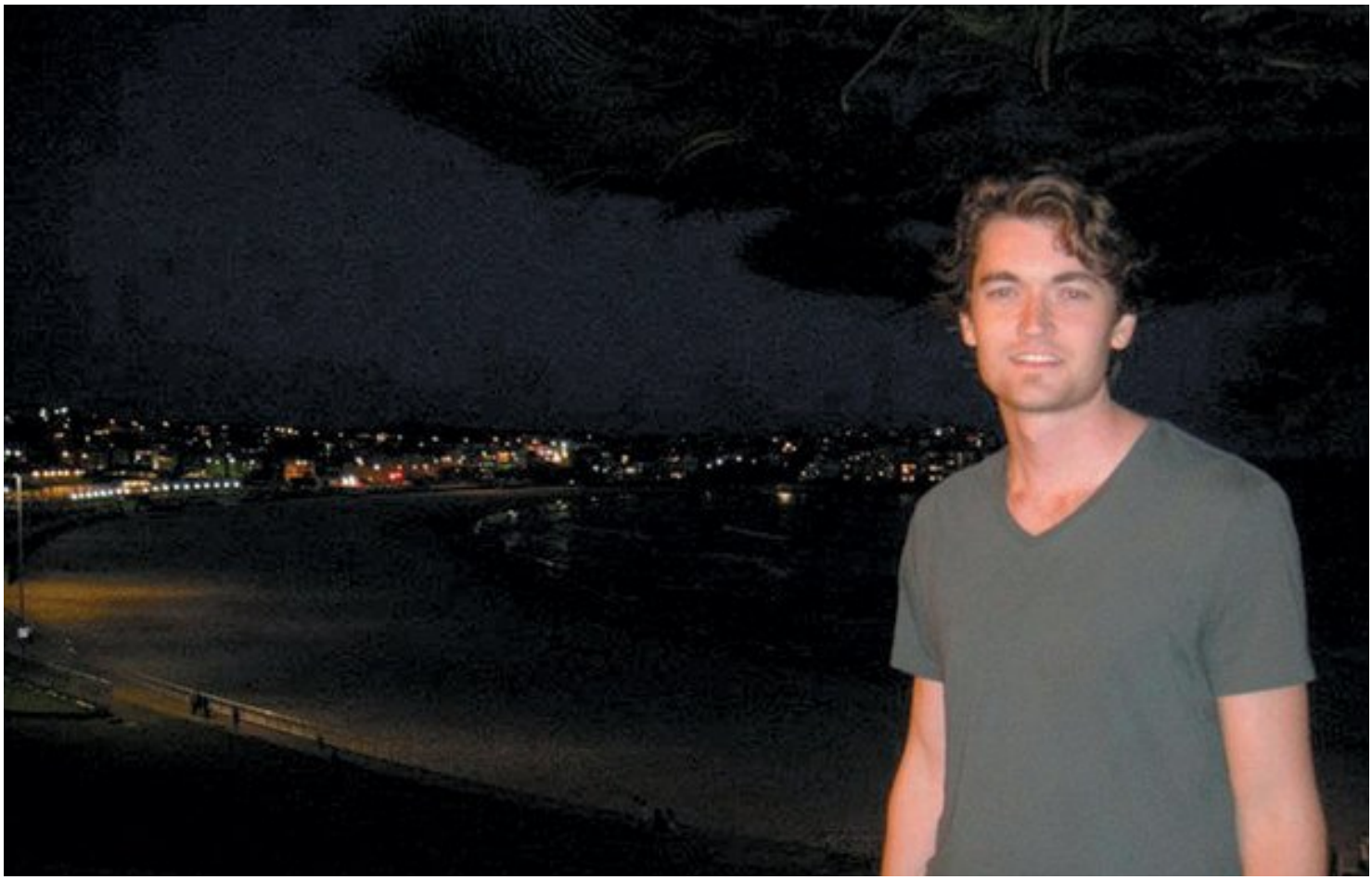
In the Depths of the Net

Sue Halpern

OCTOBER 8, 2015 ISSUE

The Dark Net: Inside The Digital Underworld
by Jamie Bartlett
Melville House, 308 pp, $27.95



freeross.org

Ross Ulbricht, who was recently sentenced to life in prison for running the illegal dark-Net marketplace Silk Road

