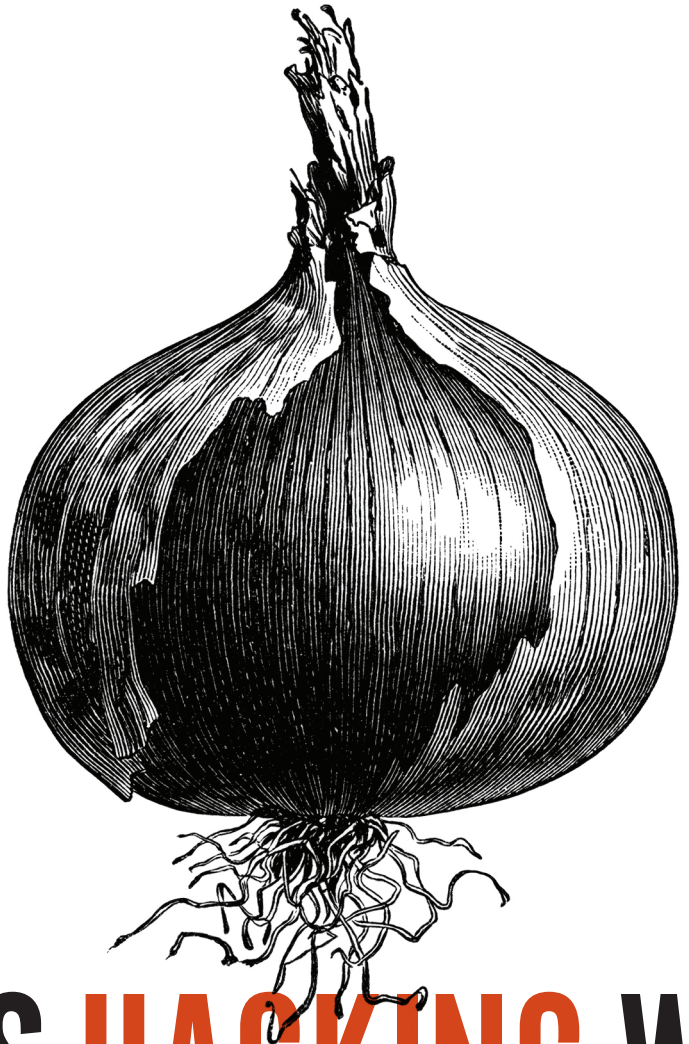
What can you do with a Tor exploit? **Renée Ridgway** discusses an ethical dilemma for security researchers, a surreptitious game of federal investigators, and the state of online anonymity today.



WHO'S HACKING WHOM?

WHO IS HACKING WHOM? The case of Brian Farrell (a.k.a. "Doctor Clu") raises a host of interesting questions about the nature of hacking, vulnerability disclosure, the law, and the status of security research. Doctor Clu was brought to trial by FBI agents who identified him by his Internet Protocol (IP) address. But Clu was using Tor (The Onion Router) to hide his identity, so the FBI had to find a way to "hack" the system to reveal his identity. They didn't do this directly, though. Allegedly, they subpoenaed some information security researchers at Carnegie Mellon University's Software Engineering Institute (SEI) for a list of IP addresses. Why did SEI have the IP addresses? Ironically, these Department of Defense-funded researchers had bragged about a presentation they would give at the Black Hat security conference on de-anonymising Tor users "on a budget." For whatever reason, they had Clu's IP address as a result of their work, and the FBI managed to get it from them. Clu's defense team tried to find out how exactly it was obtained and argued that this was a violation of the 4th amendment, but the judge refused: IP addresses are public, he said; even on Tor, where users have no 'expectation of privacy.'

In this case, security researchers 'hacked' Tor in a technical sense; but the FBI also hacked the researchers in a legal sense – by subpoenaing the exploit and its results in order to bring Clu to trial. As in the recent WannaCry ransomware attack, or the Apple iPhone vs. FBI San Bernardino terrorism investigation of summer 2016, this case reveals the entanglement of security research, the hoarding of exploits and vulnerabilities, the use of those tools by law enforcement and spy agencies, and ultimately citizens' right to privacy online. The rest of this piece explores this entanglement, and asks: what are the politics of disclosing vulnerabilities? What new risks and changed expectations exist in a world where it is not clear who is hacking whom? What responsibilities do researchers have to protect their subjects and what expectations do Tor users have to be protected from such research?

