell's first trial Young was subpoenaed as a witness, and argued on the stand that Bell had never intended to carry out any of his antigovernment plans so much as trumpet them around the Net.

In 1998, the committee for the Chrysler Award for Innovation in Design contacted Young to ask him, based on his architecture work, to nominate candidates for their annual award. Naturally, he submitted Jim Bell for "Assassination Politics," a groundbreaking work in "government accountability systems."

--- -... -.. ....-. -.-- -.- -.- ... --. .-- -. .- --.

Julian Assange continued to throw occasional jabs and quips into the mail list's discussions of everything from the NSA's TEMPEST project to "Assassination Politics" well into the late nineties. When Bell was sentenced to his first prison term and a copycat wrote up a new flavor of his murder-for-hire project aimed at celebrities, Assange posted it with the subject "Jim Bell . . . lives . . . on . . . in . . . Hollywood!"

Contributing to the melee of controversial ideas offered some light amusement for a wayward ex-con crypto-savant. But cypherpunks write code. And Julian Assange was a cypherpunk.

The story of Julf Helsingius and the Scientologists had sharply illustrated the human vulnerabilities in any encryption scheme. No matter how strong crypto may be or how cleverly the key is hidden, the cypherpunks had learned a user threatened with jail or bodily harm will cough up the goods. Cryptographers, with typical dark humor, call the method Rubber Hose Cryptanalysis: Rather than try to break an encryption scheme, simply

imprison the user and beat the key out of him or her with a length of heavy tubing.

So a year after Helsingius broke under the pressure of a Finnish warrant, Assange posted a newly coded creation to another cypherpunk-friendly mail list, designed to outsmart rubber hose bullies. He called it Marutukku, after an Akkadian deity of protection, though he and his cocreators, a fellow researcher named Ralf-Philipp Weinmann and coauthor of *Underground* Suelette Dreyfus, would soon rename it, simply, "Rubberhose."

Like Zimmermann's PGP, Rubberhose was designed for activists in repressive regimes to smuggle out controversial data. But where a captured rebel activist with a laptop hard drive encrypted with PGP might be vulnerable to torturous key extraction, Rubberhose offered a clever solution. The keyholder would have multiple secret keys, each of which would appear to decrypt the entire hard drive. But the program could hide volumes of the drive like a false bottom of a box. (In fact, the effect works by spreading each encrypted portion of the data evenly over the entire hard drive to give the appearance that one volume fills the entire capacity, with no room for more secrets.)

When the torturer pulls out the rubber hose, the user simply pretends to give in, handing over a key that decrypts a volume full of decoy data. Thanks to Rubberhose's unique properties, the torturer should believe he's seen the full contents of the drive and grudgingly release the activist.

The program included an antiauthoritarian mission statement: "Entrenched moguls . . . label the activists as trouble-makers or whistle blowers to justify misusing them," it read. "Where there is injustice, we like to upset the status quo too, and to support others who want to do the same. Our motto is 'let's make a little trouble.'"

But there was a darker side to Rubberhose, one that reveals something about Assange's style of cold calculation. Say the torturers know that the user encrypted the hard drive with Rubberhose. Then there's little she (Assange, in cryptographers' fashion, calls her Alice) can do to prove that she's given up all the keys. With the understanding that her torturers will beat her endlessly regardless of what she does, Alice has little incentive to

give up information that incriminates her comrades to save herself. Like a cyanide capsule hidden in a spy's tooth, Rubberhose actually motivates users to sacrifice themselves rather than give up their friends' information. As Assange wrote:

> With Rubberhose-style deniable cryptography, the benefits to a group member from choosing tactic 1 (defection) are subdued, because they will never be able to convince their interrogators that they have defected. Rational individuals that are "otherwise loyal" to the group, will realise the minimal gains to be made in choosing defection and choose tactic 2 (loyalty), instead.

Or as he put it more simply in the Rubberhose documentation: "Alice certainly isn't in for a very nice time of it. (Although she's far more likely to protect her data.)"

Despite Rubberhose's cleverness, Assange wasn't content to create mere tools. But it would take him another decade to evolve from the creation of his own equivalent of PGP to his own equivalent of BlackNet. He spent two years traveling the world, shaking off the anger and frustration of his years in legal limbo. In 1999, he registered Leaks.org in a moment of foresight, but had no clear idea of what to do with it and left it fallow for years longer.

When Assange returned to the Cypherpunk Mailing List after his travels, he seemed to have taken on a new political radicalism. The list's popularity was waning and it was choked with spam. In his second-to-last message he posted the following, which seems almost a rebuttal to Tim May's libertarian dismissal of the "clueless 95%." "The 95% of the population which comprise the flock have never been my target, and neither should they be yours," he wrote. "It's the 2.5 percent at either end of the normal that I find in my sights, one to be cherished and the other to be destroyed."

That same liberal radicalism drove him to give up on formal education at military-tinged Melbourne University. And finally it pushed him to write the essay that would become his own "Crypto-Anarchist Manifesto." Fresh from the influence of university, he typed it up in the font and style of an

academic math paper and posted it to his blog with the name "Conspiracy as Governance."

The paper described authoritarian regimes as collections of nodes connected by lines of communication that depend on technology for their survival: Internet, phones, fax machines. And the key to toppling those structures was to cut those data-lines, Assange wrote.

> When we look at an authoritarian conspiracy as a whole, we see a system of interacting organs, a beast with arteries and veins whose blood may be thickened and slowed until it falls, stupefied; unable to sufficiently comprehend and control the forces in its environment.
>
> Later we will see how new technology and insights into the psychological motivations of conspirators can give us practical methods for preventing or reducing important communication between authoritarian conspirators, foment strong resistance to authoritarian planning and create powerful incentives for more humane forms of governance.

In fact, "later" never came. The essay gave no explanation of how technology could be used for cutting those communication lines. But it did say, in what seems to be a jab at Jim Bell, that killing conspiratorial leaders wasn't the answer. "The act of assassination—the targeting of visible individuals, is the result of mental inclinations honed for the pre-literate societies in which our species evolved," Assange wrote.

Later that month in his blog, Assange would write the solution to the puzzle of "Conspiracy as Governance," like an answer key at the back of a textbook. The solution was leaks.

> The more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning coterie. This must result in minimization of efficient internal communications mechanisms (an increase in cognitive "secrecy tax") and consequent system-wide cognitive decline resulting in decreased ability to hold onto power as the environment demands adaption.

Leaks had a twofold purpose in Assange's view: They empowered the regime's enemies with damning facts. But more important, they induced the regime to stop communicating internally, a kind of calcification of its circulatory system more deadly than any outside enemy. "Hence in a world where leaking is easy, secretive or unjust systems are nonlinearly hit relative to open, just systems," Assange wrote.

Which leaves one final, unspoken question: how to make leaks happen? That's a puzzle Assange had worked out years before, hiding the answer in his introduction to the pseudo-autobiographical *Underground*.

He quotes Oscar Wilde: "Man is least himself when he talks in his own person. Give him a mask and he'll tell you the truth."

While Assange theorized about leaks, Young was busy springing them.

After years of merely digging up public documents and reposting news, the anonymous tips began to flow. In May 1999, an anonymous e-mail referred Young to an article, already pulled from the Web at the time of the e-mail, in an issue of *Executive Intelligence Review*, which listed 116 names of MI6 officials sent to the newsweekly, along with locations and dates showing their movements across the globe. Young posted the file to Cryptome and it was downloaded tens of thousands of times within days.

The next year, Young received a UK MI5 report from an anonymous source, detailing the surveillance of a Libyan diplomat in London that British intelligence suspected of being a spy. The paper accused the diplomat of being involved in the murder of a UK-based Libyan dissident. It was marked "TOP SECRET DELICATE SOURCE UK EYES." Young published it in its entirety.

A few months later, Young published a list of six hundred Japanese intelligence agents who were being sent abroad after the failure of Japan's Public Security Investigation Agency to gather sufficient intelligence to

shut down the Aum Shinrikyo cult that carried out a sarin gas attack on the Tokyo subway, killing thirteen people. The list was titled "The Most Incompetent Intelligence Agency in the World." Young received the list anonymously at first, but the source, a PSIA agent named Hironari Noda, revealed his identity within days.

The Japanese leak was followed by a list of 2,619 CIA informants from an anonymous sender. Young posted the names alphabetically with every source's address. Within a week the leaker outed himself as the journalist Gregory Douglas, who had been given a trove of files by an ex-CIA agent to be published at his death.

Young's next scoop came from old-fashioned investigative reporting. He filed a Freedom of Information Act request to the NSA that it release all nonclassified data on TEMPEST, the electromagnetic spying trick that allowed intelligence agents to read screens through walls. The NSA first denied his request but gave in on appeal. He published hundreds of pages of detailed descriptions of the mechanisms behind the NSA's epic hack. Much of it was painstakingly transcribed into HTML from the paper documents.

By 2006, Young had received two more leaks outing MI6 agents and was publishing controversial images of secure government facilities on a regular basis. He had gotten the attention of the three letter agencies: NSA programs crawled his website daily to monitor his material, and he'd received visits from the FBI and calls from DHS officials.

At some point, he also got the attention of Julian Assange. The PGP-encrypted e-mail hit Young's in-box in early October 2006: "You knew me under another name from cypherpunk days. I am involved in a project that you may have feeling for. I will not mention its name yet in case you feel you are not able to be involved.

"The project is a mass document leaking project that requires someone with backbone to hold the .org domain registration. We would like that person to be someone who is not privy to the location of the master servers which are otherwise obscured by technical means.

". . . Will you be that person?"

Young agreed, and two months later he found himself subscribed to an

internal mailing list for developers on Assange's secretive project. Every e-mail on the list began with the message: "This is a restricted internal development mailinglist for w-i-k-i-l-e-a-k-s-.-o-r-g. Please do not mention that word directly in these discussions; refer instead to 'WL.'"

The list argued over everything from the logo for the site—originally a mole breaking through a wall in front of a phalanx of dark bureaucratic figures—to potential funding sources and figureheads. The group approached Chinese-American dissident professor Xiao Qiang, Ben Laurie, a cryptographer who had developed an open-source version of the SSL protocol for encrypting Web traffic, and perhaps most significantly Daniel Ellsberg, the leaker upon whom all their greatest hopes were modeled.

"We have come to the conclusion that fomenting a world wide movement of mass leaking is the most cost effective political intervention available to us," read the group's e-mail inviting Ellsberg to join their advisory board. "New technology and cryptographic ideas permit us to not only encourage document leaking, but to facilitate it directly on a mass scale. We intend to place a new star in the political firmament of man."

Ellsberg never responded to that message. But the e-mail to the archetypal twentieth-century leaker crystallized everything Assange had learned from the cypherpunks: WikiLeaks would share all of David Chaum's, Tim May's and Phil Zimmermann's beliefs in the power of cryptography to effect political change. It had all the ambitious complexity of "Assassination Politics," with its illegality and violence carefully excised. And it had learned from Cryptome's model of soliciting and anonymizing leaks as a self-propelled weapon against authority.

John Young's tenure as a WikiLeaks adviser was short. Just two weeks after Young joined the mail list, Assange suggested attempting to raise five million dollars from sources like the Soros Foundation. Like my innocuous question about Young's childhood when we met in an Upper East Side restaurant, the notion seemed to flip a switch in Young's unpredictable mind.

The Cryptome founder responded with a series of increasingly angry and sarcastic e-mails, sent too fast to even allow responses from the other WikiLeakers. "The CIA would be the most likely $5M funder. Soros is

suspected of being a conduit for black money to dissident groups racketeering for such payola," he wrote bitterly, suggesting that WikiLeaks attempt to raise a hundred million dollars from the CIA instead.

"Fuck your cute hustle and disinformation campaign against legitimate dissent. Same old shit, working for the enemy," Young added, vowing to leak the entire mail list on Cryptome—which he soon did. He signed off, "In solidarity with fuck em all."

Assange responded shortly thereafter. "J., We are going to fuck them all."

Then he unsubscribed John Young from the list.

. ---- -. --- -- ---. .... -.-. .... -.-- --- -.. ---- ...

In February 2011, I e-mailed a request to a Sheridan, Oregon, detention facility to speak with Jim Bell, who was serving the last years of the same sentence for a parole violation that had put him in prison earlier in the decade.

The month after my e-mail, I received a seven-page letter from Bell, single-spaced, written on a typewriter, and virtually free of typos. The letter was focused on two points: First, that Bell had been the subject of a fraudulent show trial, and that he wanted me to request that *Forbes*'s internal counsel help him prove that the Ninth Circuit Court had forged records of an entire appeals case that ruled against him without his knowledge or participation.

Second, Bell wrote that while in the Special Housing Unit, also known as the "hole," in 2009, he had made a "truly phenomenal discovery in the areas of Chemistry, Physics, and Material Science, of total value well in excess of $100 Billion." (The underlining is his.)

Although he didn't remember Assange's comments on the Cypherpunk Mailing List, he expressed his admiration for WikiLeaks, and wrote that after being released from prison and becoming enormously wealthy in the following six months to one year, he planned to donate somewhere between a hundred thousand and a million dollars to the group.