Early this year, a robot in Switzerland purchased ten tablets of the illegal drug MDMA, better known as "ecstasy," from an online marketplace and had them delivered through the postal service to a gallery in St. Gallen where the robot was then set up. The drug buy was part of an installation called "Random Darknet Shopper," which was meant to show what could be obtained on the "dark" side of the Internet. In addition to ecstasy, the robot also bought a baseball cap with a secret camera, a pair of knock-off Diesel jeans, and a Hungarian passport, among other things.

Passports stolen and forged, heroin, crack cocaine, semiautomatic weapons, people who can be hired to use those weapons, computer viruses, and child pornography—especially child pornography—are all easily obtained in the shaded corners of the Internet. For example, in the interest of research, Jamie Bartlett—the author of *The Dark Net: Inside the Digital Underworld*, a picturesque tour of this disquieting netherworld—successfully bought a small amount of

marijuana from a dark-Net site; anyone hoping to emulate him will find that the biggest dilemma will be with which seller—there are scores—to do business. My own forays to the dark Net include visits to sites offering counterfeit drivers' licenses, methamphetamine, a template for a US twenty-dollar bill, files to make a 3D-printed gun, and books describing how to receive illegal goods in the mail without getting caught. There were, too, links to rape and child abuse videos. According to a study released a few years ago, 80 percent of all dark-Net traffic relates to pedophilia.

The standard metaphor for explaining the dark Net's relation to the Internet is the familiar iceberg. The towering spire, looming above the water, is the Internet that we navigate daily when we use a search engine like Google or type in a Web address. Underneath it, massive and ghostly, is its sinister consort, the dark Net. But that's not quite accurate. There is a tremendous amount of quotidian Internet traffic, like online banking and medical record-keeping, that is intentionally and appropriately kept out of sight, locked away in secure databases, protected by passwords or tucked behind paywalls, none of it nefarious or unlawful. This is what is known as "the deep Web," and by some estimates it is five hundred times larger than the "surface Web"—the Web of Amazon and YouTube and Twitter and Tumblr.

It is within the deep Web that the dark Net (or the dark Web) resides. It is comprised of sites without standard Web addresses, addresses that are not indexed and often not fixed, so that only those who know them can find them. And because these sites are hard to discover, the dark Net is home to a whole range of illicit and covert activities. As Bartlett puts it in the obliquely sympathetic way typical of his book, "Terrorists, extremists, serious organized criminals, and child pornographers, denied mainstream channels, are often early adopters of new technology and also have an incentive to stay secret and hidden."

Secret and hidden are the hallmarks of the dark Net, for while it is possible to use Google to find sites on the surface Web that sell cannabis by the pound (www.marijuanaonline 007.com), guns without a federal firearms license (www.gunbroker.com), and stolen credit card data (www .tomsguide.com/us/how-to-buy-stolen-credit-cards,news-18387.html), and while Bartlett himself introduces readers to a trio of young women who perform sex acts via webcam for money (as he sits a few feet away) on an easily accessible site called Chaturbate, anyone who engages with these businesses leaves a trail that can be easily tracked. What makes the dark Net especially attractive to people who would subvert the law is that it promises—and most often delivers—anonymity to buyers and sellers, as well as to anyone else who wants to be unobserved. This could include, for example, whistleblowers, activists, terrorists, and citizens of authoritarian regimes aiming to bypass their censors.