"TOR'S MOTIVATION FOR THREE HOPS IS ANONYMITY"[1]

"Tor is a low-latency anonymity-preserving network that enables its users to protect their privacy online" and enables "anonymous communication" (AlSabah et al., 2012: 73). The Tor p2p network is a mesh of proxy servers where the data is bounced through relays, or nodes. As of this writing, more than 7,000 relays enable the transferral of data, applying "onion routing" as a tactic for anonymity (Spitters et al., 2014).[2] Onion routing was first developed and designed by the US Naval Research Laboratory in order to secure online intelligence activities. Data is sent using Tor through a proxy configuration (3 relays: entry, middle, exit) adding a layer of encryption at every node whilst decrypting the data at every "hop" and forwarding it to the next onion router. In this way, the "clear text" does not appear at the same time and thereby hides the IP address, masking the identity of the user and providing anonymity. At the end of a browsing session the user history is deleted along with the HTTP cookie. Moreover, the greater the number of people using Tor, the higher the anonymity level for users who are connected to the p2p network; volunteers around the world provide servers and enable the Tor traffic to flow.

There is also controversy surrounding the Tor network, connecting it to the so-called "Dark Net" and its "hidden services" that range from the selling of illegal drugs, weapons, and child pornography to sites of anarchism, hacktivism, and politics (Spitters et al., 2014: 1). All of this has increased the risks involved in using Tor. As shown in numerous studies (AlSabah et al., 2012, Spitters et al., 2014, Çalışkan et al., 2015, Winter et al., 2014 and Biryukov et al., 2013), different actors have compromised the Tor network, cracking its anonymity. These actors potentially include the NSA, authoritarian governments worldwide, and multinational corporations: all organisations that would like to discover the identity of users and their personal information (see for example, the case of Hacking Team).[3] Specifically, it should not be discounted that Tor exit node operators have access to the traffic going through their exit nodes, whoever they are (Çalışkan et al., 2015: 29). Besides governmental actors in the security industries, activists, dissidents and whistle-blowers using Tor, there are also academics that carry out research attempting to "hack" Tor.

THE RESEARCHERS' ETHICAL DILEMMA

In January 2015, Brian Farrell aka "Doctor Clu," was arrested and charged with one count of conspiracy to distribute illegal "hard" drugs such as cocaine, methamphetamine and heroin at a "hidden service" marketplace (Silk Road 2.0) on the so-called "Dark Net"(Geuss 2015).[4] His IP address (along with other users) was purportedly captured in early 2014 by researchers, Alexander Volynkin and Michael McCord, when they were carrying out their empirical study at SEI, a non-profit organisation at Carnegie Mellon University (CMU) in Pittsburgh, U.S.A. The SEI researchers were supposedly able to bypass security and with their hack, obtain around 1000 IP addresses of users.

> *Since the beginning of 2014, an unnamed source had been giving authorities the IP address of those who accessed this specific part of the site* (Vinton 2015).

The researchers from SEI at CMU were invited to present their methods and findings on how to "de-anonymize hundreds of thousands of Tor clients and thousands

1 (Winter et al., 2014: 6).

2 https://torstatus.blutmagie.de/

3 "The Italian organisation, which even its CEO called a "notorious" provider of government spyware, was looking to expand its line of products, Rabe said. That included targeting the anonymizing Tor network, where civil rights activists, researchers, pedophiles and drug dealers alike try to hide from the global surveillance complex" (Fox-Brewster 2015).