In later letters he would explain that he had invented a new form of fiber optic cable that would transmit data 33 percent faster than conventional fiber optics, and planned to obtain five thousand patents after he was released, five times more than Thomas Edison. "It will affect virtually every science, every field of engineering, thousands or even tens of thousands of products," he wrote. "You will find this hard, even impossible to believe, yet it is quite true."

Bell was right: I didn't believe him. But I did approach *Forbes*'s counsel to ask her assistance in pursuing Bell's legal case. She read Bell's letter, then checked his legal file, which showed that he had fired practically every court-appointed lawyer ever assigned to him—little wonder that he had botched his appeals. It also showed he had filed fifty-one lawsuits against the government while in prison—nearly all dismissed immediately. She wanted nothing to do with it.

I wrote back to Bell apologizing that I couldn't offer legal help, and asking whether he still planned to pursue "Assassination Politics" when he was released.

He mailed back an even longer letter, mostly chastising me for failing to help him expose the government's fraud and accusing me of being in the pocket of the authorities. "Wake up! Wake up! Wake up!" he wrote. "You need to tell your editorial counsel that I have given you a very specific example of a crime the government committed against me. . . . If he isn't fully behind assisting you in exposing this crime, then he must be part of the problem."

And then he wrote about "Assassination Politics."

> Unfortunately, you reveal a little of your biases by saying, "Do you still hope/plan . . ." Implying I did so, etc. Nope! At the time I wrote AP, I presumed that I wouldn't be the one to implement it, and that is, indeed, WHY I publicized the idea with my own name.

Bell went on to write, however, that he would soon be a "hero of scientific and technological progress," and that his "inventions and technologies will usher in a boom unlike the world has ever seen. I've already probably solved the 'energy crisis' a dozen times over." As the world realized the bril-

liance of his inventions, "thousands of people" would reassess his ideas, including "Assassination Politics." If no one else were to implement the contract killer system, it would be easy enough for him to do it himself, he wrote.

> It would be as simple as directing a work-group, or (more likely) forming a new division in my set of corporations. The AP system is sufficiently similar to [the] insurance or gambling industry, and a dozen lawyers or two will ensure that it stays within the laws of the region it is sited at.
>
> . . . [T]he government (and those employed by it) should defend their continued existence (life) in the face of what they have done to America's finances.
>
> Interesting benchmark: The French Revolution in [1794] resulted in the guillotining of about 19,000 persons, of a total population in France of 25 million people. Adjusted for a population of America of about 300 million, that would be about 230,000 persons. Do you really believe that those in the [U.S. government] would have run up that $14 trillion debt (actually a lot more, depending on the kind of analysis) if they knew that at some point in the near future, 230,000 of their kind would be killed?

As this book went to press, Jim Bell was scheduled for release from prison on March 12, 2012.

CHAPTER 4

THE ONION ROUTERS

Jacob Appelbaum drops a black, hard plastic container the size of a small suitcase on the conference table in a sterile-chic conference room in MIT's Media Lab, a six-story structure of sleek white walls and glass that resembles a giant iPod. Twenty or so motley hackers sitting around the table and lounging in the corners of the room suddenly look up from their laptops. Appelbaum cracks the box open to show off a large chunk of white, ruggedized hardware encased in foam. The group admires it in hushed tones, slowly drawing closer.

The twenty-seven-year-old stands in the center of the room, six feet tall, with neatly parted black hair, Italian glasses, and tattoos that run up his left arm. His T-shirt is a baseball jersey with the word KINSEY written across the back and the number three, a reference to his position on the Kinsey Institute's sexual persuasion scale. (Zero indicates heterosexual, six homosexual.) "This," he says, chewing a piece of raspberry chocolate with studied nonchalance, "is what I've been working on."

Until that moment in the Tor Hackfest, things had been getting dangerously technical. Tor is one of the world's most widely used and perhaps most secure anonymity programs. And Nick Mathewson, Tor's grinning, round-faced, ponytailed chief architect and codirector, had kicked off the

day by dropping the room into the deep end of the cryptographic swimming pool. The geekery had gotten so thick that even some of Tor's modern-day cypherpunks and volunteer coders, loath as they might have been to admit it, might just have gotten lost. Within minutes, Mathewson, wearing a sport jacket over a Tor T-shirt over a dwarfish potbelly, was delving into security issues like "epistemic attacks" and "Byzantine fault tolerances." By the time he sat down, still grinning, a growing fraction of the room seemed baffled or possibly bored.

Appelbaum's presence, on the other hand, is as much guerrilla as geek. He's Tor's field researcher, unofficial revolutionary, and man on the ground in countries from Qatar to Brazil. And he knows the appeal of a sexy piece of hardware. After instantly acquiring the room's attention, Appelbaum explains that the device his small audience is ogling is a satellite modem, one that he's just rented with the aim of figuring out how to make Tor accessible to those in the Middle East who need to use satellite connections to access the Internet.

The project is not theoretical. For the prior three weeks, an entire civilization has been turning itself upside down. The wave of revolts that overthrew the government of Tunisia and ousted President Hosni Mubarak from Egypt has just spilled into massive protests in Morocco, Libya, and Bahrain. And while the rest of the world has been lauding the power of Twitter and Facebook to organize and catalyze those movements, the digerati in this room know that the protesters' connection to the Internet has a more sinister side. Unless they use anonymity tools like Tor, every dissident who plugs into those online services can have his or her information perpetually monitored by governments that don't hesitate to knock down doors and haul away political enemies on a whim. Hence Appelbaum's latest science experiment: He aims to shield the identities of dissidents and journalists who use satellite connections to get online even when the government has locked down, throttled, and surveilled their bandwidth.

But there's a problem, Appelbaum says. Tor hides a user's IP address, but a satellite modem's communication protocols reveal its location to the satellite provider. "Even if you use Tor, someone can still find all the users in a

given country," Appelbaum cautions. "That means you need to connect to the network and then drive fifty kilometers, or you get the cruise missile."

"If you need GPS spoofing, my people in Zurich can help with that," offers one clean-cut researcher with expertise in hacking pacemakers and cardiac defibrillators.

"OK," Appelbaum says in an unimpressed tone that implies spoofing GPS is about as difficult as microwaving a burrito.

The gaggle of hackers pepper him with questions about the modem's specs and the company he rented it from. "I gave them your information, Mike," he says, turning to another Tor programmer with a mock-sheepish smile. "Sorry."

No one needs to ask why Appelbaum wouldn't hand out his own personal data. Even among Tor's security-conscious crowd, Appelbaum is an exemplar of privacy paranoia in its purest form. And lately, for good reason. Because aside from his day job as a programmer and evangelist for Tor, Appelbaum moonlights as a freelance Internet freedom fighter, one that many governments, including America's, might like to see disappear.

Just the night before the MIT gathering, for instance, the young hacker was probing the digital infrastructure of Libya, where the military was busy firing live ammunition at defenseless crowds that included women and children. Muammar Qaddafi's dictatorship had shut down most of the Internet, leaving only its military and government connections online. So Appelbaum used a tool he created called BlockFinder to list which branches of the country's networks remained online and broadcast their IP addresses to any and all hacker allies. "Systems that are online in Libya are probably worth scanning; those are the systems required or used by the current government oppressors," he wrote on Twitter. He suggested digging into one connection in Palermo, Italy, that connected North Africa with the Internet at large, what he identified as "the Arab dictator's favorite uplink."

"Now is the time for all good black hats to come to the aid of humanity," he added, throwing in a riff off a line from the film *Full Metal Jacket*: "I wanted to visit exotic Libya . . . I wanted to meet interesting and stimulating people of an ancient culture . . . and own them."

"Black hats," of course, are hackers who engage in usually illegal tactics

of intrusive or destructive hacking. And to "own" a target is hacker jargon for penetrating or taking control of its systems. As in a message Appelbaum had posted just a few hours earlier: "Shooting unarmed protesters in the head? Bahrain's government has demonstrated that they are over the line. It's ethical to own them."

During the protests in Egypt a few weeks earlier, Appelbaum had put out another call for help in tracking down President Hosni Mubarak to prevent him from fleeing the country in the midst of the revolution there. "I'm looking for Mubarak or his handlers' cell phone numbers—if you've got them, I'll track them," he wrote.

"Mubarak is trying really hard to not end up like Nicolae Ceauşescu," he added, referencing the Romanian dictator who was executed by a firing squad after a two-hour trial during the country's 1989 revolution. "Good luck with that, you son of a bitch!"

Appelbaum later explains to me that a technique known as an HLR query can approximate a user's location on a carrier's network. Did he ever successfully use that trick to pin down Mubarak's location? The young hacker smiles and changes the subject.

But organizing penetrations of Libyan Internet infrastructure and tracking dictators' cell phones, as legally questionable as those feats may be, aren't the most pressing reason for the young hacktivist's privacy obsession. Appelbaum has ties to WikiLeaks. Not simply as a nameless volunteer, but as one of its most die-hard supporters and its most prominent American face. In late 2010, Julian Assange told *Rolling Stone* that "Tor's importance to WikiLeaks cannot be understated" and that "Jake has been a tireless promoter behind the scenes of our cause." In late 2010, when Assange seemed to be on the brink of long-term jail awaiting questioning for alleged sex crimes, one WikiLeaks staffer told me he hoped Appelbaum might even be the favored successor to Assange in WikiLeaks' hierarchy.

None of which is news to the U.S. government. Several months earlier, Twitter revealed that the company had been directed by the Department of Justice to hand over Appelbaum's data, along with that of two others associated with Julian Assange's secret-spilling group, likely part of a larger dragnet to

build a conspiracy charge against WikiLeaks staffers. Since then, the threat of an indictment that could put Appelbaum in prison for a significant portion of the rest of his life has been hanging just a few inches above his neck.

Even here at the MIT Hackfest, that threat makes its presence felt rather awkwardly when, as Appelbaum tells it, he runs into a State Department official later in the day, a clean-shaven man dressed in a gray fleece. Appelbaum greets him politely. "You probably want to shoot me in the head," he says with a wary grin.

"We have other people who do that," the official says, also smiling.

Neither of them seems quite sure whether this is a joke.

.... .-.. .. ... -- .--. - -- .... .-.. --- ....-.. ... .--.

At least twice now in the evolution of leaking, it was the U.S. government, specifically the U.S. military, and even more specifically the Defense Advanced Research Projects Agency, or DARPA, that built the machine that would ultimately hemorrhage the government's secrets.

DARPA, after all, created the prototype for the Internet, that massive secret-siphoning neural network. And along with the State Department and the Naval Research Laboratory, DARPA would also build and fund Tor, the tool that WikiLeaks would use to effect the largest-ever public data breaches against the military and the State Department, exactly the institutions that created it.

Stranger yet is that even after Tor was allegedly used by Bradley Manning and potentially many others to anonymously leak massive troves of highly secret U.S. government documents, government agencies haven't withdrawn their support for the tool any more than they've withdrawn from the Internet. Because just as government agents can't survive without the Internet's information-sharing powers, they also sometimes need the ability to be completely anonymous online. Not simply private, but strongly, cryptographically anonymous.

Tor offers that cryptographic anonymity to its users with the same principles as David Chaum's Mix Network, but stripped down and built to function at Web speed. Like a Mix, the software doesn't necessarily prevent anyone

from seeing what a Web user is writing or reading. Instead, it's designed to prevent anyone from knowing who is doing the writing or the reading. That's because if a CIA informant in Iran is visiting the agency's website to drop a tip, the government spying on the informant's connection doesn't need to know what information he's passing on: Even if the data he shares is encrypted, just the knowledge that he was talking to American spooks is likely to earn him a knock on the door from the country's secret police.

The State Department funds Tor to communicate with political dissidents from Iran to Myanmar and to help them access the unfettered Web, a key element in Secretary of State Hillary Clinton's mission of so-called "Internet Freedom." The U.S. military uses Tor for open-source intelligence, gleaning foreign policy or military strategy from other countries' websites without tipping them off to a spook's presence. Corporations use Tor to facilitate industrial espionage or, in some cases, prevent it. One example offered by Tor's executive director Andrew Lewman: IBM hosts a copy of the U.S. Patent and Trademark Office database. If someone at Hewlett-Packard wants to browse sensor designs in that database without tipping off its biggest competitor, it had better use a thick cloak of anonymity.

But Tor can also work in reverse: A website implementing a Tor feature called a Hidden Service can mask its location and allow users to find it in the Web's ether without anyone knowing where the site is physically hosted. To access a Tor Hidden Service, the user has to run Tor, too, so both the visitor's physical location and that of the site are completely masked. Neither reveals anything other than the information they're sharing, like two trench-coated men handing off a briefcase in a dark parking structure.

And like any setting where packages are exchanged in the shadows, crime has found its way in too. It's no secret that Tor is used by child pornographers and black hat hackers. Seconds after installing the program a user can untraceably access sites like Silk Road, an online bazaar for hard drugs and weapons, or one of several sites that claim to offer untraceable contract killings. But Tor is also used by the FBI to infiltrate those lawbreakers' ranks without being detected, and for cybersecurity researchers to test websites without tipping them off that they're being patrolled by

McAfee or Symantec. "When I'm speaking to a law enforcement crowd and someone complains that Tor is used for crime, I find an agent who uses Tor every day for fighting crime, and I try to get those two to talk to each other," says Tor's director, Roger Dingledine.