To reach a dark-Net address, one must log onto one of the small number of Web browsers that conceal both identity and location, the most popular of which is called Tor. Developed by the United States Naval Research Laboratory to provide a safe way for dissidents in repressive regimes to communicate online, Tor continues to be funded in part by the US government through the National Science Foundation, as well as by a number of civil liberties organizations. Built on top of the Firefox Web browser, anyone, anywhere, can download the Tor browser and use it to navigate the entire Internet—the surface, the deep, and the dark Web—and do so leaving no trace. As Andrew Lewman, the executive director of the Tor Project, described it to the BBC last year:

> The Tor Network is a network of about 6,000 relays, which are servers spread around 89 countries or so. And what we do is relay your traffic through three of these relays in sort of a random order, so that where you are in the world is different to where you appear to come from. So you know you are sitting here in the UK, you start up the Tor browser. You could pop out from Japan, Argentina, the United States.

In addition to the Tor browser, Tor also runs something called Tor Hidden Services, which essentially scrambles the address of a website, to make it undetectable. To connect to a hidden service, users are sent to a "rendezvous" point somewhere else on the Internet, and in so doing neither they, nor the site they are seeking, knows the other's network identity. This works fine when the user knows how to direct the computer to the site with which to rendezvous, but given the proliferation of sites using Tor Hidden Services—Bartlett estimates that there are 40,000–60,000 of them—their fluidity, and their typically obscure addresses containing digits and letters, they can be hard to find.

While that may be the point, all this secrecy makes it difficult to conduct business, so a few enterprising souls have

come up with various ways to help users make their way in the dark. These include a search engine called Grams that looks nearly identical to Google (same font, same color scheme, same "I'm feeling lucky button") and that guides users to thousands of illegal drug sellers all over the world; the Hidden Wiki, a compendium of information in the spirit of Wikipedia that directs users to obscure dark-Net locales, but especially, it would seem, to sites devoted to pedophilia; and a number of dark-Net malls, some that could be described as department stores of contraband, and others that are devoted to particular kinds of goods: the Alpha Bay for stolen credit cards, the Got Milk Pharmacy for drugs, and the Real Deal Market for hacking instruments.

By far the best-known dark-Net marketplace was the Silk Road, a bazaar of drugs and illegal services including, apparently, murder-for-hire, that was shut down by the FBI in 2013, and whose founder, thirty-one-year-old Ross Ulbricht, was sentenced in May to life in prison without the possibility of parole. Silk Road did not sell crack, cyanide, or anything else itself. Rather, it connected buyers and sellers and took a cut of the transactions. It is estimated that Ulbricht, an unassuming former Eagle Scout who lived in a shared apartment in San Francisco and ran his business out of public libraries and coffee shops, was making around $20,000 a day, while the site itself, which began operating in 2011, generated, all told, an estimated $1.2 billion. According to *The New York Times*, citing government investigators:

> During Silk Road's nearly three years of operation, more than 1.5 million transactions were conducted on the site, involving over 100,000 buyer accounts and nearly 4,000 vendor accounts…. At the time of its closing, the site listed more than 13,000 offerings of illegal drugs.

Prior to sentencing, Ulbricht's lawyers argued that by moving drug sales off the street to a dark-Net Amazon-like marketplace where buyers could rate sellers,

> transactions on the Silk Road web site were significantly safer than traditional illegal drug purchases, and included quality control and accountability features that made purchasers substantially safer than they were when purchasing drugs in a conventional manner.

Jamie Bartlett, who bought his cannabis from a Silk Road vendor, echoes the defense when he writes:

> Online drugs markets are transforming the dirty business of buying drugs into a simple transaction between empowered consumers and responsive vendors…. The real secret of dark net markets is good customer service.

The judge, however, resoundingly rejected this line of reasoning, calling it "a privileged argument and…an argument made by one of the privileged" before handing down a sentence that was remarkably harsher than the harsh sentence requested by the prosecution.

