The U.S. government designed and funds the best defense against its own surveillance.

By Dune Lawrence

Spy Vs. Spy

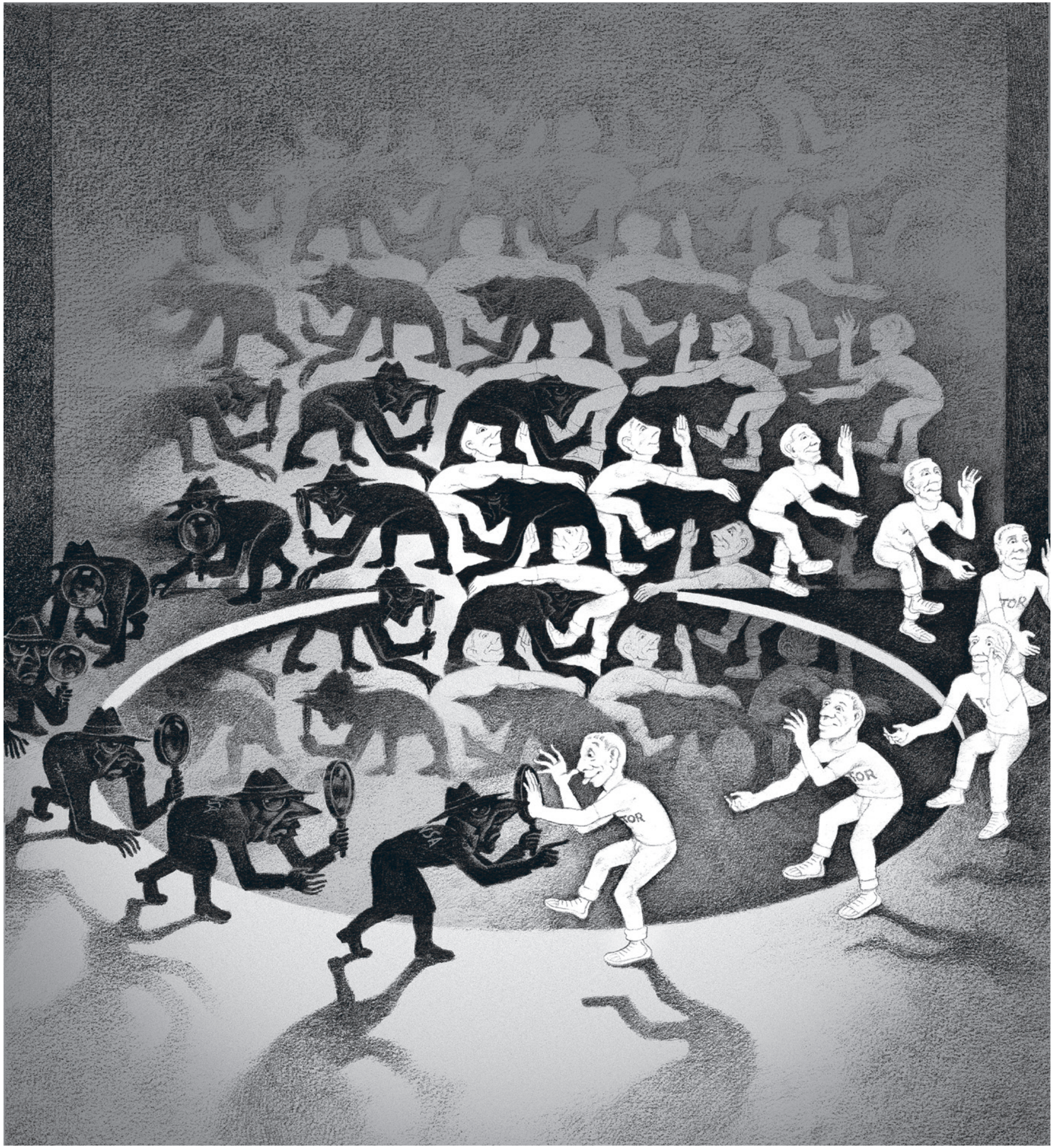


Illustration by David Parkins

Last year, Edward Snowden turned over to the *Guardian*, a British newspaper, some 58,000 classified U.S. government documents. Just a fraction of the files have been made public, but they outline the National Security Agency's massive information-collection system. They've thrown light onto the methods of an arm of the government used to working in the shadows and started an intense debate over national security and personal liberty. One of the earliest and most explosive revelations was the existence of Prism, a top-secret program giving the NSA direct access to the systems of Google, Facebook, and other U.S. Internet companies. ¶ Snowden himself remains something of a mystery even as the U.S. government attempts to obtain his return from Russia, where he's in hiding, and very possibly jail him for the rest of his life. As an infrastructure analyst for the NSA, he came to understand at a high level how information moves around the Internet. Snowden almost certainly relied on one very specific and powerful tool to cover his tracks. In photographs he's often with his laptop, and **on the cover of his computer, a sticker shows a purple and white onion: the "o" in the word "Tor."**

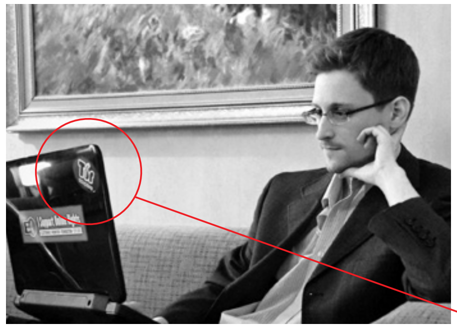


ILLUSTRATION: AFTER M.C. ESCHER; LEWMAN: PHOTOGRAPH BY HARRY GOULD HARVEY IV FOR BLOOMBERG BUSINESSWEEK; SNOWDEN: BARTON GELLMAN/GETTY IMAGES

Tor, an acronym for "the onion router," is software that provides the closest thing to anonymity on the Internet. Engineered by the Tor Project, a nonprofit group, and offered free of charge, Tor has been adopted by both agitators for liberty and criminals. It sends chat messages, Google searches, purchase orders, or e-mails on a winding path through multiple computers, concealing activities as the layers of an onion cover its core, encrypting the source at each step to hide where one is and where one wants to go. Some 5,000 computers around the world, volunteered by their owners, serve as potential hop points in the path, obscuring requests for a new page or chat. Tor Project calls these points relays.

