2014

Code is Law, But Law is Increasingly Determining the Ethics of Code: A Comment

Jonathon Penney

Code is Law, But Law is Increasingly Determining the Ethics of Code

Jonathon W. Penney

In late July 2014, the information security world was on edge. Researchers from Carnegie Mellon University—who work "closely with the (US) Department of Homeland Security"—were scheduled to give a talk at the Black Hat USA infosec conference on a simple method to "de-anonymize" Tor users.[1] Many were skeptical. Tor, after all, was a respected and widely used tool for online anonymity, employed by activists, dissidents, journalists, and yes, criminals too, to cloak their activities from the prying eyes of state authorities at home and abroad; even Edward Snowden trusted its protection.[2] The idea that there was an undisclosed vulnerability that could be exploited "on a budget" to cheaply and easily unveil the identity of Tor users,[3] was difficult to believe. And yet, the security researchers in question, from the CERT unit of the CMU Software Engineering Institute (SEI), seemed credible.[4] So, people withheld judgment and waited for the talk.

But the talk never happened. It was pulled from the conference program at the last minute, with the CMU researchers, as reported in The Washington Post, claiming the materials they planned to present had "not yet been approved by CMU/SEI for public release".[5] There was plenty speculation as to the reason for the cancellation, with some suggesting a possible National Security Letter from a federal agency,[6] while others argued CMU lawyers, likely concerned by the legality of some aspects of the research, killed the talk to avoid potential liabilities.[7] The cancellation also led commentators to raise important ethical questions about the CMU research—had users' privacy been violated or laws broken? Were identities of Tor users harvested without their consent? Was CMU's Institutional Review Board—the body responsible for overseeing ethical approval for research—properly consulted? None of these questions have yet been fully debated or answered, and may not ever be. All that we can say for sure, is that the cancellation notice sent to the Black Hat USA conference came from CMU's legal counsel.[8] The law had foreclosed any ethics debate. It wasn't always like this.

Perhaps the most contentious ethics debate in the infosec community took place in the late 1990s and early 2000s, and occurred beyond, and sometimes in spite of, any relevant law. That debate was prompted by the Anti-Sec Movement and concerned the ethics of "full disclosure"; that is, the infosec industry practice—the industry norm at the time—to fully disclose security vulnerabilities in various online security forums, justified as the best means to force, or shame, vendors into patching those security holes.[9] Full disclosure itself was a product of "frustration" with an earlier and much criticized Computer Emergency Response Team (CERT) based disclosure process, wherein "bugs" were reported to CERT but kept secret until patched, with venders often dragging their feet or simply not bothering patching at all.[10] Full disclosure, so the argument went, created public pressure to encourage venders to patch vulnerabilities and do so quickly.

The hackers in the anti-sec movement disagree. They strongly opposed full disclosure, and targeted high profile infosec industry figures aligned with such disclosure practices—like OpenBSD's Theo de Raadt or Aleph1 of SecurityFocus—with hacks to make their point. Now, to be clear, anti-sec, particularly its more "violent incarnations"[11] like Pr0j3kt M4yh3m and Phrack High Council, was prone to trolling and exaggeration, and often unnecessarily offensive, but at bottom there remained an im-

portant ethos to the anti-sec movement: it took aim at the commercialization and greed it believed was overtaking the infosec community,[12] and they were not alone as many in the broader community agreed with that sentiment.[13] Full disclosure, anti-sec advocates believed, had nothing to do with security and everything to do with certain infosec practitioners building their public profile via publishing bugs and exploits to curry favor with corporate interests and secure lucrative security jobs.[14] For anti-sec, full disclosure was not only betrayal of the hacker underground, but also deeply irresponsible security wise—because even with public disclosure venders were still slow to patch, leaving any "script kiddie" with an Internet connection to wreak havoc with published exploit code.[15]

Whatever your views on their modus operandi, the antisec movement did provoke a broader debate over security vulnerability disclosure practices, with far ranging implications. Disclosure practices ultimately evolved with "responsible disclosure" now the norm, where researchers work behind the scenes with vendors to protect end users, but usually with a fixed deadline for publication to incentivize bug fixing.[16] Applied properly, it balances incentives for vendors to act, while avoiding the problems with what Bruce Schneier calls "bug secrecy" (personified by the CERT reporting system) and the dubious ethical practice (and broader insecurities) resulting from full vulnerability disclosure that anti-sec movement criticized.[17] Here, abroad and contentious debate within a research community led to better ethics and security practices in the wider industry.

But plenty has changed since the days of Pr0j3kt M4yh3m; most importantly, the legal landscape. Expansive laws like the Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act, coupled with aggressive enforcement by state authorities and corporate interests, have subjected an increasing array of online activities to criminal and civil penalty. What was once considered "full disclosure" may today constitute a criminal act under the CFAA or DMCA.[18] The Tor de-anonymization talk, which may have once led to a much needed infosec community debate about research ethics and the security and dignity of users, was cut off by lawyers and legal concerns. Similar problems are arising in data research beyond information security. The discussion concerning the controversial Facebook "contagion" study, for example, was arguably also dominated by lawyers, with concerns about the study's legality potentially deterring similar research or, at least, publication thereof, in the future.[19] A "destructive silence" from social computing researchers and data scientists on the broader social, technological, and ethical implications of the Facebook study was filled by the lawyers and legal questions.[20]

"Code is Law", the aphorism Larry Lessig popularized, spoke to the importance of computer code as a central regulating force in the Internet age. That remains true, but today, overreaching laws are also increasingly subjugating important social and ethics questions raised by code to the domain of law. Those laws—like the CFAA and DMCA—need to be curtailed or their zealous enforcement reigned; they deter not only legitimate research but also important related social and ethics questions. But researchers must act too. The infosec community, and research communities like it, must not fall silent in the face of legal threats nor tolerate research censorship, as is the case with the Tor de-anonymization talk. The point is not that researchers must launch some divisive "project" or movement within this or that discipline; only that they need, at the very least, to re-assert control over the social, legal, and ethical direction of their fields. Otherwise, law will increasingly determine the direction of data science and the ethics of code.