When he was arrested, Ulbricht was said to be worth about $30 million, though none of his money was denominated in legal tender. Instead, his wealth was sequestered online in bitcoins, the dark Net's currency of choice, since it veils users, much like the dark Net itself. As Bartlett describes it:

> A Bitcoin is nothing more than a unique string of numbers. It has no independent value, and is not tied to any real-world currency. Its strength and value come from the fact that people believe in it and use it. Anyone can download a Bitcoin wallet on to their computer, buy Bitcoins with traditional currency from a currency exchange, and use them to buy or sell a growing number of products or services as easily as sending an email. Transactions are secure, fast, and free, with no central authority controlling value or supply, and no middlemen taking a slice.

In 2009, when the first bitcoin transaction took place, a single bitcoin was worth less than half a penny. By April 2013, its value had risen more than 9,999,900 percent, to $100. Then, in November of that year, after a Senate Homeland Security Committee hearing, which was described by the press as a "lovefest" between officials from the federal government and representatives of the bitcoin community, the value of a single bitcoin rose to an astronomical $1,023. Since then it has incrementally decreased to about $280 today, even as a growing number of conventional retailers in the United States and Europe have begun accepting bitcoins as payment for real goods, including Overstock, Microsoft, and Dell in the United States, Monoprix in France, and AirBaltic in Latvia, to name just a few. By the end of the year,

Barclays Bank in the UK will begin accepting deposits in bitcoins.

Even so, there is a way in which bitcoin, which is fundamentally a concept—an idea rooted in pure numbers rather than pegged to a physical asset like gold or silver—does not exist, at least not in the material world. That explains why, during that Homeland Security Committee hearing in 2013, Senator Thomas Carper called it a "virtual" currency. To quote him directly: "Virtual currencies, perhaps most notably bitcoin, have captured the imagination of some, struck fear among others and confused the heck out of the rest of us."

Newsha Tavakolian/Magnum Photos

A billboard honoring Kurdish women soldiers who died while fighting ISIS, Rojava, northern Syria, 2015

That confusion arises in large part because bitcoin is based on an obscure mathematical formula developed by someone—or someones, it's never been determined—going by the name Satoshi Nakamoto. Each bitcoin is created, or "mined," by those who can provide the considerable computing powers to validate bitcoin transactions and ensure their security through a cryptographic function that produces a unique digital fingerprint for each one. (It's an intensive process; special hardware is needed; the total number that can be mined has been capped by Satoshi at 21 million.) In the initial white paper outlining the bitcoin system published in 2008, Satoshi defines it as

> a purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution.

The intention was not to create a payment system that was ideal for the dark Net but, rather, to create a payment system that did not rely in any way on trust. It just happened that they were the same thing.

When the FBI seized the bitcoin computer accounts (called "wallets") that they believed to be Ross Ulbricht's, they were not completely certain that the accounts belonged to him. That is because bitcoins are almost always purchased and held under false names. Though the address of every bitcoin transaction is posted online in a public ledger called a "block chain," those addresses look something like this: 1JArS6jzE3AJ9sZ3aFij1BmTcpFG gN86hA. Unless a block chain address can be linked to an individual, that person will remain unknown, even though the transaction is not. Bitcoin patrons are advised to use different addresses for each transaction so those transactions are less likely to be associated with a single person. As one explanatory website puts it, this is "the equivalent of writing many books under different pseudonyms."

But pseudonymous is not the same as anonymous: once the FBI was in possession of Ulbricht's computer, its agents found 144,000 bitcoins stored in his bitcoin wallets, as well as the digital keys to unlock them. From there they were able to trace all of his activities on the public ledger. As *Wired*'s Andy Greenberg observed after FBI agent Ilhwan Yum testified at the Silk Road trial, "If anyone still believes that bitcoin is magically anonymous internet money, the US government just offered what may be the clearest demonstration yet that it's not."