Its users are global, from Iranian activists who eluded government censors to transmit images and news during the 2009 protests following that year's presidential election, to Chinese citizens who regularly use it to get around the country's Great Firewall and its blocks on everything from Facebook to the *New York Times*. In addition to facilitating anonymous communication online, Tor is an access point to the "dark Web," vast reaches of the Internet that are intentionally kept hidden and don't show up in Google or other search engines, often because they harbor the illicit, from child porn to stolen credit card information.

It's perhaps the most effective means of defeating the online surveillance efforts of intelligence agencies around the world, including the most sophisticated agency of them all, the NSA. That's ironic, because Tor started as a project of the U.S. government. More than half of the Tor Project's revenue in 2012, or $1.24 million, came from government grants, including an $876,099 award from the Department of Defense, according to financial statements available on the project's website.

Yet because of Snowden, we now know that the NSA has been working to unpeel the protective layers built by the Tor system. Along with evidence of the NSA's mass data collection, Snowden leaked an agency presentation that demonstrated just how surveillance-proof the software is. It was titled "Tor Stinks." The spooks, according to the slide deck, were thwarted by the software at every turn. Gaining access to some Tor relays, for example, didn't work, because they had to control all three computers in a circuit to defeat the encryption. "We will never be able to de-anonymize all Tor users all the time. With manual analysis we can de-anonymize a very small fraction of Tor users," one slide reads. NSA spokeswoman Vanee Vines said in an e-mailed statement: "It should hardly be surprising that our intelligence agencies seek ways to counteract targets' use of technologies to hide their communications. Throughout history, nations have used various methods to protect their secrets, and today terrorists, cybercriminals, human traffickers, and others use technology to hide their activities. Our intelligence community would not be doing its job if we did not try to counter that."