Technically, Tor faces the same tricky paradox Chaum aimed to solve in 1981: Location equals identity. If someone can locate your computer, they know where you live or work, which is a trivial step from knowing who you are. So Tor needs to accomplish the Internet's main task—mapping out connections between people so that data can travel to and fro as quickly as possible—without letting anyone in the system know where those two ends lie.

Like its users, Tor operates in a state of functional paranoia. It assumes that its network of messengers is littered with traitorous spies, and no single node can be trusted. So taking a cue from Chaum's original Mix idea, the data is triple-encrypted. No one node can figure out the entire route. Each node unscrambles one of those three layers, as if each of the series of messengers removes one opaque skin from an onion to find the address of their next contact written on the surface underneath. Hence Tor's name, an abbreviation for "The Onion Router."

Since Tor employs the uniquely targeted scrambling of public key encryption, each layer of onion skin is wrapped in a way that can be unwrapped only by the next node. All the messengers have keys to a layer of the onion, but they can only open the layers specifically addressed to them. So that first node in the chain might see that an Iranian informant wants to visit a website, but it can only open the layer of encryption that tells it to pass the rest of the onion on to a node in Cupertino. Even if Iran's secret police control that relay, they'll never know that the data jumped from California on to Berlin and finally to the CIA website in Langley, Virginia.

But is Tor secure enough to stymie the CIA itself, along with its brainier cousin, the NSA? The typical answer to that question is one I hear from Chris Soghoian, a Soros Foundation fellow who lives in Washington, D.C., and spends his days fighting for stronger privacy and anonymity regulations. "I have you got a better alternative?"

Tor, as Soghoian and most other security researchers will tell you, is not secure. For those who have watched the world of cryptography long enough, nothing is. Every crypto-system has hidden weaknesses that another cleverer cryptographer will ferret out. And almost any scheme can be cracked with enough time and computing power. But "Tor has been torn apart and banged on for years," says Soghoian. "Every year flaws are found and fixed. Because of that, it's better than the rest. It's the only solidly peer-reviewed anonymity system for real-time communications."

In fact, Tor has been shown to be vulnerable to a slew of brilliant attacks, most found by Tor staffers themselves. One, for instance, involves a website feeding the user a sequence of data that can be recognized coming out the other side of the network to match up a user with his online activities. Another uses flaws in common file-sharing programs to reveal the IP addresses of the programs' users and then extrapolate the addresses of others. A third depends on the temperature of the servers: Hotter computers run faster, and an attacker can start to recognize and analyze Tor Hidden Services based on fingerprinting those timing differences.

Whether those attacks could be performed at scale to identify a leaker remains an open question. If anyone could perform massive cryptographic and signals intelligence feats on large networks, it would be the NSA. For now, there's no known real-world case of Tor being broken to identify a user. (All signs still indicate, for instance, that it was Adrian Lamo, not the NSA, that ultimately fingered Bradley Manning, the Tor user federal agencies would have liked to have identified more than practically any other.) Even many of those who are most skeptical of Tor's security suggest that users seeking absolute anonymity should still use the tool along with other, commercial proxy services to create extra layers of defense.

But it can't be denied that Tor has a fundamental flaw, and one that is also its greatest strength: Any agency or individual can set up a Tor node on a computer. By subtly starting up hundreds or thousands of nodes around the world, the U.S. government might be able to get access to a large enough fraction of the comings and goings of Tor users to map out their communications and find their endpoints. To do so, of course, would

mean ingeniously disguising the nodes and competing with every other government that seeks to track the network, many of whom might not be keen on sharing their intelligence.

In fact, Tor's community-built properties are fundamental to its functioning. They were, in some ways, the seed that germinated from an idea deep inside the military's institutional mind into the public Tor Project as it exists today. And if onion routing's inventors hadn't needed to share the technology beyond the walls of the Pentagon to make that volunteer system work, it might never have become a software Frankenstein's monster, directing mayhem directly back at the agencies that created it.

. ...- . -.. .-. --- -.- . .---. -- .... - .---- .... -.- .---.

When Paul Syverson, the researcher known by many today as the "father of onion routing," arrived at the Naval Research Laboratory in 1989, most of his degrees were in philosophical logic, not mathematics or computer science. As an undergraduate bumping up for the first time against ideas from epistemic logic—a field that seeks to rigorously answer formalized questions about what can be known—he pored over the puzzle books of Raymond Smullyan, the eccentric writer, pianist, and magic performer. (Smullyan once dazzled the audience on Johnny Carson's *Tonight Show* with questions like this one: Say you have three opaque containers of coins, one full of nickels, one of dimes, one of both types of coin mixed together. All three have been mislabeled with one of the others' names. How many coins do you have to pull at random from each jar to properly rearrange the labels? The surprise answer: just one coin from the container labeled "mixed." Late night television audiences were clearly more entertained by epistemic logic puzzles in 1982 than they would be today.)

Smullyan would later sit on Syverson's dissertation committee at the University of Indiana, and often wandered into the young graduate student's office to pull cards out of Syverson's ears or rehearse logical scenarios with the younger researcher. Smullyan's books permutated ever-more-complex versions of a type captured by a well-known riddle, the one about asking directions from two men, one who always tells the truth and one who always

lies. His increasingly tangled conundrums were populated by vampires who always lie, humans who always tell the truth, insane humans who think they're telling the truth but lie, insane vampires who think they lie but actually tell the truth, and some in-between actors whose truth-telling is utterly unpredictable.

So it's fitting that when Syverson approached the problem in 1995 of how to route the Web's information anonymously, his solution would depend on tolerating many thousands of untrustworthy characters.

Syverson, with fellow NRL researchers David Goldschlag and Michael Reed, was determined to build a Mix Network for the Web. But they faced the same challenge that inspired Lance Cottrell's Mixmaster e-mail anonymity program: Clever spies can correlate messages going in and going out of a network based on timing. "The bad guy watches three bytes go in and three bytes come out," says Syverson. "When the data is moving in real time, it's an analysis that's easy to perform, and hard to defeat." Lance Cottrell had solved that problem in Mixmaster by designing the program to collect individual messages for hours or even days, the better to obscure their timing. On the Web, where users hardly tolerate a second's delay, that approach would fall flat.

So the researchers suggested a less-than-elegant fix: a network so big, with data going into and coming out of thousands of nodes, that matching up the head and tail of every connection in real time becomes a matter of finding two ends of a needle in a haystack full of bits of needles. "If your adversary is in a position to watch both ends of the communication, he wins," says Syverson. "But if the adversary can't see those ends, he doesn't even know where to start looking."

And the most practical way to expand the network? Invite everyone to join it. The NRL team imagined a volunteer network run by a diverse crowd of hosts, each controlling its own piece of the mix of relay nodes. In that populist system, no user can trust every node. But every user can be relatively sure that no single host—not even the system's creator, the navy—is watching the entire network and tracing users' paths. (Today Tor

has more than three thousand nodes, each receiving and sending off data packets in unpredictable paths, and Tor's organizers hope to someday broaden the network of relays to tens or even hundreds of thousands more.)

To work, that volunteer mix didn't just need to be big. It needed to be diverse. Lots of unlikely bedfellows hosting nodes—everyone from the U.S. intelligence agencies to cypherpunks—attract a motley network of users. And without a diverse set of users, an anonymity network is hardly anonymous; if only the navy used Tor, it wouldn't take much Smullyanian logic to figure that anyone using Tor would be part of the navy. For Tor to offer meaningful anonymity, the military had to set it free, to be both maintained and used by everyone from hackers to revolutionaries to criminals to G-men.

In that sense, even though Tor was first created behind government walls, there could never be the sort of debate over the public distribution of the strong anonymity tool that took place over the public access to strong encryption in the 1990s. Even if the government had sensed that the software it was funding for masking users' identities was a dangerous weapon, it couldn't keep that program to itself. To be effective, Tor had to be shared with everyone—even those who would use it against the very institutions that created it.

The Naval Research Lab's idea of recruiting a volunteer network wasn't Tor's cleverest trick—just a formalization of what Mix Networks had already been doing since the early cypherpunk days. But to work at Web speed, Tor also needed a new, faster way to route data at Web velocity through its three-stop circuit. Chaum's original idea used public key encryption to scramble the data it sent from one node to the next, a process that took as much as a thousand times too long for real-time traffic.

So the NRL team suggested a shortcut. Old-fashioned symmetric key encryption, where the same key is used to encrypt and decrypt data on both ends, is far faster than the public key encryption invented by MIT's cryptographers in 1977. But symmetric key encryption is less secure, in that the keys have to travel to their destination and might be eavesdropped.

If, however, those symmetric keys are themselves encrypted with public

key encryption and only decrypted once they reach the nodes in the network, they can be securely set in place, well guarded and ready to decrypt data far faster than public key encryption keys.

In Syverson's system, each node would use slow, secure, public key encryption to generate public keys for encrypting and private keys for decrypting. Then the user's software would triple-encrypt the first parcel of data with the public keys of three randomly selected nodes in far-flung places around the globe, just like any Mix Network. But the first message sent along that triple-bounce path wouldn't be any real communication from the user. It would simply hold three more keys, of the old-fashioned symmetric key encryption sort. Only once those new, speedy private keys were placed safely in the three nodes around the globe, laying out a path to their destination, would the user start sending packets of real content bundled in three layers of symmetric key encryption that the relays could peel off, one after another, at blinding Web speed. (In fact, Tor today repeats that entire preparatory process every ten minutes, repeatedly laying down new paths with public key encryption to offer one more safeguard against surveillance.)

Syverson coined the term *onion routing* because the first data package to travel across the network was less like a triple-wrapped rock with a hard center of information than an onion, with nothing but layers all the way down. It would be a carefully wrapped envelope with no message inside. The crucial data held by that envelope, like the sweetness of a Georgia Vidalia, was in the skin itself.

Even with the navy's innovations, Tor was still just an idea. But it bounced around Syverson's brain for years like so many triple-encrypted data packets, well after Goldschlag and Reed had moved on to other research topics. So when Syverson received a grant from DARPA to revive the project in 2001, he needed help: The father of onion routing, despite his logical prowess, had never quite learned to code.

Syverson had met Roger Dingledine a year before at the Privacy Enhancing Technologies conference in Berkeley, where the recent MIT

graduate was presenting his own digital-freedom-focused brainchild, a project Dingledine called Free Haven. Dingledine, a ponytailed and apple-cheeked savant with strangely unblinking eyes and a robotically logical manner of speaking, explained that Free Haven would function as a distributed, uncensorable publishing system. He pointed to examples like the property records that had been destroyed in the Kosovo refugee crisis in the late nineties: Kosovars displaced by Serbian attacks returned to their land to find that no one had any formal proof of who owned what. "Someone didn't want those records around," says Dingledine. "If Free Haven had existed, there might have been an archive of that data. And it wouldn't have been vulnerable to political, social, or corporate pressure."

Dingledine's project, outlined in his master's thesis at MIT, depended on distributing information among many anonymous volunteer publishers and constantly grading how reliably each node served up data. To Syverson, it sounded like a project near to Tor's heart.

By the time Syverson found Dingledine, the young hacker had joined a Cambridge start-up called Reputation.com and was using ideas analogous to his Free Haven reliability system to grade the reputation of suppliers in business-to-business commerce. The system presaged the reputation network used by eBay to rate buyers and sellers, and offered plenty of intellectual challenge. But it lacked the political drive of Dingledine's anticensorship work. So when Syverson asked Dingledine to help him implement a real-world tool for creating total anonymity, Dingledine was ready to jump. Syverson was soon using DARPA's money to contract work from the younger researcher, and then convinced him to leave Reputation.com outright.

It wasn't long before Dingledine's role at Tor started to exert a gravitational pull on his closest college friend and co-worker at Reputation.com, Nick Mathewson.

A few years earlier, Mathewson and Dingledine had immediately bonded as freshmen at MIT. Mathewson had grown up watching and rewatching *Tron* on VHS, fiddling with PGP, and reading the Cypherpunk Mailing List archives. Dingledine, raised in North Carolina, had found

early dial-up access to the Internet through the University of North Carolina at Chapel Hill's VAX system and created an architecture for networked, text-based dungeon worlds where users could meet, talk, and embark on fantastical quests.

The two teenage hackers moved into MIT's Senior House, a dormitory with a legendarily bizarre culture, captured best by its official emblem: a star-spangled-banner-emblazoned skull with the words "Only life can kill you" in its teeth and the motto "Sport Death" written below. That two-word phrase, once found written in pen in the MIT library copy of Hunter S. Thompson's *Fear and Loathing on the Campaign Trail '72*, denoted an attitude of pushing life to its limits, whether in politics, recreation, or hacking. "Sport Death" culture mixed MIT nerdery into a stew of anarchism, leather jackets, drugs, and polyamorous sex. Music blared at all hours, boxes of computer components often littered the hallways, and sleep was generally considered an occasional nuisance.