Still, bitcoin remains the currency of choice for dark-Net commerce and its offshoots. In July, the *Times* ran a story with the headline "For Ransom, Bitcoin Replaces the Bag of Bills," noting how cybercriminals, especially, are partial to payments in the cryptocurrency. And it's not just underworld hackers who are keen on bitcoin. A year ago a blogger going by the name "AmreekiWitness" (American witness) urged members of the Islamic State—many of whom already communicate on hidden dark-Net sites—to use the cryptocurrency, and offered instructions on how to do that. A bitcoin donation system, he wrote, "could send millions of dollars worth of Bitcoin instantly from the United States, United Kingdom, South Africa, Ghana, Malaysia, Sri Lanka, or wherever else right to the pockets of the mujahideen."

But this, it turned out, was aspirational. In an exchange with a writer named Zubair Muadh on the website deepdotweb.com, AmreekiWitness, when asked if the Islamic State accepted bitcoins, said that it did not. That was last September. Nine months later, the FBI unmasked and arrested AmreekiWitness, who turned out to be a seventeen-year-old computer-savvy high school student in Virginia and ISIS supporter who had facilitated the journey of an eighteen-year-old friend from the United States to Syria to join the Islamic State. In August he was sentenced to eleven years in federal prison.

If ISIS is not yet using bitcoin, the prospect that it will in the near future worries Jennifer Calvery, the head of the US Treasury Department's Financial Crimes Enforcement Network. As she told a *Foreign Affairs* forum on cryptocurrency policy last February:

> What keeps me up at night when I am thinking about digital currencies…the real threats out there,… these days… we're thinking a lot about ISIL…. How they're moving their money, and how potential US-based individuals are becoming foreign fighters: Are they moving their money, can we identify them by the movement of their money? And what does it mean if they start moving that money through Bitcoin?

Even without the subterfuge of bitcoin, terrorists have become avid, if not sophisticated, digital natives. In its investigation "Jihadism on the Web," the General Intelligence and Security Service of the Netherlands (AIVD) found several hundred jihadist websites and Internet forums worldwide, most of them on the dark Net. These, the report's authors declared, are "the *de facto* core of the global virtual Jihad movement, propelling it like a turbo." This was in 2012, before the Islamic State assumed its current form. Two years later ISIS was operating between 46,000 and 70,000 Twitter accounts, which it used for recruitment and propaganda. The group also had developed its own Twitter application, "Dawn of Good Tidings," to provide adherents with the latest jihadi news while, in addition, giving ISIS leaders the ability to send tweets through users' personal accounts. (Though dropped from the Google Play Store, the app still can be loaded onto Android phones.)

As novel as these uses of the Internet might seem, it's important to put them into perspective. The Internet long has been home to extremists of every stripe who have used it to disseminate and amplify their message. In the 1980s and 1990s, before the invention of social media, and before even the creation of the World Wide Web, white supremacist

groups like the Aryan Brotherhood and Stormfront figured out how to use bulletin board systems and Usenet groups to communicate with and rally members. Since then, as Bartlett reports, the Stormfront website storm front.org "hosts a long-standing forum, which has close to 300,000 members, who between them have posted close to ten million messages." Moreover, a study of terrorism on the Internet from 2003–2004 by the United States Institute for Peace found that

> all active terrorist groups [worldwide] have established their presence on the Internet…[employing it for] psychological warfare and propaganda [and] highly instrumental uses such as fundraising, recruitment, data mining, and coordination of actions.