Countering Tor is clearly frustrating for the NSA, and Internet users have taken note. Hits to Tor's download page almost quadrupled last year, to 139 million. "Encryption works," Bruce Schneier, a cybersecurity expert who helped the *Guardian* analyze the Snowden documents, said at a talk in New York in January. "That's the lesson of Tor. The NSA can't break Tor, and it pisses them off."

Tor's world headquarters occupies one room of a YWCA in Cambridge, Mass. Its neighbor is Transition House, which helps survivors of domestic abuse. Of 33 "core people" listed on Tor's website, nine are full-time employees, and the majority work remotely. For the most part, the project is crowdsourced: Hundreds of volunteers around the world work on improving Tor's software and solving technical challenges like staying ahead of censors in China, which has devoted enormous resources to shutting down anti-censorship tools, including Tor. A request to visit the office in person provoked some mild skepticism from Kelley Misata, who handles press for the group. "The Tor team is primarily virtual (and spread around the world)," she e-mailed, "so our office is made up of only a few members of the team working there on a regular basis."

On a Friday in December, Executive Director Andrew Lewman, Misata, and a researcher named Sarah Cortes showed up to talk at the office, which has the air of a temporary camp, with little décor other than an enlarged Tor logo stuck between two windows and one Ikea run's worth of furniture. We sat at a tall table surrounded by stools that required an awkward perch.

Lewman, 43, has longish dark hair threaded with gray and pulled back by a headband, accentuating heavy eyebrows and large dark eyes. He swallows audibly and speaks quickly. He says he first came across Tor in 2003, when he was working for a large international company with employees in China—he won't say which one—who needed to get around Beijing's increasing Internet controls. Tor was an effective and inexpensive solution, and he began volunteering as a code developer, eventually designing the software's user interface. He's been executive director since 2009. "People now know about Tor. They've heard the name," he says. "What most of the world takes away is this privacy stuff exists, there's this thing called Tor, and the NSA doesn't like it."

Lewman seems, if not tired of talking about the NSA, at least eager to shift discussion to the many uses of Tor that are totally unrelated to three-letter agencies. When the Chinese government clamped down on the Internet in 2009 to ensure a triumphant 60th anniversary celebration of the founding of the People's Republic, Tor saw a spike in use in the country. Teenagers in the Boston exurb of Natick installed it on school-issued laptops so they could get on Facebook, to the school district's displeasure.

Lewman also works with victims of domestic violence, teaching them to get online without revealing to abusers their location and activities. Tor and Transition House are developing guidelines for women at the shelter regarding technology use and online safety.

For Lewman—as with other people behind Tor—the cause has a personal side. When he worked for an Internet marketing firm in the mid 2000s, a consumer, irritated by marketing e-mails, found Lewman's name on the website and began to threaten him, and then his family, online. The stalker eventually showed up at the office, requiring intervention by the police.

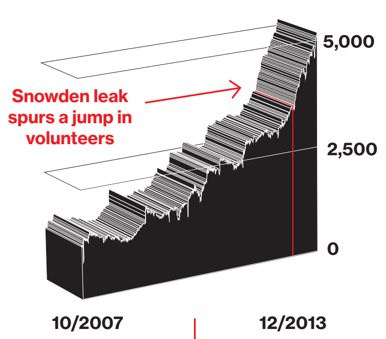
Misata has also had her privacy invaded online. A former colleague cyberstalked her for five years, she says, including posting nasty allegations that topped Google results, complicating job applications. She became an advocate and motivational speaker against cyber harassment. When she heard Lewman speak in 2012, she decided Tor was the safest place for her to work. "A lot of the conversations that I have in D.C., when they stand on their soapbox and say, 'Tor is only used by bad guys,' it's very easy for me to step back and say, 'Here's why it's so important to keep the network open for those who need

➜

▶ "What most of the world takes away is this privacy stuff exists, there's this thing called Tor, and the NSA doesn't like it." —Lewman it,’ ” says Misata, who is pursuing a Ph.D. at Purdue University and researching the use of technology in human trafficking.