Mathewson painted the larger two walls of his room bright red, and the other two black. His theory was that the red walls' psychosomatic effect would keep him alert and reduce his sleep requirements, with the black ones offering enough contrast to shock his brain into hyperactivity again every time he returned his gaze to the red. Mathewson and Dingledine spent much of their college lives in their rooms, hacking away at a half-dozen computers, each kept running constantly. Dingledine named his flock of PCs and servers after *Lord of the Rings* characters, while Mathewson named his after personae from the songs of Frank Zappa. "Most of the interesting things I did in college, I did in software," says Mathewson.

Mathewson and Dingledine subscribed to Sport Death's antiauthoritarian politics, and they lived by the mantra embodied by Tim May and Eric Hughes: "Cypherpunks write code." Don't spend your time arguing with politicians in the physical world about the rules of the digital one. Create the digital world and, with it, your own rules. "Network protocols are the unacknowledged legislators of cyberspace," says Mathewson. "We believed that if we were going to change the world, it would be through code."

So when Reputation.com suddenly found itself sinking into the quick

sand of the dot-com bust, Mathewson was ready to join his comrade in digital progressivism at Tor. Funded by the navy and DARPA for the next three years, Dingledine and Mathewson took apart the tangled code-base developed by the NRL and rebuilt it from scratch. By 2004, there were still only about a hundred nodes on the nascent Tor network, mostly researchers who were curious about the project—Mathewson and Dingledine, perhaps still living in an MIT-like bubble where everyone was an adept hacker, were distributing Tor as raw source code, tough to use for nongeeks.

The civil liberties group, the Electronic Frontier Foundation, on the other hand, saw Tor's potential for mass adoption: They injected another round of funding for Tor to create Windows, Mac, and Linux versions that anyone could install, and Tor's network quickly mushroomed out to several hundred more relays.

But it was only in 2006 that Tor's value suddenly left the realm of computer science theory and jumped onto the world stage. That year, Dingledine and Mathewson started to get e-mails from users in countries like Iran and China, regimes that filter their Internet and monitor it to spy on opposition groups. Tor, unbeknownst to the hackers who created it, had accidentally become one of the world's most effective censorship circumvention tools. By encrypting traffic and routing it indirectly to and from websites via foreign nodes, Tor stymied the digital filters in countries that weed out sites with antigovernment messages and pornography. And unlike other services that promise to skirt censorship—programs like Freegate, Ultrasurf, Hotspot Shield, and Psiphon—it doesn't merely give users access to verboten content while potentially allowing the regime to track their online activity. Tor offers a portal to the Web that's both censorship- and surveillance-free.

The Broadcasting Board of Governors, a little-known U.S. government agency responsible for U.S.-run media outlets like Voice of America, Radio Free Europe, Radio Free Asia, and the Persian-language Radio Farda, contacted Dingledine and asked whether he'd be interested in financial backing to make Tor sleeker and more usable for its censor-skirting audience. The State Department followed up with its own infusion of cash. The result was enough funds to pay the project's entire small staff and

develop a new incarnation of Tor known as the Browser Bundle, a program that can be installed with more or less two clicks. Tor incorporated as a nonprofit. Since then, both its number of nodes and users have exploded. The service added thirty-six million users in 2010 alone.

But Tor's tens of millions of new friends came with powerful enemies. In a gesture to the transparency of its inner workings, Tor publishes the IP address of every relay in its network. To prevent a government from simply blocking all those addresses, it maintains some semipublic relays that it calls "bridges," publishing them on chat networks and social media sites. In 2009, China began crawling the entire Chinese-language Web looking for Tor node addresses and blocked nearly all of them.

Since then, Tor has been playing a game of cat and mouse with the authorities who seek to strangle it. And it's often winning by only a move or two. That's not enough to satisfy Dingledine. "We need to take big steps if we're going to stay ahead," he says grimly. "We need to win this arms race for a while."

Tor has two aces up its sleeve. One is a plan to build a Tor home Wi-Fi router. The Wi-Fi hot spots, in theory, would sell for less than a hundred dollars each and run Tor by default, automatically pushing all the users' traffic through the anonymity network. In exchange, it would function as a Tor bridge relay. Tor's staff hopes those little boxes might add as many as ten thousand nodes, vastly strengthening its network.

Its other secret weapon is a small army of globe-trotting developers. One of them is Jacob Appelbaum. Since Appelbaum joined the nonprofit as a staffer in 2008, the young anarchist has served as one of Tor's primary coders as well as one of its international evangelists, preaching the gospel of anonymity wherever he goes. In a one-month span just before we met in Boston, for instance, Appelbaum had traveled to Brazil, China, Turkey, Poland, Germany, and England, as well as several U.S. cities, giving talks, rallying like-minded hackers to run Tor nodes and volunteer for the organization, and distributing copies of Tor and bridge relay addresses.

If the users or developers he meets worry that Tor's government funding compromises its ideals, there's no one better than Appelbaum to show the

group doesn't take orders from the feds. He refers to capitalism as a "system of violence," and in spite of Tor's early navy funding, he speaks disdainfully of those who work with the military as "war profiteers." In his role as an auto-mythologizing hacktivist, Appelbaum looks the part: His hair has taken the form, variously, of sculpted black spikes, a shaggy side-mop, or a bleached blond crop. His face is studded with piercings that periodically migrate, and tattoos have staked out a growing portion of his body. The largest, on his upper left arm, is a symbol of a peacock taken from the symbology of a group of Satan-worshipping animists he met while traveling in war-torn Iraq. (Several of his personal stories of radicalization—including a few from that trip—were, fittingly, unverifiable.)

But Appelbaum's best evidence of Tor's purity from Big Brother's interference, perhaps, is his very public association with WikiLeaks, the American government's least favorite website. In a surprise speech at the Hackers on Planet Earth conference in July 2010, Appelbaum gave a keynote address on behalf of WikiLeaks after Julian Assange decided that traveling to the United States spelled legal trouble. Since then, the U.S. government has expressed its displeasure with him by tasking Customs and Border Protection agents with harassing him every time he crosses the border, where the Fourth Amendment's restrictions on searches and seizures abandon citizens. According to Appelbaum's accounts, he's often detained for hours, searched in intrusive bodily detail, and forced to miss any connecting flight.

In those detainment sessions, Appelbaum is separated from any phones, computers, or storage devices that he may be carrying, a painful security breach for a privacy-conscious cypherpunk. After abandoning several computers that he considered compromised, he no longer travels with a hard drive in his machines. How does that work? I ask. "Not very well," he says.

He takes the harassment with a dose of humor, often live-blogging his run-ins with customs on Twitter and at least once leaving a spring-loaded snake inside a fake can of nuts for a customs agent to find. But the intimidation as he tries to reenter his own country serves as a constant reminder to Appelbaum of the looming threat of prosecution. When the agents

interrogate him, he says the questions are always the same: "What's your relationship to Julian Assange? What's your association with WikiLeaks?"

Appelbaum usually responds to those questions with stony silence, and he won't answer them for me either. But when I ask Appelbaum if Tor is in fact the powerful tool for anonymous whistleblowing that Assange and others believe it to be, he smiles. Then he quotes Assange quoting Oscar Wilde.

"Give a man a mask," he says, "and he'll tell you the truth."

.-.. .... --- - .-. .--. - --.. --.- -.-- .--- .... .--- -- -.- ...

Appelbaum was born in Northern California to two poor, freewheeling, secular Jews who never married. To call the environment of his early childhood a dysfunctional family wouldn't capture just how rarely it functioned at all: Appelbaum describes his mother as a paranoid schizophrenic who split with his father before Appelbaum was born—he would later hear stories that she believed his father had molested him while he was still in her womb. Appelbaum's father was a heroin addict and, in the eyes of the court, was hardly more fit than his mother to care for their newborn son. The couple's custody fight would last a full decade of his life.

During that prolonged legal battle, Appelbaum lived with his mother's sister, but he says she wasn't ready for parenthood. At the age of eight she sent him to live at the Sonoma County children's home. One of his only happy memories of the next lonely years, he says, was a night when an older child at the home taught him to hack the building's combination keypads by blowing chalk dust onto them, revealing the entry pattern in finger oils. Appelbaum remembers slipping out into the night and wandering an empty baseball diamond, for a moment free and in control of his life.

Appelbaum would spend another two years in the home and in foster care before his father won custody of him. Despite seeing him rarely for the first ten years of his life, Appelbaum still paints his father in heroic terms. An actor, director, and member of a band called the Tattooed Vegetables, Ricky Appelbaum ran in the same circles as Frank Zappa and the Lithuanian-American sculptor and dancer Vito Paulekas and was known

to have sported half a beard on one side of his face and half a mustache on the other. According to his son, he also became a serial burglar for several years in the 1970s, mostly robbing pharmacies to feed his addiction.

The stories Appelbaum shares of his father's exploits are legendary, if unconfirmable: how he learned to lift fingerprints from random surfaces, set them in latex, and plant them at the scenes of crimes; how he stole police cars, went joyriding, and crashed them; how, the night he was finally caught by the cops, he'd had a nervous breakdown and lain down behind the counter of a store he had broken into. (In fact, no legal records show any convictions.) Soon after moving in with his father, the young Appelbaum says his father showed him how to crack the safe he kept in his office, listening to its inner workings with a stethoscope.

Like his father, the younger Appelbaum slipped naturally into life on the fringes of society, cross-dressing, dying his hair, and begging for change on the street. As much as he idolized his father, living in his drug-fueled, anarchic world was often nightmarish. The family spent much of its time in homeless shelters or moving from house to house. When they did settle down temporarily, Appelbaum's father would sublet most of the rooms of their home to fellow junkies to pay for his own habit, leaving Appelbaum with half of the kitchen as a bedroom and only a hanging sheet for privacy.

Appelbaum remembers the cast of housemates who inhabited that broken home: One lunatic who believed he was Anthony Burgess and spent his time rewriting *The Doctor Is Sick* in blue ballpoint pen. A small balding man who spat on the floor. Two Rastafarian junkies who once used the lightbulbs in Appelbaum's "bedroom" to smoke mothballs; he woke up in the middle of the night to the sounds of their laughter, choking in the dark on the acrid fumes.

One morning, he walked into the bathroom before school to find a woman convulsing in the tub with a syringe in her arm. Another day, Appelbaum came home from school and found his own father overdosing on the couch. He had written a note: "Dear Jake. Life is hard. Goodbye. I love you." Appelbaum woke his father up, walked him around the house, and he survived.

Despite those experiences, Appelbaum doesn't blame his father for his

tarnished childhood. Ricky Appelbaum's inability to kick drugs, he believes, stems in part from a childhood accident: The elder Appelbaum was hit by a drunk driver at the age of nine and for the rest of his life suffered from incurable pain. Appelbaum himself was hit by a car while crossing the street at the age of fourteen—he was wearing a black dress, black tights, and a purple wig—and still suffers from chronic back injuries. "We weren't so different," he says. "I chose computers instead of heroin."

Appelbaum's first PC, in fact, was a gift from his father, a Macintosh 7200/90 that was almost certainly stolen. ("Junkies don't acquire things like that by buying them," he explains.) A friend at school and a neighbor's father taught him about networking protocols, the inner workings of operating systems, simple programming. He read the Cypherpunk Mailing List archives and rediscovered its lessons about the power of cryptography to counter authority and violence, how it "shifts the balance of power from those with a monopoly on violence to those who comprehend mathematics and security design." And the digital world at large offered him an abstract realm free of the corruption of his psychotic and drug-addled home, a place unhooked from reality where he could reinvent himself at will.

Appelbaum had a knack for manipulating that world and its tools. But his formal education was cut short. At the age of twenty, he dropped out of Santa Rosa Junior College to take care of his father, who by then was suffering from cirrhosis of the liver, hepatitis C, and diabetes. To pay his bills and those of his ailing father, he took a job working in a nonprofit that refurbished old computers for charity. On the side, he began volunteering for activist collectives and NGOs, groups with names like Resist.ca, and the Ruckus Society.

In 2002, those gigs led Appelbaum to his first real job: an information technology administrator position at Greenpeace. It was a tougher and more practical education than anything he would have found at Santa Rosa Junior College. Appelbaum learned from a combative, grizzled Linux guru at the NGO who went by the hacker handle Shord. His mentor—and the rest of Greenpeace—took information security seriously. The group's radical environmentalists often referenced the *Rainbow Warrior*, a ship Greenpeace used in its antiwhaling activities that was sabotaged and sunk by

French intelligence agents in 1985, drowning one of the group's photographers. "Greenpeace's security issues are real," says Appelbaum. "When things go badly, people die."

Appelbaum's induction into radical activism was also the beginning of his borderless lifestyle, flying around the world to participate in the group's direct actions. He helped perform reconnaissance for a San Francisco stunt in which the group dropped a massive banner over the Wells Fargo building to protest its funding of Appalachian mountaintop-removal coal mining. At one point he flew to Amsterdam to meet the Dutch cypherpunk Rop Gonggrijp and his business associates, who handed over Pelican cases of CryptoPhones. Greenpeace was among the first independent organizations to test those encryption-enabled mobile devices, now widespread among intelligence agencies and those that fear them.