Extremists and terrorists, in other words, use the Internet like everyone else. If, in the very early days of the Internet, their activities were largely obscure, it was because the technology itself was largely obscure. If those activities are opaque now, it is because they have been deliberately moved to the dark Net. As the Brookings Institute researcher J.M. Berger told a Senate hearing on social media and terrorism in May, once a potential recruit who has connected with ISIS on an open forum like Twitter or Facebook has expressed serious interest in taking the association further, the conversation usually moves to a more secure venue via one of the widely available and popular private messaging apps like Kik or WhatsApp, which are encrypted. Senator Ron Johnson asked Berger for clarification:

> *Johnson*: Our authorities can follow the open source social media, but the minute those individuals who are really serious about it go offline, we go dark? We lose our capability of following that and we really have no idea? Is that correct?
>
> *Berger*: Well, you can approach it with subpoena and other authorities….
>
> *Johnson* (interrupting): If we can decrypt. That's part of the problem, isn't it? And Silicon Valley is resistant to allowing us to decrypt, and even if they were to allow it, there would be other sites offshore that will also encrypt. So we are losing our capability of being able to follow this.
>
> *Berger*: Yes….

This exchange was reiterated a few weeks later during another congressional hearing, when Homeland Security Committee Chair Michael McCaul was questioning Michael Steinbach of the FBI's counterterrorism division:

> *McCaul*: I've read some of these Twitter accounts and Tweets, they have thousands of followers and thousands following, which means they are actively communicating…and then they go into messaging. And then they go into a more secure space that if we have coverage, we can pick up that communication, but as you suggested in your testimony, then they have the ability to go onto what's called "dark space," to another platform that is secure-comm, that we don't have the ability to monitor…. Is that correct?
>
> *Steinbach*: That is correct, sir.

One month later, at yet another congressional hearing, this one of the Senate Intelligence Committee, Steinbach's boss, FBI Director James Comey, stated flatly that Internet encryption was a public menace, arguing that the privacy rights established by the Fourth Amendment were not absolute. Then he asked for something fourteen of the world's leading cryptographers and computer scientists said was impossible in a study issued just the day before: a back door that would give law enforcement a way to decipher encrypted communications that would not, at the same time, compromise encryption more generally. "A whole lot of good people have said it's too hard," Comey told the senators, "but my reaction to that is: I'm not sure they've really tried."

Until the mid-1970s, encrypted messages were deciphered using a single key shared by both sender and receiver. This was its weakness. Not only did the message need to be transmitted, so did the method of decoding it. Then, in 1976, a team of mathematicians at MIT invented a much more robust two-key encryption system, where a public key was used to scramble the message and a private key was used to unscramble it, making strong, end-to-end encryption possible.

Nearly two decades later, an antinuclear activist named Phil Zimmermann employed the public key protocol when he created the e-mail encryption program Pretty Good Privacy (PGP) to shield his group's messages from the prying eyes of the government. While PGP itself has gone through many iterations since then, Pretty Good Privacy remains a popular way to protect e-mails.

This was the program Edward Snowden required Glenn Greenwald to use before the whistleblower would communicate with the journalist, and the one many people installed on their computers after Greenwald revealed that the National Security Agency was collecting and reading the private electronic correspondence of ordinary citizens. And it was not only e-mail encryption they were downloading. According to Bartlett:

> The daily adoption rate of PGP keys tripled in the months following Snowden's revelations. Anonymous browsers like "Tor" are becoming ever-more popular: there are now an estimated 2.5 million daily users.

Bartlett calls this "The Snowden Effect."

The other Snowden effect, this one pitched by members of Congress, the intelligence services, and the Obama administration, among many others, is that the Snowden leaks drove terrorists to use encrypted communications. This is their rationale for eliminating encryption—the position, for example, of British Prime Minister David Cameron—or for creating the back door FBI Director Comey is after. In fact, as Glenn Greenwald has reported in *The Intercept*, Islamic terrorists have been using encryption and other dodges since at least 2002. Greenwald cites a document seized by British authorities and called by them "The Jihadist Handbook," which details these methods.

Simple math suggests that the majority of people adopting encryption or using an anonymizing browser, post-Snowden, are neither terrorists, extremists, drug dealers, nor pedophiles. The problem for law enforcement may not be that more terrorists are going dark, but that an increasing number of regular folk are, crowding that space and making the work of discerning bad guys from good much more labor-intensive.