4 (U.S. v. Farrell, U.S. District Court, W.D. Wash., No. 15-mj-00016) Complaint for Violation. https://cdn.arstechnica.net/wp-content/uploads/2015/01/5498263-0-14302.pdf

A Schedule Update:

For more than 16 years, Black Hat has provided a venue for attendees and the larger community to find the very latest in information security research, developments and trends. We strive to deliver one of the most empirically selected lineups of content in the industry. One of our selected talks, "You Don't Have to be the NSA to Break Tor: Deanonymizing Users on a Budget" by CERT/Carnegie Mellon researcher Alexander Volynkin was scheduled for a Briefing at Black Hat USA this August in Las Vegas. Late last week, we were informed by the legal counsel for the Software Engineering Institute (SEI) and Carnegie Mellon University that: "Unfortunately, Mr. Volynkin will not be able to speak at the conference since the materials that he would be speaking about have not yet approved by CMU/SEI for public release." As a result, we have removed the Briefing from our schedule.

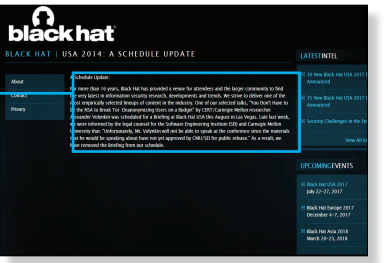


FIGURE 1 (ABOVE AND LEFT): Black Hat 2014 website Schedule Update.
FIGURE 2 (BELOW): Black Hat 2014 Briefings.

YOU DON'T HAVE TO BE THE NSA TO BREAK TOR: DEANONYMIZING USERS ON A BUDGET

PRESENTED BY

Alexander Volynkin & Michael McCord

The Tor network has been providing a reasonable degree of anonymity to individuals and organizations worldwide. It has also been used for distribution of child pornography, illegal drugs, and malware. Anyone with minimal skills and resources can participate on the Tor network. Anyone can become a part of the network. As a participant of the Tor network, you can choose to use it to communicate anonymously or contribute your resources for others to use. There is very little to limit your actions on the Tor network. There is nothing that prevents you from using your resources to de-anonymize the network's users instead by exploiting fundamental flaws in Tor design and implementation. And you don't need the NSA budget to do so. Looking for the IP address of a Tor user? Not a problem. Trying to uncover the location of a Hidden Service? Done. We know because we tested it, in the wild...

In this talk, we demonstrate how the distributed nature, combined with newly discovered shortcomings in design and implementation of the Tor network, can be abused to break Tor anonymity. In our analysis, we've discovered that a persistent adversary with a handful of powerful servers and a couple gigabit links can de-anonymize hundreds of thousands Tor clients and thousands of hidden services within a couple of months. The total investment cost? Just under $3,000. During this talk, we will quickly cover the nature, feasibility, and limitations of possible attacks, and then dive into dozens of successful real-world de-anonymization case studies, ranging from attribution of botnet command and control servers, to drug-trading sites, to users of kiddie porn places. The presentation will conclude with lessons learned and our thoughts on the future of security of distributed anonymity networks.

of hidden services" at the *Black Hat* security conference in July 2014, but they never showed up and the reason of their cancellation is still posted on the website (Figure 1). As the next screenshot of the Internet Archive's Way Back Machine reflects (Figure 2), the researcher's abstract elucidated their braggadocio of a low budget exploit of Tor for around $3000, as well as a call out to others to try:

> *Looking for the IP address of a Tor user? Not a problem. Trying to uncover the location of a Hidden Service? Done. We know because we tested it, in the wild….* (Volynkin 2014).

With regard to ethical research considerations, the researchers' "anonymous subjects" didn't realize or know they were participating in a study-cum-hack. Many in the security research community regard this as an infringement of ethical standards included in the *IEEE Code of Ethics* that prohibits "injuring others, their property, reputation, or employment by false or malicious action" (IEEE n.D.: section 2.4.2). Even when following such an officially recognized IEEE ethical code, "failure, discovery, and unintended or collateral consequences of success" (Greenwald et. al. 2008:78) could potentially harm "objects of study" – in this case the visitors to the Silk Road 2.0. The Dark Net is perhaps trickier than other fields but there are also academics carrying out research there, contacting users, building their trust and protecting their sources.[5] Supposedly SEI started hosting part of Tor's relays, but intentionally set up "malicious actors" so that they could carry out their research. According to one anonymous source reported at *Motherboard*, SEI

> *had the ability to deanonymize a new Tor hidden service in less than two weeks. Existing hidden services required upwards of a month, maybe even two months. The trick is that you have to get your attacking Tor nodes into a privileged position in the Tor network, and this is easier for new hidden services than for existing hidden services* (Cox 2015).