When he wasn't working for Greenpeace, Appelbaum volunteered and contracted his computer skills to groups like the Rainforest Action Network, the Tactical Tech Collective, and the Open Society Institute. He met Roger Dingledine and Nick Mathewson at the Defcon hacker conference at the Bellagio Hotel in Las Vegas, and soon began volunteering for Tor, too, running Tor nodes on whatever PCs he had available. Dingledine, in return, became Appelbaum's educator in all things anonymous. "Roger is the Gutenberg of anonymity. He taught me how to think," says Appelbaum. "They were welcoming. They had a community. I joined it."

Out of his shattered childhood, Appelbaum had assembled a life on the front lines of digital activism. And then it all fell apart again.

Ricky Appelbaum died four days before Christmas in a San Francisco hospital. The younger Appelbaum blames the junkies who had shared his father's home. He says they had withheld his drugs, repeatedly injecting his legs instead with warm water. When Ricky Appelbaum died of cirrhosis and infected abscesses in his legs, they left the apartment with practically everything he owned. The police, his son says, weren't interested in investigating. He claims they told him that "no one cares about junkies" and instead threatened to arrest him for possessing his father's drug paraphernalia.

"My hatred of authority was pretty much solidified," he says.

After his father's death, activism no longer felt like enough. Appelbaum wanted to escape American society, to "stop contributing to a world of bullshit evil," as he would later describe it. He decided to leave the United States and visit an old friend from Greenpeace who had started a wireless infrastructure business in a place as far as possible from San Francisco and the ghost of his father: Iraq.

No military escort or even a visa; he would smuggle himself over the northern border with Turkey. "I guess I was tired of my first-world problems," Appelbaum says. "I decided that I would either come back whole, or come back full of holes."

-- - .. .- --- -- .... .-. -.-- -. -.-. .... --. .- . ....

In the months before Julian Assange dropped out of college in 2005 to pursue his antiauthoritarian dreams, he was plagued by ideas that seemed to have lodged in his mind, so deeply that when they emerged in discussions with fellow students, they burst forth almost as fully formed lectures.

One of the topics over which Assange obsessed was the Bourbaki, a circle of 1930s French mathematicians who all wrote under the name Nicolas Bourbaki. The Bourbakis' goal was to create a new groundwork for mathematics out of solid and apparent first principles. Seeking to delete ego from their rigorous, systematic work, they assumed the Bourbaki name to expel all public identity beyond that of the group itself. Assange dreamed of a group that would apply the same ideas to journalism, building stories out of public documents available to all, and posting them under a single, pseudonymous byline.

Another of Assange's idées fixes, one fellow student remembers, was onion routing. And over beers one evening in an Irish pub called Pugg Mahones at the edge of Melbourne University, he laid out Paul Syverson's elegant idea to that friend in pedagogical detail: a wrapped ball of information shedding skins as it bounced between relays from secret origin to secret destination. The perfect conduit for Oscar Wilde's masked truth-teller.

In 2005, Assange quit school and moved into a nearby house that became a proto-headquarters for what would become WikiLeaks. He covered the walls with blueprints for the site's architecture, code, and mathematical formulas. He worked for long hours, installed a red lightbulb in his bedroom in an effort to regulate his sleep, and ate little. The house filled with fellow hackers and like-minded activists who would crash in the house rent-free in exchange for working on Assange's project.

WikiLeaks, in its original conception, would use a wide variety of tricks to keep the world—and even itself—totally ignorant of its sources' identities. It deployed Secure Sockets Layer encryption like any banking or e-commerce site to scramble its communication with all visitors and obscure its content from snoops. One of WikiLeaks' initial advisers, Ben Laurie, had invented an open-source version of that protocol for the Web server software Apache, OpenSSL, that nearly half the world's websites use today.

Encryption wasn't enough, however. WikiLeaks didn't want to simply hide what sources said, but rather completely obliterate any way of finding out who they were. The server that ran the site would keep no logs of any IP addresses of visitors; Assange would risk no Penet-type subpoena debacle. But WikiLeaks added another, unique trick to that end: a script that launched in the browser of any visitor to the site and generated commands that looked like randomly sized submissions to WikiLeaks' secure server. To anyone snooping on WikiLeaks' visitors, it would be impossible to distinguish between those who had come to the site to read its publications or make a donation and those who intended to drop secrets. Thanks to the cover traffic of spoofed submissions, everyone looked like a leaker.

But it was Tor, of course, that would become WikiLeaks' core tool for protecting the anonymity of both its most sensitive sources and the site itself. The leaking site's submission system would run a Tor Hidden Service, so that users could access it through rendezvous points in its volunteer network of relay nodes. The submissions server's location would be just as hidden as that of the user. In theory, no one who wanted to launch a digital or legal attack on the site would even know where to begin, and sources would have the assurance from Tor that their identity was as anonymous as any Web communication could be.

In the early WikiLeaks developer communications leaked by John Young, Assange also describes physical drop-offs: mailing addresses where

sources could anonymously send materials ranging from CDs to thumb drives to paper documents. Some would be "deniable" submissions addresses, in that the material would be encrypted with WikiLeaks' public key, and the drop-off handler wouldn't have the private key to unscramble the material. The uploader would never have any knowledge or responsibility for the leaked content. But other volunteers would accept unencrypted documents by post and even scan in reams of paper submissions and convert them to text files.

The postal system, for anyone careful with fingerprints, has the potential to be more anonymous than any means of digital communication. But aside from its snailish speed, physical mailings with no return address have an obvious bug compared with onion-routed digital leaks: They don't provide a way to write back. In the United States, even setting up a post office box as a return address requires two forms of identification, hardly the ideal feedback channel for an anonymous leaker.

Tor, on the other hand, allows instant feedback. WikiLeaks initially ran a chat room that used the instant messaging protocol IRC. An anonymous source communicating by Tor-protected instant messages could be questioned one second and respond the next with a verifying fact, another crucial document, or simple technical fixes.

For Assange, Tor may have also possessed another unique capability, one that served a far more morally ambiguous purpose—as much an inherent bug in the system as a feature. Anyone who controls a node on the edge of the network, with a few simple tools, can read every unencrypted file that comes out of it. While Tor triple-encrypts all the files it routes as a key step in its anonymity mechanism, that encryption is stripped away in the routing process. Any data that isn't encrypted before it enters Tor's maze of pipes won't be encrypted when it comes out the other end either. The service, after all, is designed to hide who the user is, not the data he or she is accessing or uploading.

Traditional implementations of encryption like SSL and PGP can solve that problem. But as with every security mechanism, users slip up. And much of the Web isn't configured for SSL. The result, apparent to thousands of

the hacker types who run Tor nodes, is that a clever relay operator can essentially suck out copies of any unencrypted data that exits the anonymity network through the node he or she controls. Tor's administrators explain as much in the tool's documentation:

"Tor anonymizes the origin of your traffic, and it makes sure to encrypt everything inside the Tor network, but it does not magically encrypt all traffic throughout the Internet," the site warns. "Yes, the guy running the exit node can read the bytes that come in and out there."

And many believe that WikiLeaks did exactly that.

In a June 2010 profile of Assange, *The New Yorker* reported that before WikiLeaks' launch, a member of the project who ran a Tor exit node had noticed Chinese hackers using the relay to hide their tracks. Millions of documents were passing through the computer as the cyberspies went about their daily business of penetrating target servers and exfiltrating vast amounts of data. WikiLeaks' volunteers began to record that traffic, and the immense bolus of information that they collected became a repository of documents that Assange would later tout, in what may have been a less-than-honest bit of marketing, as proof of WikiLeaks' early success. "We have received over 1.2 million documents so far from dissident communities and anonymous sources," WikiLeaks boasted on its site circa 2007.

When that *New Yorker* account of WikiLeaks' origin story became a headline on Wired.com, Assange issued a vague and circuitous denial. "The imputation is incorrect," he told the tech news site The Register. "The facts concern a 2006 investigation into Chinese espionage one of our contacts [was] involved in. Somewhere between none and a handful of those documents were ever released on WikiLeaks."

But in another 2006 e-mail published by John Young on Cryptome after his falling-out with WikiLeaks, Assange described something that sounds very much like hoovering up sensitive data as it spills out of a Tor node. "Hackers monitor Chinese and other intel as they burrow into their targets," he wrote to Young. "When they pull, so do we."

The result, Assange continued breathlessly in that message, was an "inexhaustible supply of material. Near 100,000 documents/emails a day."

The data flood, he wrote, included hacked internal documents from the Council on Foreign Relations, half a dozen foreign ministries, the United Nations, trade groups, the World Bank, even the Russian cybercriminal mafia. Mendax's hacker dream made reality.

"We're drowning. We don't even know a tenth of what we have or who it belongs to. We stopped storing it at one terabyte," he wrote. That data trove would have been thirty times the size of every text article stored on Wikipedia today.

Whether or not those files were ever released, they marked the first seeds of WikiLeaks' power. Assange sounds in his e-mail like a man made practically giddy over the wealth of secrets at his fingertips. "We're going to crack the world open," he told Young, "and let it flower into something new."

When Appelbaum told the guards on the Turkish-Iraqi border that he was a tourist, as he recounts the story, they laughed at him and waved him through, refusing to even stamp his passport. A taxi had taken him from Diyarbakir through the Turkish city of Batman, and crossed into Iraq over a bridge straddling a river Appelbaum describes as "so brown and polluted that you wondered whether, if you fell in it, your bones would reach the bottom."

In the Iraqi city of Zakho, he was picked up by his old Greenpeace friend and his wife in a white SUV, with a Glock, an AK-47, and Browning nine millimeter handgun in the backseat. They drove to the northern town of Arbil, stopping to look in ghostly abandoned buildings along the highway. In one they found children's drawings of helicopters firing on humans, rockets hitting buildings. In Arbil, Appelbaum spent the next days photoblogging and interviewing locals, uploading the results with a satellite modem and the peer-to-peer file-sharing protocol BitTorrent. To any Iraqis who seemed computer-savvy, he distributed copies of the open-source operating system Linux, spreading free software like a hacker Johnny Appleseed.

Appelbaum found in his conversations that the local Kurds, unsurprisingly, were mostly happy with the U.S. invasion and the toppling of Saddam Hussein's regime. But from the Arabs who lived in Arbil he claims to

have heard more disturbing stories of soldiers who fired .50 caliber bullets at oncoming cars at checkpoints, killing their drivers and all passengers, rather than aim for the engine block. A man told Appelbaum he kissed his wife every morning before leaving the house, thinking he would never see her again. Iraqis asked him sincerely whether Americans understood that they were normal people with homes and families. "As an American, I found myself feeling pretty awful about what we'd contributed to," he says.

In Kirkuk, the trio's vehicle broke down. While they waited for help on the side of the road, an enormous boom sounded over the hill behind them, and a black cloud of smoke rose from what seemed to be an oil refinery. Minutes later, two truckloads of soldiers, one American followed by one Iraqi, drove by. Appelbaum's group laid low until his friends' co-workers could bring them a new car, and then drove on. But the incident reminded him of how close he was to real harm. When his friends left Iraq for Istanbul, he left with them. "I was not in the greatest headspace, I guess," he says. "But at some point my desire to live started to outweigh my desire to be shot in a war zone."

Appelbaum returned to San Francisco and took a job at a security start-up, building software that automatically scanned code for vulnerabilities. The company was acquired and his entire office was laid off. Soon after, he was at a party in the city's Mission District when news hit that the levees had broken in New Orleans: Hurricane Katrina had left nearly two thousand dead and tens of thousands more stranded in sports stadiums used as shelters. When one of the partygoers tried to turn off the television and lighten the mood, Appelbaum angrily grabbed the remote, turned up the volume, and refused to change the channel.

Days later, he flew to Texas, created a press pass for an obscure news agency, and slipped into the Astrodome to interview Katrina's victims. "I got through the checkpoints the same way you hack firewalls: by identifying and exploiting weaknesses," he says. Inside the makeshift shelter, he reported the inhabitants' stories of prisonlike conditions: A man beaten in the shower. Nightly curfews, women raped. Some of the evacuees believed that the Army Corps of Engineers had blown up New Orleans's levees to preserve more expensive real estate while flooding their parishes. Some other reports

disputed those stories. But for Appelbaum, "This American disaster was a lot like the other American disaster I witnessed in Iraq," he says. "The same thing, over and over again. The disconnection. The lack of humanity."

Appelbaum worked with a group of activists that collected radios and distributed them to the Astrodome's inhabitants to provide news for those trapped inside. Then he loaded up on provisions and drove to the Algiers neighborhood of New Orleans, moved into a house organized by the activist collective Common Ground, and helped to set up EVDO wireless Internet connections so that the area's hard-hit inhabitants could register online with FEMA to receive aid.

When Appelbaum returned from New Orleans, his tour through two levels of hell had left him more committed than ever to the liberating powers of technology. But he had yet to find the community that would be his own cypherpunks, the crypto-obsessed peers who would enwrap him in a larger movement and push him to greater feats of crypto-anarchy.