Lewman’s message is the same, whether he’s talking to teenagers, Fortune 500 companies, or the U.S. Drug Enforcement Agency, whose agents must maintain deep cover as they infiltrate smuggling and production networks: Everything on the Internet is tracked and recorded, and you might not want that. “A simple question I ask companies is, ‘What do you Google for?’ ” Lewman says. “A number of firms are starting to realize, when we are doing sensitive things, we shouldn’t be doing it ‘naked’ on the Internet.”

Tor Relay Race



Companies routinely use Internet traffic analysis to track what’s coming from competitors’ IP addresses. Searches for patents on specific technologies can lead to hints about what another company is planning. What if a company wants to research a competitor’s pricing? Chances are, Lewman says, if they’re doing it without cloaking their identity, they’ll get answers tailored for them, not the answers a real customer would get.

Living up to its credo of anonymity online, Tor doesn’t have detailed data on its users. They’re clearly not all noble political dissidents, though. Tor had a cameo in October in the FBI takedown of the online drug market, Silk Road, an operation that took years for the Feds to crack because it operated exclusively on the network. Tor estimates that users currently number about 300,000 a day, down from a peak of more than half a million a day over the summer.

“Tor’s biggest problem is press. No one hears about that time someone wasn’t stalked by their abuser. They hear how somebody got away with downloading child porn,” says Eva Galperin, global policy analyst at the Electronic Frontier Foundation, a civil liberties advocacy group in San Francisco. “The reason bad guys use Tor is because it works better than anything else. But at the same time, if there was no Tor, bad guys would still find a way of maintaining their anonymity and everyone else would be left out in the cold.”

Paul Syverson at the U.S. Naval Research Laboratory in Washington is one of the world’s foremost researchers on encrypting and routing data and one of Tor’s creators. He works in the lab’s Center for High Assurance Computer Systems, where a joke nameplate outside his office reads “cryptologicist.” I meet him in December in an all-purpose room stuffed with detritus, including a vacuum cleaner, half-dead plants, some battered cardboard boxes, and shelves crammed with old journals. White dust from a chalkboard scrawled over with formulas covers the floor and chairs.

Syverson, 55, has a Ph.D. in philosophy and looks distinctly unmilitary in an oversize flannel shirt and cargo pants. “The thing we had in mind when we started working on it was to protect government workers going on the public Internet,” he says, specifically analysts doing open-source intelligence gathering. That was in 1995, the Internet’s infancy. By 1996 the research lab had a publicly accessible onion routing system in place, hosted on a Navy server with virtual relays, to demonstrate the concept.

In 2000, Syverson met Roger Dingledine, whose graduate work at the Massachusetts Institute of Technology had focused on the creation of an anonymous online publishing system. Syverson persuaded Dingledine, and eventually another MIT graduate named Nick Mathewson, to help him develop an onion router that could be deployed on the wider Internet. (Dingledine is now project leader of the Tor Project and a researcher and advocate for privacy-enhancing technologies; Mathewson, a director and researcher, continues to help develop the software.)

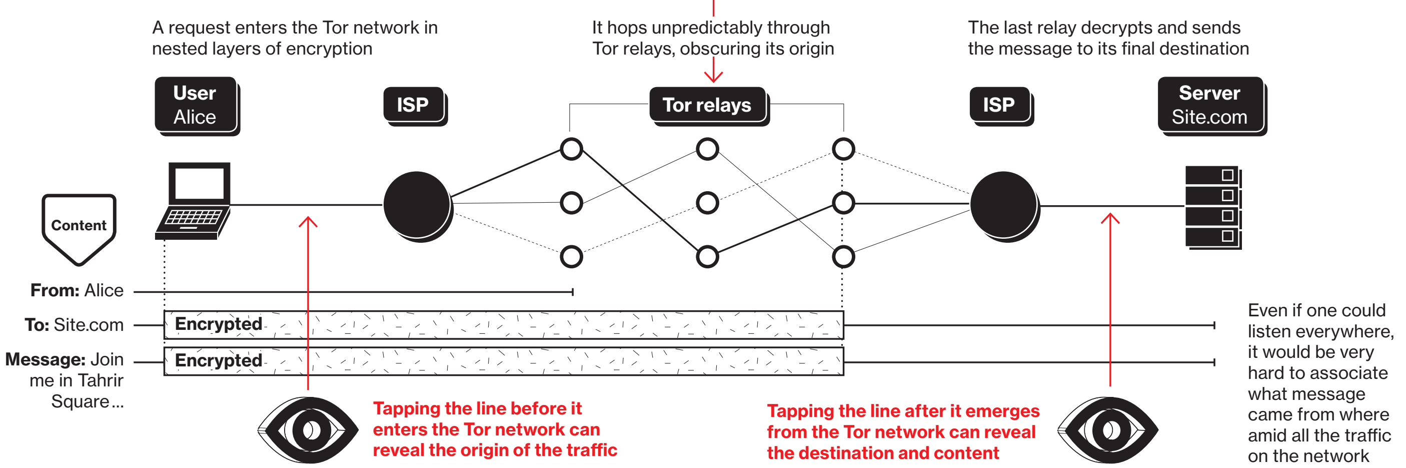
“The basic notion of onion routing is that you have a distributed collection of computers that are scattered around, and you build a cryptographic circuit,” Syverson says. “We wanted it to work with parts of the Internet that don’t know anything about onion routing.”