It is crucial that the Tor Project is always informed of the exploit even before it is released so that they can fix potential flaws that enable deanonymization. During the past several years, researchers have continuously shared their data with the Tor Project and reported their findings, such as malicious attacks, or what is called "sniffing" – when the exit relay information is compromised. Once a study is published, patches are developed and Tor improves upon itself as these breaches of security are uncovered. Unlike other empirical studies, the SEI researchers did not inform the Tor Project of their exploits. Instead Tor discovered the exploits and contacted the researchers, who declined to give details. Only after the abstract for Black Hat (late June 2014) was published online did the researchers "give the Tor Project a few hints about the attack but did not reveal details" (Felten 2014). The Tor Project ejected the attacking relays and worked on a fix for all of July 2014, with a software update release at the end of the month, along with an explanation of the attack (Dingledine 2014). As this case shows, not only "malicious actors," but also certain researchers can collect data on Tor users. According to the Tor Project director Roger Dingledine the SEI researchers acted inappropriately:

> *Such action is a violation of our trust and basic guidelines for ethical research. We strongly support independent research on our software and network, but this attack crosses the crucial line between research and endangering innocent users* (Dingledine 2014).

A SUBPOENA FOR RESEARCH

In November 2015, the integrity of these two SEI researchers was again brought into question when the rumour circulated that they had been subpoenaed by the FBI to hand over their collated IP addresses. According to an assistant researcher at CMU Nicolas Christin, SEI is a non-profit and not an academic institution and therefore the researchers at SEI are not academics but instead are "focusing specifically on software-related security and engineering issues" and in 2015 the SEI renewed a 5-year governmental contract for 1,73 billion dollars (Lynch 2015). In an official media statement, CMU's SEI responded by explaining that their mission encompassed searching and identifying "vulnerabilities in software and computing networks so that they may be corrected" (CMU 2015). Important to note is that the US government (specifically the Departments of Defense and of Homeland Security) funds many of these research centers, such as CERT (Computer Emergency Response Team), a division of SEI which has existed ever since the Morris Worm first created a need for such an entity (Kelty 2011). To be precise, it is one of the Federally Funded Research and Development Centers (FFRDC), which are