That group would be the Chaos Computer Club.

In many ways, the CCC had progressed years ahead of Tim May and Eric Hughes's crypto-liberation movement in California. Founded by the German hacker luminary Wau Holland in 1981, the Hamburg- and Berlin-based nonprofit had been demonstrating the insecurity of public computer systems as early as 1984, when its hackers used the home terminal system created by the German postal system to transfer the equivalent of $50,000 from a bank to the CCC's accounts. (The money was given back in a public ceremony the next day.) With a true surveillance state looming just over the Berlin Wall, privacy, antiauthoritarianism, and the need for strong crypto had been steeped into the group's core.

Almost exactly a year after his father's death, Appelbaum flew to Berlin to attend the CCC's annual Chaos Communication Congress. The topic of his talk was the same problem that had troubled Julian Assange years earlier, one central to any activist who believes in the power of cryptography: how to keep encrypted data encrypted, even when authorities are standing over the user, rubber hose in hand, demanding the key.

In his talk in Berlin, Appelbaum walked the audience through a series

of crypto-schemes, grading various software and taking special pleasure in giving Apple an F. (The user's unencrypted key could be extracted from a file Apple carelessly left on the computer's hard drive.) And then he came to Julian Assange's very own solution to the problem of violent key extraction—Assange's 1997 invention, the crypto-scheme Rubberhose.

"In today's world," Appelbaum told the audience of European hackers, "this is probably going to get you killed."

Appelbaum cited the obvious issue: If the jailer knows his prisoner, Alice, is using Rubberhose, he'll never stop torturing her to try and get more of the data that may be hidden on her hard drive. "I don't think it's a good idea to never be able to prove you don't have any more secrets," Appelbaum told the CCC crowd.

Instead, he offered an idea for a new theoretical solution: MAID, or mutually assured information destruction. In the system Appelbaum suggested, Alice keeps her cryptographic keys on a faraway server, accesses it only with Tor to keep its location obscured, and sets a certain time limit. If that time limit passes without Alice checking in, MAID automatically deletes all her keys. When Alice gives in to her jailer after either suffering through a certain period of torture or legal silence, she can show him that the keys no longer exist. Everything on the server full of secrets becomes permanently, irrevocably encrypted. "You're not obstructing justice anymore," Appelbaum explained. "Justice was just too slow to catch you."

In the questions period following the talk, Ralf-Philipp Weinmann, the researcher who had developed Rubberhose with Assange a decade earlier, stood up and laid into Appelbaum, defending Rubberhose and pointing out flaws in the MAID concept. They debated genially and then agreed to talk afterward.

That conversation drew Appelbaum into Assange's circle, albeit indirectly. Appelbaum became a CCC regular, and Assange would attend the next year to introduce a project he was working on: WikiLeaks.

Friends say they met at that wintry Berlin conference. Their paths must have felt uncannily parallel: broken, wayward childhoods, IQs beyond those of the hated authorities that tried to exert power over their lives, and a

belief in the redemptive power of cryptography to defeat those forces. By Appelbaum's fourth year at the conference, they had become close. Appelbaum told me he woke up on New Year's Day after the Twenty-sixth Chaos Communication Congress in bed with Assange and two women. "That was how we rolled in 2010," he says, smiling. (He later clarifies that they had busied themselves the night before with programming, not sex, and slept in different beds. "I can dream," he adds.)

The two never spoke about Appelbaum's critique of Rubberhose. But the CCC conference where Appelbaum spoke on the superiority of cryptography to violence, the young cypherpunk says, was "the start of a good friendship."

--- -- .. -.-- -.-. .... ---- ... -.-. . -.-. .--- -.- .- .... .

Browsing WikiLeaks' archives from 2006 to late 2009—the years before it was catapulted onto the world stage—feels like opening a creaking door onto a dusty museum of badly organized, fascinating secret artifacts: A purported draft of a resignation letter from Venezuelan president Hugo Chavez. A military report on the prevalence of hash-smoking among a group of American soldiers. An internal video from networking tech giant Cisco showing every television and movie scene in which it had purchased product placement. A list of sites to be censored by a Norwegian Internet service provider. A report on incompetence among safety staff at the Rocky Mountain Biological Laboratory. A censored image of the Belgian chief of police photoshopped into a pornographic scene. The handbooks of secret rituals for nine different fraternities.

It all started with a single, unverified document. Whether by sniffing the Tor network, receiving it from a Tor-masked source, or through other untraced means, Assange and WikiLeaks obtained and published its first leak: It was a Somalian government document calling for the assassinations of leaders in two rogue Somali states.

John Young, who at that point hadn't yet broken off from the group, warned that the leak could easily be disinformation or a forgery. "This is not to suggest leaks are not to be trusted, just not blindly so, for they are now

standard tools for lying, smearing and stinging by governments, corporations, persons of all demonics," Young wrote on the WikiLeaks mail list.

In the end, WikiLeaks did post the Somalian leak, but with a breathless disclaimer: "Is it a bold manifesto by a flamboyant Islamic militant with links to Bin Laden? Or is it a clever smear by US intelligence?"

As WikiLeaks' profile rose, the answer never surfaced, and hardly mattered. Assange traveled to Kenya, moved into the compound of Doctors Without Borders, and continued to tout WikiLeaks at the World Social Forum, a collection of nonprofits and activists that shadowed the World Economic Forum. Seeking to create a "WikiLeaks advisory board for Africa," he met with Mwalimu Mati, an organizer of Transparency International in Nairobi. "We had tried many online whistleblowing sites," says Mati. "But WikiLeaks' idea of using cryptography to separate the whistleblower and the source . . . that seemed to me to be very useful and clever."

The Kenyan leak that would put WikiLeaks on the map, it turned out, had little to do with encryption. In 2004, the Nairobi government of Mwai Kibaki had taken power after the long reign of Daniel arap Moi, promising an end to the corruption of the Moi regime. Kibaki commissioned a report into the previous regime's embezzlement, suspected to be billions of dollars, that would come to be known as the Kroll Report. But when Kibaki's government started to come under fire for its connections to the Moi indiscretions, the report wasn't released.

Instead, someone printed it out and mailed it to Mati. It confirmed the worst: more than two billion dollars siphoned to Moi's associates' properties in twenty-eight countries, hundreds of millions given to his children, and even reports of currency counterfeiting by the regime's organized crime connections. Knowing that Nairobi's media was hardly independent enough to publish the bombshell report, Mati gave it to WikiLeaks. *The Guardian* picked up WikiLeaks' release and printed the front-page headline "The Looting of Kenya." Mati and Assange followed up with another major leak, again sourced to an envelope that appeared on Mati's desk. It detailed the extrajudicial executions of members of a criminal gang called the Mungiki, a crackdown that led to the indiscriminate police killings of thousands of young men.

After those exposés, "the site's popularity rocketed," says Mati. Leaks began to flow in earnest to the site's submissions system: A detailed account of the Cayman Islands tax shelters administered by the Swiss bank Julius Baer, an internal report from the mining giant Trafigura detailing the effects of its toxic dumping in the Ivory Coast that had been legally prevented from appearing in British media. Icelandic banking documents that would catalog the country's financial meltdown and eventually inspire a transformative legal movement in the volcanic island. And a collection of pager messages from September 11, 2001, that would catch the attention of one young analyst in a dusty base in Iraq.

But for Assange, the most gratifying moment of WikiLeaks' ascendancy may have had a smaller, but more personally meaningful, target: the Church of Scientology. Since the days of Penet and Suburbia, the church's lawyers had continued to intimidate anyone that leaked its manifold secrets, both to traditional media and digital outlets. So when WikiLeaks published a 208-page strategy manual that seemed to have been written by founder L. Ron Hubbard himself and detailed strong-arm tactics for attacking journalists and even tricking airlines into revealing their flight details, the church responded with its usual suppressive methods. A letter from the group's lawyer asked WikiLeaks to remove the documents immediately.

Assange, needless to say, did not. And instead of merely holding an eleven-person protest as he had in his cypherpunk days, this time he fired back with both barrels. "WikiLeaks will not comply with legally abusive requests from Scientology any more than WikiLeaks has complied with similar demands from Swiss banks, Russian off-shore stem cell centers, former African kleptocrats, or the Pentagon. WikiLeaks will remain a place where people of the world may safely expose injustice and corruption," read a letter sent back to the church's lawyer. "In response to the attempted suppression, Wikileaks will release several thousand additional pages of Scientology material next week."

Today, the site has a special Scientology section in its archives. It holds more than one hundred documents, one of the largest collections of the church's internal papers stored anywhere in the world.

In July 2010, three months after WikiLeaks had released a clip of a U.S. Apache helicopter gunning down civilians and journalists in a Baghdad suburb and just days before the group would publish seventy-six thousand secret military documents from Afghanistan, Julian Assange was scheduled to deliver the keynote address to an audience of thousands at the Hackers on Planet Earth conference, a gathering held at the venerable Hotel Pennsylvania in New York. But when the keynote began, it was a young, dark-haired American, not Assange, who walked onto the stage. He wore a T-shirt that read "Stop Snitching," a reference to Adrian Lamo, and was introduced by the conference organizers merely as "WikiLeaks."

"Hello to all my friends and fans in domestic and international surveillance. I'm here today because I believe we can make a better world," Appelbaum told a bewildered crowd that had expected a blonder, more Australian figure. "Julian, unfortunately, can't make it, because we don't live in that better world right now, because we haven't yet made it."

"I wanted to make a little declaration for the federal agents that are standing in the back of the room and the ones that are standing in the front of the room, and to be very clear about this: I have, on me, in my pocket, some money, the Bill of Rights, and a driver's license, and that's it. I have no computer system, I have no telephone, I have no keys, no access to anything. There's absolutely no reason that you should arrest me or bother me. And just in case you were wondering, I'm an American, born and raised, who's unhappy. I'm unhappy with how things are going."

He explained that he worked for Tor, but that he wasn't at the conference to represent his employer. "I'm certain they wouldn't be too unhappy with me speaking here, but they certainly didn't know about it before this moment." Then he explained that he believed in standing up for human rights and social change, for free speech without retribution.

"To quote from *Tron*," he said, "I fight for the user."

For the next hour and fifteen minutes, Appelbaum railed against the war in Iraq and Afghanistan in steady, simple rhetoric. He lashed out at

WikiLeaks' critics and Lamo, whose name he refused to even utter, for informing on Bradley Manning. He argued against the idea of "speaking truth to power." "You stick it to the man and show the man how it is? Well I think that's stupid. Power knows power because power's in power," he told the crowd. "It's important to take this power and give it to people who are not simply the ones who make the decisions. Give it to the people who vote them in and out of office.

"The people in power cannot issue a denial when everyone knows the truth," he continued. "They can't redact a document when everyone has a copy of it in their heart and in their mind."

And then, he delivered the news: Appelbaum announced that WikiLeaks' submissions system, which had been down the previous months, had been redesigned and relaunched. He displayed the Tor Hidden Services page that any leaker could visit to anonymously feed documents to the site.

And then Appelbaum went further, directly appealing for the audience of hackers, many of whom held day jobs in corporate cybersecurity, to become an army of leakers.

"I never expect to work in the computer security industry again. But that's OK. I think this is far more important than anything like that," Appelbaum said, with a vulnerable note in his voice. "Some of you won't make this choice, and that's OK. And some of you will pretend not to make this choice, and you'll go in deep. And thank you for that."

Appelbaum paused. The audience response began with a few sparse claps, as if the crowd wasn't yet sure about its commitment to the role they were being asked to take on. Then it slowly grew, rippling through the room, and swelled into a steady roar of applause. As his talk ended, Appelbaum exited the stage, and seemed to reappear donning a black hoodie.

In fact, the hoodie wearer was a decoy. Appelbaum had slipped out a back exit to board a flight to Berlin. While he surreptitiously left the hotel, the Collateral Murder video was projected onto an enormous screen. Apache gunfire echoed over a silent throng of hackers: a dark orientation video for the newborn leaking movement.

PART THREE

THE FUTURE OF LEAKING

"Paranoia will kill us."

BIRGITTA JÓNSDÓTTIR

SOURCES

This is a book, in a sense, about primary source documents. E-mails, chat logs, memos, and manuals are the currency of the leaking movement, and like the book's subjects, I've sought to use them whenever possible to underpin this story.

In this age of overflowing, recorded digital communications, my task in writing several chapters was to carve a narrative out of hundreds or thousands of pages of text—often leaked themselves—whether it be Adrian Lamo's and Bradley Manning's instant message logs, the decade-plus archive of the Cypherpunk Mailing List, or the hacked e-mails of HBGary Federal. If I had adhered to Julian Assange's doctrine of scientific journalism, which demands that the reporter publish the entire source document of a story along with his or her interpretation, this book would have been many thousands of pages long.

But for many sections of the book I also resorted to the usual method of a reporter: hundreds of hours of interviews, conducted face-to-face whenever possible, and when necessary by phone, e-mail, instant message, and letters. I interviewed every person included in the character list at the front of this book, with the exception of Bradley Manning, who for the duration of my reporting has been in a military jail or a courtroom. I'm especially

grateful to many sources who spent hours with me, speaking under the condition of anonymity with no direct personal benefit.