The group developed the system as it works today, creating a routing process in which the cryptographic keys for each leg of the path are separate and ephemeral, so that no one can go back and decrypt old traffic. It’s one of the elements that has frustrated the NSA—in the original design, a single hostile node could record traffic and compromise the rest of the system.

For the onion router to work properly, the Navy needed to step back from running it. A cloaking system is not useful if all the cloaks say “Navy” on them. “If you have a system that’s only a Navy system, anything popping out of it is obviously from the Navy,” Syverson says. “You need to have a network that carries traffic for other people as well.” Tor Project was incorporated as a nonprofit in 2006 to manage operations.

In technical terms, Tor provides privacy by separating identity from routing online. In a normal session online, you’re browsing from your computer or a router that’s assigned its own IP address. Every request you send out carries that address, and information is returned there. When you use Tor, instead of your chat message, or the URL you type going directly to its destination, it’s routed through Tor’s network of volunteer nodes, moving through at least three of them, before exiting the network and proceeding to the endpoint. The website that receives it doesn’t know what your IP address is, nor does any point in the Tor circuit except for the entry relay. For most users, a Tor session does not feel different from going on the Web with the Firefox browser. But all the winding through relays does slow things down, and the default settings disable some functions for security reasons—including plugins that allow videos—but they can be turned back on.

Peeling the Onion


A request enters the Tor network in nested layers of encryption
It hops unpredictably through Tor relays, obscuring its origin
The last relay decrypts and sends the message to its final destination
User
Alice
ISP
Tor relays
ISP
Server
Site.com
Content
From: Alice
To: Site.com
Message: Join me in Tahrir Square...
Encrypted
Encrypted
Tapping the line before it enters the Tor network can reveal the origin of the traffic
Tapping the line after it emerges from the Tor network can reveal the destination and content
Even if one could listen everywhere, it would be very hard to associate what message came from where amid all the traffic on the network

Despite being designed to enable secrecy, Tor’s methods are almost totally transparent. From the start, Tor has been built on open-source code, meaning the software’s building blocks are freely available. Anyone with the skill to read code can look at how it’s built and how it works—and help improve it.

Such transparency is one of the organization’s key tenets. The Snowden documents have revealed the NSA’s effort to undermine encryption techniques and insert “back doors,” or deliberate vulnerabilities, into hardware and software that the NSA can then use to get into and spy on systems. In December, the German magazine *Der Spiegel* revealed the existence of vulnerabilities for commercially developed systems from the likes of Juniper Networks and Cisco Systems. (When contacted by *Der Spiegel*, both companies denied having knowledge of such back doors or collaborating with the government; Juniper reiterated this to *Bloomberg Businessweek*.) With Tor’s code open for all to see and examine, flaws can’t remain hidden—or as easy to exploit.