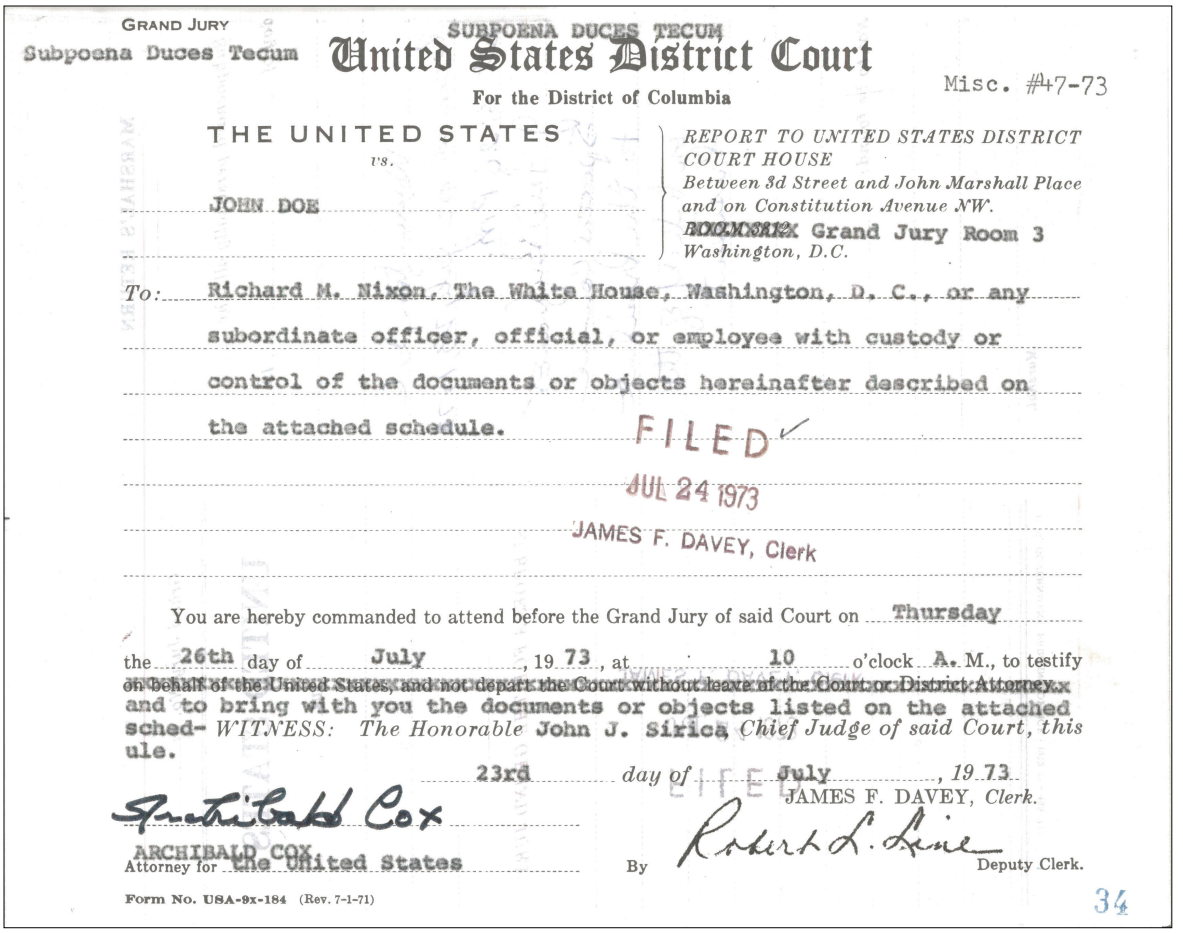
> *unique non-profit entities sponsored and funded by the U.S. government that address long-term problems of considerable complexity, analyze technical questions with a high degree of objectivity, and provide creative and cost-effective solutions to government problems* (Lynch 2015).

Legally, in the U.S., the FBI, SEC and the DEA can all subpoena researchers to share their research. However, the obtained information was not for public consumption, but for an agency within the U.S. Department of Justice, the FBI. Matt Blaze, a computer scientist at the University of Pennsylvania made the following statement about conducting research:

> *When you do experiments on a live network and keep the data, that data is a record that can be subpoenaed. As academics, we're not used to thinking about that. But it can happen, and it did happen* (Vitáris 2016).

Besides the ethical questions regarding the researchers handing over their findings to the governments that have supported them (ostensibly with tax-payer money), the politics of security research and vulnerability disclosure continues to be a heated debate within academia and the general public. It seems that issuing subpoenas by law enforcement might provide a means to gather data on citizens and to obtain knowledge of academic research – which then remains hidden from the public. Computer security defense

5 I refer here specifically to Jamie Bartlett's 'The Dark Net' research.



GRAND JURY
Subpoena Duces Tecum

SUBPOENA DUCES TECUM
United States District Court
For the District of Columbia

Misc. #47-73

THE UNITED STATES
vs.
JOHN DOE

REPORT TO UNITED STATES DISTRICT COURT HOUSE
Between 3d Street and John Marshall Place and on Constitution Avenue NW.
ROOM 5512 Grand Jury Room 3
Washington, D.C.

To: Richard M. Nixon, The White House, Washington, D. C., or any subordinate officer, official, or employee with custody or control of the documents or objects hereinafter described on the attached schedule.

FILED
JUL 24 1973
JAMES F. DAVEY, Clerk

You are hereby commanded to attend before the Grand Jury of said Court on Thursday the 26th day of July, 19 73, at 10 o'clock A. M., to testify on behalf of the United States, and not depart the Court without leave of the Court or District Attorney, and to bring with you the documents or objects listed on the attached schedule.

WITNESS: The Honorable John J. Sirica, Chief Judge of said Court, this 23rd day of July, 19 73.