The very few bits of dialogue in the book that I didn't personally hear were recounted to me by witnesses who were present, and thus may not be recorded exactly verbatim. I've edited some quoted texts' punctuation and capitalization for readability. With the exception of any stray facts that may have been missed in my efforts to note all sources, everything I've written that's not cited below can be attributed to my own reporting.

Primary sources and interviews aside, I'm particularly indebted to a few prior books and articles as instructive signposts for my reporting and primary sources in their own right. They include Daniel Ellsberg's memoir *Secrets*, Suelette Dreyfus and Julian Assange's *Underground*, Steven Levy's *Crypto*, Daniel Domscheit-Berg's memoir *Inside WikiLeaks*, Robert Manne's "The Cypherpunk Revolutionary: Julian Assange" in Australia's *The Monthly*, Nathaniel Rich's "The Most Dangerous Man In Cyberspace" in *Rolling Stone*, and Raffi Khatchadourian's spectacular *New Yorker* article "No Secrets."

PROLOGUE: THE MEGALEAK

trick companies' employees into revealing their passwords over the phone Suelette Dreyfus and Julian Assange. *Underground: Hacking, madness and obsession on the electronic frontier.* First published by Mandarin, a part of Reed Books, Australia, 1997, available at http://suelette.home.xs4all.nl/underground/Underground.pdf

speculation that WikiLeaks' target would be Bank of America shaves off $3.5 billion from the company's total value Dan Fitzpatrick. "Bank's stock declines on WikiLeaks Anticipation." *Wall Street Journal,* November 29, 2010.

Many of them cited WikiLeaks' revelations about the U.S. State Department's disdain for Tunisian president Ben Ali Sami Ben Hassine. "Tunisia's youth finally has revolution on its mind." *The Guardian,* January 13, 2011.

"WikiLeaks, which publishes information written by lying ambassadors in order to create chaos" Robert Mackey. "Qaddafi Sees WikiLeaks Plot in Tunisia." *The New York Times,* January 17, 2011.

WikiLeaks had cratered negotiations that might have kept them there longer CNN wire staff. "Obama: Iraq war will be over by year's end; troops coming home." CNN.com, October 22, 2011.

choking it to the point of paralysis Will Oremus. "Almost Broke, WikiLeaks Suspends Operations." Slate, October 24, 2011.

actively coached the young Army private, potential grounds for his own indictment Kim Zetter. "Jolt in WikiLeaks Case: Feds Found Manning-Assange Chat Logs on Laptop." Wired.com, December 19, 2011.

94 percent of the world's recorded information Martin Hilbert and Priscilla Lopez. "The World's Technological Capacity to Store, Communicate, and Compute Information." *Science,* February 2011.

five times as many pages being added to the world's classified libraries as to its unclassified ones Peter Galison. "Removing Knowledge." *Critical Inquiry,* Autumn 2004.

76.7 million documents were classified in 2010, compared with 8.6 million in 2001 and 23.4 million in 2008 Information Security Oversight Office Annual Report, April 15, 2011.

Of those, about 1.2 million have top secret clearance Greg Miller. "How many security clearances have been issued? Nearly enough for everyone in the Washington area." WashingtonPost.com, September 20, 2011.

"These Days the Web Unmasks Everyone." Brian Stelter. *The New York Times,* June 20, 2011.

as the *New Yorker* cartoon caption reads Peter Steiner. *The New Yorker,* July 5, 1993.

"a series of unfortunate events" Clay Shirky. "WikiLeaks has created a new media landscape." *The Guardian,* February 4, 2011.

CHAPTER 1: THE WHISTLEBLOWERS

only other analyst at RAND who knew about and sympathized with Ellsberg's leaking plans Daniel Ellsberg. *Secrets* (London: Penguin Books, 2002), p. 295.

Was that peculiar green color some kind of radiation? Ibid., p. 302.

comb through the encyclopedia-size pile to excise them Ibid., p. 370.

nonchalantly consume a sweet roll and a cup of coffee over the course of several hours Ibid., p. 332.

greet the policemen politely, and carry on his work as soon as they left Ibid., p. 301.

understand exactly what he had done, and why Ibid., p. 305.

aide hastily rescinded the offer Ibid., p. 333.

"Pretty simple and unglamorous" Evan Hansen. "Manning-Lamo Chat Logs Revealed." Wired.com, July 13, 2011.

"a very dangerous precedent for the government the way it wants to operate today" Sam Bozzo. "Hackers Wanted." Available on YouTube http://www.youtube.com/watch?v=cLJbMP2S5sA

"If you had unprecedented access to classified networks fourteen hours a day seven days a week for eight plus months, what would you do?" Hansen.

"Isn't it after all only history?" Ellsberg, p. 357.

"I'm sorry, I can't do it." Ibid., p. 363.

sneak into the Cambridge apartment, have the papers photocopied in a nearby shop, and return them Ibid., p. 375.

Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U.S. Involvement Neil Sheehan. "Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U.S. Involvement." *The New York Times*, June 13, 1971.

Gelb immediately fixated on Ellsberg as the source Wells, p. 407.

"Ellstein" as Nixon called him Ibid., p. 426.

Boston Globe*, the *L.A. Times*, *The Christian Science Monitor*, the *St. Louis Post-Dispatch Ibid., p. 396.

the one who had offered Ellsberg her photocopier—testified to the bureau's agents too Ibid., p. 404.

"The culture fed opportunities" Hansen.

"Resources are strained." Ibid.

"That truly baffles me" Senate Homeland Security Committee hearing, March 10, 2011. Originally broadcast on C-Span, available on YouTube: http://www.youtube.com/watch?v=w_VZ4GANG1o

"Frankly, most of our focus was on the outside intruder threat, not the inside threat" Ibid.

Manning described to Lamo how he used a combination of security tools Hansen.

"Lie to me," he had told Manning Ibid.

"Have a good day" "Court told of Bradley Manning 'link to WikiLeaks.'" BBC News, December 20, 2011.

"That's all there is to it!" Ellsberg, p. 426.

Try him in the press Ibid., p. 432.

The plan was scrapped G. Gordon Liddy. *Will: The Autobiography of G. Gordon Liddy* (New York: St. Martin's Press, 1980), p. 170.

"totally incapacitate" "Nixon White House Counsel John Dean and Pentagon Papers Leaker Daniel Ellsberg on Watergate and the Abuse of Presidential Power from Nixon to Bush." DemocracyNow.com, April 27, 2006.

unlucky protesters at the event's edges Ellsberg p. 451.

"The bizarre events have incurably infected the prosecution of this case" Wells, p. 556.

had himself been indicted on charges of conspiracy, obstruction of justice, and perjury Ellsberg, p. 456.

"enjoy a modicum of legal protection" Hansen.

"They touch my life, I touch their life, they touch my life again . . . full circle" Ibid.

Only a life sentence in a military prison "Court martial sought for suspected WikiLeaks leaker." Reuters, published on MSNBC.com, January 12, 2012.

protesting Manning's inhumane confinement in a Quantico, Virginia, military prison Video available on YouTube: http://www.youtube.com/watch?feature=player_embedded&v=Gq0CpWhVag4

Outside the base there, he staged another sit-in and was arrested again Ibid.

"I was Bradley Manning" Ashley Fantz. "Pentagon Papers leaker: 'I was Bradley Manning.'" CNN.com, March 19, 2011.

The president turns away, and the conversation is over Video available on YouTube: http://www.youtube.com/watch?feature=player_embedded&v=IfmtUpd4id0

The materials that Ellsberg leaked were actually of a *higher* top-secret classification Glenn Greenwald. "The intellectual cowardice of Bradley Manning's critics." Salon.com, December 24, 2011.

"I can't tell you how much that affected me." Fantz.

CHAPTER 2: THE CRYPTOGRAPHERS

one unit of data switching from a one to a zero or vice versa seemingly of its own accord Daniel S. Morrow. "Craig R. Barrett, Ph.D. Oral History." Computerworld Honors Program International Archives, October 24, 2002.

"He went off and did something wonderful" Ibid.

"Anonymous networks, digital pseudonyms, reputations, information markets, black markets, collapse of governments" Tim May. "The Crypto-Anarchist Manifesto." In Peter Ludlow, ed. *High Noon on the Electronic Frontier* (Cambridge: Massachusetts Institute of Technology, 1996), p. 239.

long-bearded hermit, living in a well-fortified redoubt in the mountains Thomas Fischermann. "Die Piraten des 21. Jahrhunderts." *Die Zeit*, December 4, 2003.

By 1996, Clipper was sunk Levy, p. 268.

Your name has come to our attention Tim May. "Introduction to BlackNet," in Ludlow's *High Noon,* p. 241.

report any contact with the shadowy organization Tim May. "Untraceable Digital Cash, Information Markets, and BlackNet." Talk at the Computers Freedom and Privacy conference, 1997.

"Classified classifieds," so to speak. "No More Secrets" Tim May. "BlackNet Worries," in ibid., p. 245.

CHAPTER 3: THE CYPHERPUNKS

"was in heaven" Stephen Muirhead. "MUMS the Word: Julian Assange, Wikileaks, and the Fight to End Government Secrecy." *Paradox,* August 15, 2010.

insisting that it be replaced with an image of an alien Ibid.

most physicists pathetically lugged about with pride and ignorance Julian Assange's blog at IQ.org, July 12, 2006 **(no longer online but mirrored at** http://aworldbeyondborders.com/research-raw-materials/julian-assange-writings/).

inaccurately, according to the department's staff Muirhead.

rolling over them and burying them alive Nicki Barrowclough. "Keeper of Secrets." *The Age,* May 22, 2010.

Assange invented a game: The Puzzle Hunt Muirhead.

Another conundrum involved factoring large numbers into primes Melbourne University Mathematics Society Puzzle Hunt 2004 Puzzles, available at http://www.ms.unimelb.edu.au/~mums/puzzlehunt/2004/puzzles.html

a secret about a secret that is veiled by a secret. Ibid.

"when you have to do something or you'll lose the game" Barrowclough.

"standing around looking pretty, even making tea" Muirhead.

Hello Puzzle Hunters Ibid.

a political version of the Puzzle Hunt, with great social implications Ibid.

"homemade nitroglycerin in the old cypherpunks blast shack has gone off" Bruce Sterling. "The Blast Shack." Webstock.org.nz, December 22, 2010

archival footage of Hiroshima Cryptome.org, April 2011 archive, available at http://cryptome.org/cryptomb29.htm

immigration papers for Barack Obama Sr. Ibid.

Wau Holland Foundation Ibid.

"Don't believe anything you see there" Cryptome.org privacy policy, available at http://cryptome.org/other-stuff.htm

maneuvers by Microsoft to remove his site from the Internet in 2010 Ryan Singel. "Microsoft Takes Down Whistleblower Site, Read the Secret Doc Here." Wired.com, February 24, 2010.

"Well, I'm actually looking for that information right now" Michael Crowley. "Let's Shut Them Down. These websites are an invitation to terrorists." *Reader's Digest,* March 2005. Reproduced at http://cryptome.org/Web-threats.htm

all while periodically stomping around the room Dreyfus and Assange, *Underground.*

***splendide mendax*, the "nobly untruthful" in Horace's Odes** Raffi Khatchadourian. "No Secrets." *The New Yorker,* June 7, 2010.

Assange was determined to access Minerva Dreyfus and Assange.

"Yes, it's L-U-R-C-H—full stop." All the above comes from ibid.

"living in a bikini" and "going native" "Julian Assange's Mother Recalls Magnetic." *Magnetic Times,* August 7, 2010.

opossums ran across their beds in the dark George Hirst. "Christine Assange Recalls Her Magnetic Island Days." *Magnetic Times,* August 31, 2011.

"There was a sense of safety and security" Ibid.

"I wasn't sorry to leave when presented with the dental bills of my tormentors" Assange, blog at IQ.org, July 18, 2006.

fifteen different towns and at least as many schools, when he attended school at all Dreyfus and Assange.

"get out of politics" or risk being seen as an "unfit mother" Hans Ulrich Olbrist. "Interview With Julian Assange, Part I." *E-Flux,* May 2011.

"Chess is very austere, in that you don't have many rules, there is no randomness, and the problem is very hard" Khatchadourian.

Therefore its readership remained at three Dreyfus and Assange.

"to enter the depths of the Pentagon's Eighth Command at the age of seventeen was a liberating experience" Hans Ulrich Obrist.

"and share information" Dreyfus and Assange.

hide his location and identity by routing his modem's phone traffic through that intermediary Ibid.

Mendax's career was over All the above in this passage comes from ibid.

"a cross between a mutter and the Oracle of Delphi" Richard Rosenkranz. *Across the Barricades* (New York/Philadelphia: J.B. Lippincott, 1971), p. 179.

"the Avery Commune was once again a functioning organism" Ibid.

"I approached a condition of human relationships that can usually be found only in the realm of ideas" Ibid., p. 44.

"I think my childhood was just great" Ibid.