Meanwhile, Silicon Valley, which was implicated in the leaked NSA documents as being a party to government mass surveillance, is trying to repair its image and regain customer trust and business by moving to strong encryption in both software and hardware. Google, for example, is adding end-to-end encryption to the traffic flowing between its data centers, Facebook is offering users the opportunity to add PGP to their messages, and IBM is encouraging buyers of its mainframe computers to install their own encryption programs, putting the company at an unreachable distance from customer data, should the NSA or FBI or GCHQ seek it.

The virtue of strong encryption—encryption that offers no back door—goes beyond a service provider such as Google being able to demur when the government comes calling. Strong encryption is one of the best defenses against online hacking. This summer's hack of the now infamous adultery site Ashley Madison, which saw the unencrypted data of its more than 32 million members dumped onto the dark Net, is a good example. The private nature of this material, which includes not only home addresses and phone numbers but also intimate details about sexual proclivities, made it ideal for blackmail and extortion. Within days, e-mails threatening exposure were being sent to people whose names were found in the cache, demanding a payment in bitcoins to be delivered to a dark-Net address.

Similarly, the Office of Personnel Management (OPM) revealed in June that data on 4.2 million government workers had been stolen from its computers (ostensibly) by the Chinese. If that information—as well as information on another 21.5 million people that the agency admitted in July had been stolen—had been encrypted, it would be of little value. Instead, it may be used to identify covert intelligence agents and to gather compromising evidence on government workers. According to a report in the *Los Angeles Times*, Russian and Chinese operatives have begun aggregating and cross-indexing the OPM and Ashley Madison data to get an even more detailed and comprehensive picture of US intelligence operations and of persons vulnerable to exploitation and manipulation. According to the *Times*, one clandestine team working with US spies has already been exposed.

A door, whether in the back, the front, or the side, is still a door; open it for the good guys, and the bad guys are going to push on it, too. This may happen surreptitiously—no doubt a back door would be a target for hackers—but also overtly, with equally disastrous consequences. This was made clear in a letter recently delivered to President Obama by

representatives of major technology companies and civil liberties groups. “If American companies maintain the ability to unlock their customers’ data and devices on request,” they wrote,

> governments other than the United States will demand the same access, and will also be emboldened to demand the same capability from their native companies. The US government, having made the same demands, will have little room to object. The result will be an information environment riddled with vulnerabilities that could be exploited by even the most repressive or dangerous regimes.

From the start, intelligence agencies have been trying to break various kinds of Internet and digital encryption. Numerous documents in the Snowden cache show the many ways they have been successful. Among these, though, one document sticks out. It is called “Tor Stinks.” Its gist is that try as it might, the NSA has had a difficult time cracking the Tor network. While this document, from 2012, may have given Tor users a sense of security, the capture of Ross Ulbricht while he was logged onto Silk Road, as well as the arrest earlier this year of three men who ran a major child pornography site through Tor Hidden Services, should give them pause. By hook or by crook, which is to say by using malware and software vulnerabilities, the FBI and the NSA are actively working to breach Tor. Who would say that child pornography should not be stopped?

It turns out that even without resorting to intensive detective work, Tor’s anonymity can be penetrated. In a paper published online, Paul Syverson, one of Tor’s original developers at the Naval Research Laboratory, along with four colleagues, demonstrated that users who regularly browsed the Internet with Tor could be easily identified. “Our analysis,” they wrote,

> shows that 80% of all types of users may be deanonymized…within six months [and] roughly 100% of users in some common locations are deanonymized within three months.

More recently, security experts have devised a simple way to distinguish Tor users by their particular style of typing. Add to these a new search engine called Memex, designed specifically to troll the dark Net, developed by the Defense Department’s research arm, DARPA. It already has successfully unmasked human traffickers working in secret.

This may be the ultimate Snowden effect: even as encryption gets stronger, even as companies resist adding back doors, even as average users opt for privacy over transparency, the darkest recesses of the Internet, for better and for worse, are being illuminated.