JAMES F. DAVEY, Clerk.

Archibald Cox
ARCHIBALD COX
Attorney for the United States

By Robert L. Lane
Deputy Clerk.

Form No. USA-9x-184 (Rev. 7-1-71)

34

LEFT: Richard Nixon's 1973 Grand Jury subpoena.

lawyer Tor Ekeland gave this comment:

> *It seems like they're trying to subpoena surveillance techniques. They're trying to acquire intel[ligence] gathering methods under the pretext of an individual criminal investigation* (Vitáris 2016).

It is not clear whether the FBI was using a subpoena to acquire exploits, or if the CMU (SEI) researchers were originally hired by the FBI and only later disclosed what happened, stating that they had been subpoenaed?[6] Either way, it would raise the issue of whether the FBI required a search warrant in order to obtain the evidence – the IP addresses.

INTERNET SEARCH AND SEIZURE

In January 2016, Farrell's defense filed a motion to compel discovery, in an attempt to understand exactly how the IP address was obtained, as well as the past two-year history of the relationship between the FBI and SEI through working contracts. In February 2016, the Farrell case came to court in Seattle where it was finally revealed to the public that the "university-based research institute" was confirmed to be SEI at CMU, subpoenaed by the FBI (Farivar 2016). The court denied the defense's motion to compel discovery. This statement from the order—*Section II, Analysis*—written by US District Judge Richard A. Jones answered the question of whether a search warrant was needed to obtain IP addresses:

> *SEI's identification of the defendant's IP address because of his use of the Tor network did not constitute a search subject to Fourth Amendment scrutiny* (Cox 2016).[7]

In order to claim protection under the Fourth Amendment, there needs to be a demonstration of an "expectation of privacy," which is not subjective but

6 February 24, 2016: "When asked how the FBI knew that a Department of Defence research project on Tor was underway, so that the agency could then subpoena for information, Jillian Stickels, a spokesperson for the FBI, told Motherboard in a phone call that 'For that specific question, I would ask them [Carnegie Mellon University]. If that information will be released at all, it will probably be released from them.'" (Cox 2016)

7 Scrutiny of the Fourth Amendment shows the original text of 1789 that was later ratified in the Bill of Rights, the first 10 amendments to the US Constitution: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. https://www.archives.gov/founding-docs/bill-of-rights-transcript

recognized as reasonable by other members of society. Furthermore, Judge Jones claimed that the IP address "even those of Tor users, are public, and that Tor users lack a reasonable expectation of privacy" (Cox 2016).

> *Again, according to the party's submissions, such a submission is made despite the understanding communicated by the Tor Project that the Tor network has vulnerabilities and that users might not remain anonymous. Under these circumstances Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network. In other words, they take a significant gamble on any real expectation of privacy under these circumstances* (Jones 2016:3).

Judge Jones reasoned that Farrell didn't have a reasonable expectation of privacy because he used Tor; but he also stated that IP addresses are public because he willingly gave his IP address to an Internet Service Provider (ISP), in order to have internet access. Moreover, the citation (precedent) that Judge Jones drew upon to uphold his order, namely, *United States v. Forrester,* ruled that individuals have no reasonable 'expectation of privacy' with internet IP addresses and email addresses:

> *The Court reaches this conclusion primarily upon reliance on United States v. Forrester, 512 F.2d 500 (9th Cir. 2007). In Forrester, the court clearly enunciated that: Internet users have no expectation of privacy in ...the IP address of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information* (Jones 2016:2–3).

TRUST

In March 2016, Farrell eventually pleaded guilty to one count of conspiracy regarding the distribution of heroin, cocaine and amphetamines in connection with the hidden marketplace Silk Road 2.0 and received an eight-year prison sentence. In this case, the protection of an anonymous IP address was thwarted in various ways (a hack, a subpoena, a ruling) with regard to governmental intrusion. Privacy technologists, such as Christopher Soghoian, have provided testimony in similar cases, explaining that the government states that obtaining IP addresses "isn't such a big deal," yet the government can't seem to elucidate how they could actually obtain them (Kopstein 2016).