"We're prepared to start right now" John Cook. "Secrets + Lies." *Radar*, August 2007.

before he could call his fellow hackers to warn them that he had tipped off the telecom's security Dreyfus and Assange.

"I am not concerned about using my skills there" All the above in this passage from ibid.

Scientologists believed in communication with plants Andrew Fowler. *The Most Dangerous Man in the World* (Melbourne: Melbourne University Press, 2011), p. 26.

"True belief only begins with a jackboot the door" Assange's blog at IQ.org, July 17, 2006.

one demanding user a "dummy" and tells him to "get a life" E-mail from Julian Assange to the Cypherpunk Mailing List, December 24, 1995.

"some research is in order before you go shooting off your mouth" E-mails from Julian Assange to the Cypherpunk Mailing List, January 14, 1996.

"afterschool Tupperware get-together" Ibid., December 30, 1995.

"Your testical, [sic] again Nancy?" and "National Gay Secrecy Unit" Ibid., February 3, 1996.

"The Internet is, by its very nature a censorship free zone" Ibid., December 17, 2003.

Eleven people showed up Fowler, p. 26.

one user with the Penet pseudonym "an144108" Sabine Helmers. "A Brief History of anon.penet.fi, The Legendary Anonymous Remailer." *Computer-Mediated Communication Magazine*, September 1997.

"All of them," answered Jim Jim Bell. "Assassination Politics," available at http://cryptome.org/ap.htm

botched a series of deals "How DigiCash Blew Everything." *NEXT*, January 1999, available in translation from Dutch here: http://cryptome.org/jya/digicrash.htm

It would be an encrypted, anonymous, digital dead pool Bell.

No military? Ibid.

put out anonymous hits on criminals just as easily as politicians Ibid.

murder those who annoy us sufficiently E-mail from anon-remailer@utopia.hacktic.nl to the Cypherpunk Mailing List, January 27, 1996.

"Others won't" E-mail from Jim Bell to the Cypherpunk Mailing List, January 26, 1996. (The seeming date discrepancy between Bell and the anonymous cypherpunk is caused by time zone differences.)

"I am out to 'get' the government" Ibid., January 29, 1996.

by resorting to violence you are no better than the ones you purport to protect us against E-mail from Jim Choate to the Cypherpunk Mailing List, February 6, 1996.

Are you a statist? E-mail from Jim Choate to the Cypherpunk Mailing List, February 10, 1996.

the e-mail that followed his BlackNet experiment more than three years earlier May in "BlackNet Worries."

leaked data in all directions Wim van Eck. "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" *Computer & Security*, December 1985. Republished at http://cryptome.org/jya/emr.pdf

water pipes and sprinkler system around a computer might propagate its electric field and spill its data even further E-mails from Jim Bell and Julian Assange to the Cypherpunk Mailing List, May 29, 1996.

"knowing that reasonable people will think you're a nut seeking celebrity martyrdom" E-mail from John Young to the Cypherpunk Mailing List, February 11, 1996.

"I may be one of the system's first victims" E-mail from Jim Bell to the Cypherpunk Mailing List, February 11, 1996.

federal agents who seized his computers, his car, three assault rifles, and a .44 Magnum handgun "Criminal complaint against Jim Bell," May 16, 1997, available at http://cryptome.org/jya/jimbell3.htm

find its way into the building's computers and short out their wiring Ibid.

dumping a chemical called mercaptan on the rug outside an IRS office in Vancouver, Washington Ibid.

"They are all either crooks or they tolerate crooks or they are aware of crooks among their numbers" Declan McCullagh. "Crypto-Convict Won't Recant." Wired.com, April 14, 2000.

where he spent his days demolishing computer monitors for forty-six cents an hour Declan McCullagh, "Jim Bell Update." Wired.com, May 25, 2002.

a groundbreaking work in "government accountability systems" Letter from John Young to Vikki Hardy, July 11, 1998, available at http://cryptome.org/jya/chrysler98.htm

"Jim Bell . . . lives . . . on . . . in . . . Hollywood!" E-mail from Julian Assange to the Cypherpunk Mailing List, January 9, 1998.

He called it Marutukku E-mail from Julian Assange to Firewalls Mail List, June 4, 1997.

at the Chaos Communication Congress, December 2005, available here: http://events.ccc.de/congress/2005/fahrplan/events/478.en.html

installed a red lightbulb in his bedroom in an effort to regulate his sleep Barrowclough.

activists who would crash in the house rent-free in exchange for working on Assange's project Khatchadourian.

accept unencrypted documents by post and even scan in reams of paper submissions and convert them to text files E-mail from Julian Assange to WikiLeaks developer list, December 13, 2006, available at http://cryptome.org/wikileaks/wikileaks-leak.htm

"Yes, the guy running the exit node can read the bytes that come in and out there" Bruce Schneier. "Lesson from Tor Hack: Anonymity and Privacy Aren't the Same." Wired.com, September 20, 2007.

a member of the project who ran a Tor exit node had noticed Chinese hackers using the relay to hide their tracks Khatchadourian.

"Somewhere between none and a handful of those documents were ever released on WikiLeaks" John Leyden. "Wikileaks denies Tor hacker eavesdropping gave site its start." TheRegister.co.uk, June 2, 2010.

"When they pull, so do we" E-mail from Julian Assange to John Young, January 7, 2007, available at http://cryptome.org/wikileaks/wikileaks-leak2.htm

thirty times the size of every text article stored on Wikipedia Wikipedia: Database download, available at http://en.wikipedia.org/wiki/Wikipedia:Database_download

"let it flower into something new" Julian Assange to John Young, January 7, 2007, available at http://cryptome.org/wikileaks/wikileaks-leak2.htm

spreading free software like a hacker Johnny Appleseed Jacob Appelbaum. "Personal experiences bringing technology and new media to disaster areas." Speech at the Chaos Communication Congress, December 2005, available here: http://events.ccc.de/congress/2005/fahrplan/events/478.en.html

"As an American, I found myself feeling pretty awful about what we'd contributed to" Ibid.

grabbed the remote, turned up the volume, and refused to change the channel Ibid.

A man beaten in the shower. Nightly curfews, women raped. Xeni Jardin interview with Jacob Appelbaum. "Katrina: 'Rape, murder, beatings' in Astrodome, say evacuees." BoingBoing.net, September 7, 2005.

"The same thing, over and over again. The disconnection. The lack of humanity." Jacob Appelbaum. "Personal experiences bringing technology and new media to disaster areas." Speech at the Chaos Communication Congress, December 2005, available here: http://events.ccc.de/congress/2005/fahrplan/events/478.en.html

transfer the equivalent of $50,000 from a bank to the CCC's accounts Steve Kettman. "Tribute to Hippie Hacker Holland." Wired.com, July 31, 2001.

even when authorities are standing over the user, rubber hose in hand, demanding the key Jacob Appelbaum. "A discussion about modern disk encryption systems." Speech at the Chaos Communication Congress, December 2005, available here: http://events.ccc.de/congress/2005/fahrplan/speakers/165.en.html

"Justice was just too slow to catch you" Ibid.

The handbooks of secret rituals for nine different fraternities All of these are available at the WikiLeaks.org archive: http://www.wikileaks.org/wiki/Category:Analyses.

"smearing and stinging by governments, corporations, persons of all demonics" E-mail from John Young to the WikiLeaks developer mail list, December 20, 2006, http://cryptome.org/wikileaks/wikileaks-leak.htm

"Or is it a clever smear by US intelligence?" "Inside Somalia and the Union of Islamic Courts." WikiLeaks.org, available at http://wikileaks.org/wiki/Inside_Somalia_and_the_Union_of_Islamic_Courts

reports of currency counterfeiting by the regime's organized crime connections Xan Rice. "The looting of Kenya." *The Guardian*, August 30, 2007.

indiscriminate police killings of thousands of young men "Oscar Foundation letter to Minister for Internal Security over extra-judicial killings in Kenya." WikiLeaks.org, October 14, 2008, available here: http://wikileaks.org/wiki/Oscar_Foundation_letter_to_Minister_for_Internal_Security_over_extra-judicial_killings_in_Kenya,_14_Oct_2008.

tax shelters administered by the Swiss Bank Julius Baer "Bank Julius Baer." WikiLeaks.org, available here: http://wikileaks.org/wiki/Bank_Julius_Baer

dumping in the Ivory Coast that had been legally prevented from appearing in British media "Ivory Coast toxic dumping report behind secret Guardian gag." WikiLeaks.org, October 13, 2009 available here: http://wikileaks.org/wiki/Ivory_Coast_toxic_dumping_report_behind_secret_Guardian_gag

Icelandic banking documents that would catalog the country's financial meltdown "Financial collapse: Confidential exposure analysis of 205 compa-

nies each owing above EUR45M to Icelandic bank Kaupthing." WikiLeaks.org, September 26, 2008 available at http://wikileaks.org/wiki/Financial_collapse:_Confidential_exposure_analysis_of_205_companies_each_owing_above_EUR45M_to_Icelandic_bank_Kaupthing,_26_Sep_2008

And a collection of pager messages from September 11, 2001 "9/11 tragedy pager intercepts." WikiLeaks.org, available here: http://911.wikileaks.org/

would catch the attention of one young analyst in a dusty base in Iraq Hansen.

"Wikileaks will release several thousand additional pages of Scientology material next week" "Scientology threatens WikiLeaks over secret cult bibles." WikiLeaks.org, April 7, 2008. No longer online but available at http://Web.archive.org/Web/20080704235334/https://secure.wikileaks.org/wiki/Scientology_threatens_Wikileaks_over_secret_cult_bibles

one of the largest collections of the church's internal documents stored anywhere in the world. WikiLeaks archive: http://www.wikileaks.org/wiki/Category:Analyses

CHAPTER 5: THE PLUMBERS

Note: Much of the material for this section regarding HBGary Federal and Aaron Barr came from AnonLeaks, a website created to publish the hacked e-mails of the employees of HBGary and HBGary Federal. The site no longer exists, and given that I no longer consider the documents taken from that site to be public, I've treated them as my own reporting and haven't cited them below.

it put the first five GPS satellites into orbit Duncan Graham-Rowe. "Fifty years of DARPA: Hits, misses and ones to watch." New Scientist.com, May 15, 2008.

developed and flew the first stealth planes Ibid.

organized a series of races of robotic, driverless cars through the desert Ibid.

driven between San Francisco and Los Angeles with no human assistance "Google Cars Drive Themselves, in Traffic" *The New York Times*, October 9, 2010.

build flying Humvees Clay Dillow. "DARPA's 'Flying Humvee' Is Moving Ahead, Ready for Prototype." Popsci.com, October, 25, 2011.

mechanical bats that can suck electricity from power lines Jonathan Fahey. "How to Build a Spy Bat." Forbes.com, June 26, 2009.

cyborg cockroaches Travis Korte. "Cyborg Insect Breakthrough: Generating Power Through Body Chemistry." HuffingtonPost.com, January 8, 2012.

roving robots that can switch between liquid and solid form Anne-Marie Corley. "iRobot's Shape-Shifting Blob 'Bot Takes Its First Steps." IEEE Spectrum, October 13, 2009.

roving robots that can feed themselves with grass and twigs Noah Shachtman. "Company Denies Its Robots Feed on the Dead." Wired.com, July 17, 2009.

Iron Man–like exoskeletons that multiply human strength by a factor of ten Larry Greenemeier. "Real-Life Iron Man: A Robotic Suit That Magnifies Human Strength." *Scientific American,* April 30, 2008.

surveillance systems designed to watch every moving object in entire cities Noah Shachtman. "Darpa's Far-Out Dreams on Display." Wired.com, March 15, 2004.

"might already have on their hands the blood of some young soldier" Adam Levine. "Top military official: WikiLeaks founder may have 'blood' on his hands." CNN.com, July 29, 2010.

said that the exposure hadn't led to any documented casualties Ellen Nakashima. "Pentagon: Undisclosed Wikileaks documents 'potentially more explosive.'" Washingtonpost.com, August 11, 2011.

another fifteen thousand civilian deaths that hadn't been previously documented "Iraq War Logs: What the numbers reveal." Iraqbodycount.org, October 23, 2010.

Nouri al-Maliki used "detention squads" in the Iraqi army to harass political rival groups Gregg Carlstrom. "Nouri al-Maliki's 'detention squad.'" Al Jazeera, October 24, 2010.

claiming it violated the company's terms of service David Leigh and Rob Evans. "WikiLeaks says funding has been blocked after government blacklisting." *The Guardian*, October 14, 2010.

"Saudi Arabia Urges US Attack on Iran to Stop Nuclear Programme" Ian Black and Simon Tisdall. *The Guardian,* November 28, 2010.

"China leadership 'orchestrated Google hacking'" BBC.co.uk, December 4, 2010.

"Did Pfizer Bribe Its Way Out of Criminal Charges in Nigeria?" Walter Armstrong. TheAtlantic.com, December 27, 2010.

"Texas Company Helped Pimp Little Boys To Stoned Afghan Cops" John Nova Lomax. HoustonPress.com, December 7, 2010.

"China 'ready to abandon North Korea'" Simon Tisdall. *The Guardian.* November 29, 2010.