Notes

1 Andrea Peterson, "Why was the Black Hat Talk on Tor de-anonymization mysteriously cancelled?," The Washington Post, July 24, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/24/why-was-the-black-hat-talk-on-tor-de-anonymization-mysteriously-canceled/.
2 Gerry Smith, "Meet Tor, The Military Made Privacy Network That Counts Edward Snowden as a Fan," The Huffington Post, August 8, 2013, http://www.huffingtonpost.com/2013/07/18/tor-snowden_n_3610370.html.
3 Peterson, ibid.
4 Peterson, ibid.
5 Peterson, ibid.
6 Richard Byrne Reilly, "How (and Why) feds killed a talk on Tor hacking at Black Hat," Venturebeat News, August 6, 2014, http://venturebeat.com/2014/08/06/how-why-feds-killed-a-talk-on-tor-hacking-at-black-hat-exclusive/.
7 Peterson, ibid.
8 Ionut Ilascu, "TOR Talk at Black Hat USA 2014 Cancelled," Softpedia, July 22, 2014, http://news.softpedia.com/news/TOR-Talk-at-Black-Hat-USA-2014-Cancelled-451645.shtml.
9 Bruce Schneier, "Full Disclosure," Crypto-Gram Newsletter, November 21, 2001, https://www.schneier.com/crypto-gram-0111.html.
10 Schneier, ibid.
11 Brian McWilliams, "White Hat Hate Crimes On The Rise," Wired, August 13, 2002, http://archive.wired.com/culture/lifestyle/news/2002/08/54400?currentPage=all.
12 Kim Zetter, "Coder Journeys From Wall Street to Prison," Wired, May 7, 2010, http://www.wired.com/2010/05/watt-reports-to-prison/all/. ("...Project Mayhem's "anti-sec" stance wasn't completely unwelcome in the security world. There was a sentiment among some in the DefCon crowd that the security community's focus on profit was at odds with hacking's roots..."); Schneier, ibid. ("...Publishing a security vulnerability is often a publicity play; the researcher is looking to get his own name in the newspaper by successfully bagging his prey...").
13 AntiSecurity, Intro/Manifesto, ibid. Phrack Inc., ibid; Zetter, ibid.
14 AntiSecurity, Intro/Manifesto, ibid. Phrack Inc., ibid. Zetter, ibid.
15 AntiSecurity, Intro/Manifesto, ibid.; Schneier, ibid. ("...Handing attack tools to clueless teenagers is part of the problem..."); Phrack Inc., ibid.
16 Chris Evans, Eric Grosse, Neel Mehta, Matt Moore, Tavis Ormandy, Julien Tinnes, Michel Zalewski (Google Security Team), "Rebooting Responsible Disclosure: A focus on protecting end users," Google Online Security Blog, July 20, 2010, http://googleonlinesecurity.blogspot.co.uk/2010/07/rebooting-responsible-disclosure-focus.html; Schneier, ibid.
17 Evans et al., ibid; Schneier, ibid.
18 Mike Masnick, "The DOJ's Insane Argument Against Weev: He's a Felon Because He Broke The Rules We Made Up," Techdirt, September 30, 2013, https://www.techdirt.com/articles/20130929/15371724695/dojs-insane-argument-against-weev-hes-felon-because-he-broke-rules-we-made-up.shtml; Schneier, ibid. (discussing controversy over Niels Ferguson's Linux vulnerability discovery and the DMCA).
19 Jonathan Zittrain, "Facebook Could Decide an Election Without Anyone Ever Finding Out," The New Republic, July 1, 2014, http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering (speaking of new laws imposed on intermediaries like Facebook for their internal studies as "ill advised"); Robinson Meyer, "Facebook's Mood Manipulation Experiment Might Have Been Illegal," The Atlantic, September 24, 2014, http://www.theatlantic.com/technology/archive/2014/09/facebooks-mood-manipulation-experiment-might-be-illegal/380717/; Mike Masnick, "Law Professor Claims Any Internet Company 'Research' On Users Without Review Board Approval Is Illegal," Techdirt, September 24, 2014, https://www.techdirt.com/articles/20140924/00230628612/law-professor-claims-any-internet-company-research-users-without-review-board-approval-is-illegal.shtml.
20 Michael Bernstein, "The Destructive Silence of Social Computing Researchers," Medium, July 7., 2014, https://medium.com/@msbernst/the-destructive-silence-of-social-computing-researchers-9155cdff659; Lorenzo Franceschi-Bicchierai, "Facebook Playing Your Feelings Is Legal But 'Creepy' Say Law Experts," Mashable, July 1, 2014, mashable.com/2014/07/01/facebook-emotions-study-legal/.