Whoever wanted to know the IP address would have to be in control of many nodes in the Tor network, around the world; and one would have to intercept this traffic and then correlate the entry and exit nodes. Besides the difficulty factor, these correlation techniques cost time and money and these exploits, including the one from the SEI researchers, were possible in 2014. Even if IP addresses are considered public when using Tor, they are anonymous unless they are correlated with a specific individual's device.[8] To correlate Farrell's IP address, the FBI had to obtain the list of IP addresses from Farrell's ISP provider, Comcast.

The judge's cited reason for denying the motion to compel disclosure was that IP addresses are in and of themselves not private, as people willingly provide them to third parties. Nowadays people increasingly use the internet (and write emails) instead of the telephone; and in order to do so, they must divulge their IP address to an ISP in order to access the internet. When users are outside of the Tor anonymity network, their IP is exposed to an ISP. However, when inside the "closed field" of Tor, is there no expectation of privacy along with the security of the content? And by extension, is there not an expectation of anonymity with the security of users' identity?

Judge Jones also argued that that Farrell didn't have an expectation of privacy because he handed over his IP address to strangers running the Tor network.

> *[I]t is the Court's understanding that in order for a prospective user to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed towards their destinations. Under such a system, an individual would necessarily be disclosing his identifying information to complete strangers* (Jones 2016:3).

Herewith the notion of trust surfaces and plays a salient role. When people share information with ethnographers, anthropologists, activists or journalists and it takes months, sometimes years to gain people's trust; and the anonymity of the source often needs to be maintained. These days when people choose to use the Tor network they trust a community that can see the IP address at certain points, and they trust that the Tor exit node operators do not divulge their collected IP addresses nor make correlations. In an era of so-called Big Data, as more user data is collated (by companies, governments *and* researchers) correlation becomes easier and deanonymization occurs more frequently. With the Farrell case, researchers' ethical dilemmas, the politics of vulnerability disclosure and law enforcement's "hacking" of Tor all played a role in obtaining his IP address. Despite opposing judicial rulings, it can be argued that Tor users do have an expectation of privacy whereas the capture of IP addresses for users seeking anonymity online has been expedited. ■

RENÉE RIDGWAY *is presently a PhD candidate at Copenhagen Business School (MPP) and a research affiliate with the Digital Cultures Research Lab (DCRL), Leuphana University, Lüneburg. Her research investigates the conceptual as well as technological implications of using search, ranging from the personalisation of Google to anonymous browsing using Tor. Recent contributions to publications include* Ephemera, SAGE Encyclopaedia of the Internet, Hacking Habitat, Money Labs *(INC)*, OPEN!, APRJA *and* Disrupting Business.

8 http://whatismyipaddress.com

BIBLIOGRAPHY

AlSabah, Mashael; Bauer, Kevin and Goldberg, Ian. 2012. "Enhancing Tor's Performance using Real-time Traffic Classification." presented at CCS'12, Raleigh, North Carolina, USA. October 16–18.

Bartlett, Jamie. 2014. *The Dark Net: Inside the Digital Underworld.* Portsmith: Heinemann.

Biryukov, A., Pustogarov, I. and Weinmann, R.P. 2013. "Trawling for tor hidden services: Detection, measurement, deanonymization," in *Security and Privacy* (SP). 2013 IEEE Symposium on. IEEE, pp. 80–94.

Çalışkan, Emin, Minárik, Tomáš, and Osula; Anna-Maria. 2015. *Technical and Legal Overview of the Tor Anonymity Network.* Tallin: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence.

Carnegie Mellon University (CMU). 2015. "Media Statement." November 18th. http://www.cmu.edu/news/stories/archives/2015/november/media-statement.html

Cox, Joseph. 2015. "Tor Attack Could Unmask New Hidden Sites in Under Two Weeks." November 13th. https://motherboard.vice.com/en_us/article/tor-attack-could-unmask-new-hidden-sites-in-under-two-weeks

—. 2016 "Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds." February 24th. https://motherboard.vice.com/en_us/article/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds

Dingledine, Roger a.k.a. arma. 2014. "Tor security advisory: "relay early" traffic confirmation attack," *Tor Project Blog.* July 30th. https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack#comment-66781