Syverson and other researchers have written voluminously about Tor’s weaknesses. The network operates within the wider Web, and the way users behave and configure their computers outside Tor is one of the biggest sources of insecurity. One way the NSA found to get around Tor’s software and spy on users was an attack called “EgotisticalGiraffe,” exploiting a vulnerability in the Firefox browser. Another approach was to try to reconstruct the encrypted path to find the identity of a Tor user by monitoring relays, according to the “Tor Stinks” presentation. Success with this approach was “negligible,” because all three hops in the circuit had to be part of the set NSA could monitor, and the agency had access to few of them.

Tor exerts little control over who volunteers to host traffic, and researchers have found evidence of abuse, such as cases where an operator is snooping on traffic. The group has worked on solving that problem by ranking some relay points as more trusted than others, and giving users the ability to choose a set of trusted computers for the first relay.

Tor has evolved in other ways to stay ahead of what are sometimes referred to on its website as adversaries. Because Tor keeps a public list of all its relays—the IP addresses that volunteer to route Tor users’ requests—the Chinese government has tried blocking all of those IP addresses. To get around that, Tor in 2009 invented “bridges,” relays provided upon request to users who are blocked from regular Tor relays. Bridges aren’t listed in a public directory, making them more difficult to block.

There is a deeper layer of Tor, where information is hosted, called hidden services. These sites are tagged with the extension “.onion” and can only be accessed using Tor. A regular Internet user’s traffic goes through at least three hops; hidden services traffic goes through at least six. Iranian activists during the Green Movement protests in 2009 maintained blogs and websites using hidden services, according to Lewman. The drug bazaar Silk Road operated as a hidden service. You couldn’t find and use Silk Road with a Google search—its IP address was hidden from users. Those who wanted to buy drugs on the site had to use Tor as their browser, type in Silk Road’s .onion address, and use Bitcoins to pay for their purchases.

There is naturally suspicion that the NSA has in fact cracked Tor. In September a security researcher, Robert Graham of Errata Security, analyzed almost 23,000 connections to a relay he’d set up, and concluded that the majority were vulnerable to NSA decryption. Three-quarters of the traffic he monitored used an older version of Tor based on encryption keys that “everyone seems to agree” the NSA can break, he wrote. Version 2.4 of Tor’s software uses a different form of encryption keys, based on something called elliptic curves, which are more difficult to decode—but according to Graham’s analysis only a small subset of users have upgraded to that software version.

▲ **“A lot of the conversations that I have in D.C., when they stand on their soapbox and say, ‘Tor is only used by bad guys,’ it’s very easy for me to step back and say, ‘Here’s why it’s so important to keep the network open for those who need it.’ ”** —Misata

PHOTOGRAPH BY HARRY GOULD HARVEY IV FOR BLOOMBERG BUSINESSWEEK; GRAPHIC BY BLOOMBERG BUSINESSWEEK; DATA: THE TOR PROJECT

Conspiracy theories abound. On one Reddit discussion about Tor’s links to the government, an anonymous poster asked: “How can we be sure that TOR isn’t a front for the CIA or FBI? I mean, it’s too easy to just download, install, and be on your merry way browsing in ‘anonymity.’ ”

Lewman’s job, as he tries to drum up more funding and more volunteers to host relays, is to counter such thinking, which the Snowden revelations have, ironically, added to. “People have such fear of the NSA and the CIA and all these other three-letter organizations,” he says, “that they’re just like, ‘Whoa, I don’t want anything to do with that whatsoever.’ ”

More bandwidth, Lewman says, is what Tor needs most. He says he wants to increase Tor’s capacity by getting universities to run it and work out all the kinks before business puts in real money—citing the example of Facebook, which also started on campus. Major corporations are interested in using Tor, but they expect a ready-made product that’s already incorporated into the big enterprise packages provided by companies such as Cisco. So far, few large corporations have offered to host relays, he says.

It’s the kind of thing the Tor developers might discuss at their next meeting. Asked how often the “virtual team” gets together in person, Misata says she’s in the midst of organizing one of two such annual get-togethers for February. The core group of 30-plus spends the first half of the week discussing current and future initiatives and “bonding” and the second half hosting public meetings to spread the word of Tor. For privacy reasons, some in the developers group refuse to come to the U.S. For the gathering, Misata ended up choosing Iceland. She’s looking for hotels that don’t require guests to provide their passport. Ⓑ