Dittrich et. al. 2009. *Towards Community Standards for Ethical Behavior in Computer Security Research.* Stevens CS Technical Report 20091, April 20th.http://mdbailey.ece.illinois.edu/publications/dbd2009tr1.pdf

Farivar, Cyrus. 2016. "Top Silk Road 2.0 admin "DoctorClu" pleads guilty, could face 8 years in prison." *Ars Technica,* April 4th. https://arstechnica.com/tech-policy/2016/04/top-silk-road-2-0-admin-doctorclu-pleads-guilty-could-face-8-years-in-prison/

Felten, Ed. 2014 "Why were CERT researchers attacking Tor?" *Freedom to Tinker Blog.* July 31. https://freedom-to-tinker.com/2014/07/31/why-were-cert-researchers-attacking-tor/

Fox-Brewster, Thomas. 2015. "$30,000 to $1 Million — Breaking Tor Can Bring In The Big Bucks." *Forbes Magazine.* November 12th https://www.forbes.com/sites/thomasbrewster/2015/11/12/earn-money-breaking-tor

Geuss, Megan. 2015 "Alleged "right hand man" to Silk Road 2.0 leader arrested in Seattle." *Ars Technica.* January 21st. https://arstechnica.com/tech-policy/2015/01/alleged-right-hand-man-to-silk-road-2-0-leader-arrested-in-seattle

Greenwald, Stephen J. et. al. 2008. "Towards an Ethical Code for Information Security?" NSPW'08, September 22–25 http://www.nspw.org/papers/2008/nspw2008-greenwald.pdf

IEEE. N.d. *IEEE Code of Ethics.* https://www.ieee.org/about/corporate/governance/p7-8.html

Jones, Richard A. 2016b. Order on Defendant's Motion to Compel *United States v. Farrell*, CR15-029RAJ. U.S. District Court, Western District of Washington, Filed 02/23/16. https://assets.documentcloud.org/documents/2719591/Farrell-Weds.pdf

Kelty, Christopher M. 2011. "The Morris Worm." *Limn. Issue Number One: Systemic Risk.* http://limn.it/the-morris-worm/

Kopstein, Joshua. 2016. "Confused Judge Says You Have No Expectation of Privacy When Using Tor." *Motherboard,* https://motherboard.vice.com/en_us/article/confused-judge-says-you-have-no-expectation-of-privacy-when-using-tor-playpen-fbi-michaud

Lynch, Richard. 2015. "CMU's Software Engineering Institute Contract Renewed by Department of Defense for $1.73 Billion." Press Release, Carnegie Mellon University. July 28th. https://www.cmu.edu/news/stories/archives/2015/july/sei-contract-renewed.html

Spitters, Martijn, Verbruggen, Stefan and van Staalduinen, Mark. 2014. "Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services," presented at *2014 IEEE Joint Intelligence and Security Informatics Conference*, Los Angeles, CA, USA; 15 -17 Dec 2014

Vinton, Kate. 2015. "Alleged Silk Road 2.0 Operator's Right-Hand Man Arrested On Drug Charges." *Forbes Magazine.* January 21. https://www.forbes.com/sites/katevinton/2015/01/21/silk-road-2-0-administrator-doctorclu-arrested-on-drug-charges/#7e4e8fc73cc5

Vitáris, Benjamin. 2016. "FBI's Attack On Tor Shows The Threat Of Subpoenas To Security Researchers."*Deep Dot Web Blog.* March 8 https://www.deepdotweb.com/2016/03/08/fbis-attack-on-tor-shows-the-threat-of-subpoenas-to-security-researchers/

Volynkin, Alexander and McCord, Michael. 2014. "Deanonymizing users on a budget." *Black Hat 2014 Briefings.* https://web.archive.org/web/20140625125021/https://www.blackhat.com/us-14/briefings.html#you-dont-have-to-be-the-nsa-to-break-tor-deanonymizing-users-on-a-budget

Winter, Philipp; Köwer, Richard, et. al. 2014. "Spoiled Onions: Exposing Malicious Tor Exit Relays." In: *Privacy Enhancing Technologies Symposium.* Springer.