Routledge
Taylor & Francis Group

Critical Studies in Media Communication

ISSN: 1529-5036 (Print) 1479-5809 (Online) Journal homepage: http://www.tandfonline.com/loi/rcsm20

Crypto War II

Sascha D. Meinrath & Sean Vitka

To cite this article: Sascha D. Meinrath & Sean Vitka (2014) Crypto War II, Critical Studies in Media Communication, 31:2, 123-128, DOI: 10.1080/15295036.2014.921320

To link to this article: https://doi.org/10.1080/15295036.2014.921320

Critical Studies in Media Communication
Vol. 31, No. 2, June 2014, pp. 123–128

Routledge
Taylor & Francis Group

Crypto War II

Sascha D. Meinrath & Sean Vitka

Revelations about the National Security Agency (NSA) and other intelligence agencies' widespread surveillance in the summer of 2013 have accelerated America's path toward a second critical battle over public cryptography. Because so much more of our society is now online, Crypto War II will be a far more devastating conflagration than the Crypto War of the 1990s—one that pits our fundamental right to control the computers and smart devices that are becoming an everyday part of our lives against a combination of corporate and government interests. While the Summer of Snowden has received widespread media coverage, the potential alignment of private and public sector surveillance interests pose a far greater threat to free communication in the 21st century than we've yet realized.

Revelations about the NSA and other intelligence agencies' widespread surveillance in the summer of 2013 have accelerated America's path toward a second critical battle over public cryptography. Because so much more of our society is now online, Crypto War II will be a far more devastating conflagration than the Crypto War of the 1990s—one that pits our fundamental right to control the computers and smart devices that are becoming an everyday part of our lives against a combination of corporate and government interests. While the Summer of Snowden has received widespread media coverage, the potential alignment of private and public sector surveillance interests pose a far greater threat to free communication in the 21st century than we've yet realized.

The Situation Today

In a world where surveillance capabilities are increasingly baked into the fabric of the internet's architecture, end-to-end encryption is a last line of defense. The knowledge that everyone's data is susceptible to sweeping government surveillance is pushing more people, companies, and organizations to use additional measures to secure their

Sascha Meinrath is Director of X-Lab. Correspondence to: sascha@thexlab.org. Sean Vitka is Federal Policy Manager of the Sunlight Foundation, writing here in his personal capacity. Correspondence to: svitka@sunlightfoundation.com

ISSN 1529-5036 (print)/ISSN 1479-5809 (online)
http://dx.doi.org/10.1080/15295036.2014.921320

information (Robinson, 2013). But these measures may soon become the casualty of bad policymaking and over-exuberant law enforcement mandates. Internet service providers are increasingly focused on prioritizing certain internet traffic and degrading specific services and applications (Brodkin, 2014). Previously, open internet rules stopped providers from degrading peer-to-peer traffic, but those rules were thrown out in 2014 when the D.C. Circuit Court of Appeals ruled against the Federal Communications Commission (FCC) (Zajac & Shields, 2014). The court found that the FCC had failed to "promulgate net neutrality regulations … under the proper legal framework." Without net neutrality, network monitoring and discriminatory behavior by ISPs is certain to increase.

Encrypting data (and obfuscating what type of application or service is being used), makes discrimination far more difficult, but such practice also draws the ire of surveillance agencies and their defenders. Such groups treat personal encryption as a target and sometimes go so far as to depict opponents of surveillance as anti-social agitators (Brooks, 2013). In the first Crypto War, the government wanted to prevent the widespread use of strong encryption—for all intents and purposes, classifying math as a munition and clamping down on the export of cryptographic software. When outright bans failed, the government attempted to mandate that back doors be implemented in cryptographic products (the Clipper Chip battle) and, finally, that a third party keep backdoor keys "in escrow" in case the government needed them. The argument was familiar: law enforcement felt it needed to be able to access communications to ensure public safety and national security. Even today, the NSA views the use of encryption as a targetable offense (Goodin, 2013). While the government eventually lost Crypto War I, the Snowden files document a massive, secret conspiracy to undermine strong encryption by introducing back doors into numerous hardware and software products that has persisted since that defeat (Simonite, 2013).

Aligned Interests

Unlike Crypto War I, however, today there is also unprecedented corporate interest in data collection and surveillance. One particularly problematic industry practice is the move by ISPs to create tiered or preferential service offerings. Plans to create tiered services have been floated for years—enabled in part by constant pressure toward less competition in the broadband market. In fact, within mobile broadband services, tiering of various applications (e.g. voice, texting, data) are already normative. But if an ISP can't tell what sort of application is being used, it doesn't know whether to prioritize or deprioritize a specific communications stream—which is why good encryption breaks one of the fundamental assumptions for this new business model. Since encryption can help circumvent discriminatory practices, the incentive to use it will expand with practices like tiering.

ISPs could use various mechanisms to dissuade users from encryption. Terms of service could even go so far as to deprioritize or forbid encrypted traffic—forcing

users to trade privacy for speed. Internet service providers already stigmatize and discriminate against other protocols and services. It was only a few short years ago that Comcast blocked BitTorrent, claiming (without merit, as was proven once the practice was stopped) that this was necessary to prevent network congestion.

In a post-Snowden world, encryption services will likely become a growing percentage of network traffic. As the debate over application discrimination continues, a growing number of users report experiencing a precipitous and unexplained drop in quality of bandwidth-heavy services like Netflix (Fitzgerald & Ramachandran, 2014). Such service degradation indicates discrimination on the user-side, data exchange deals (or lack thereof) on the provider end, or both. In response, a number of consumers have already begun to take matters into their own hands—for instance, by routing traffic through Virtual Private Networks.

Meanwhile, corporations like Google have begun encrypting the data transferred among its data centers and with its users to prevent government snooping. Thanks to their immense political power, these corporate responses to government surveillance have provided some of the most—and arguably, one of the only—effective avenues to stop the slide toward a second Crypto War. But while we may see momentary "wins," it's likely that there will be a private sector split with ISPs and content providers facing off on opposite sides of the encryption battle lines.

Such battles are likely to migrate to one of the most powerful, and least prepared, venues for technological debate on the planet—the U.S. Congress. Within this arena, law enforcement's influence is more powerful. The consistent argument is that encryption and anonymity endanger society (Clapper, 2013). With this new corporate interest, industry lobbyists will simultaneously argue that encryption is undermining their intellectual property and other business interests, and that users freely accept surveillance via the purchase of their products and use of their applications. Their narrative regarding consumer discontent is that unhappy users could always "vote with their feet" and switch providers.

Ever-Increasing Surveillance

As consumers become more privacy-conscious, it remains an open question just how this combination of corporate and government interests will respond. The U.S. government has long required many service providers in America to install surveillance capabilities within their IT infrastructures and applications. The Communications Assistance for Law Enforcement Act mandates that certain digital services be able to comply with wiretap orders, a legally enforced security vulnerability. Such demands draw anonymity oriented services, like Lavabit, into the national security agencies' crosshairs. Their data is not only sought pursuant to statutory tools like CALEA, but also through secret contracts, national security letters, and even outright hacking by government employees (Walters, 2013). The U.S. government has utilized other tactics as well, creating and endorsing encryption standards designed around subtle, difficult-to-diagnose, exploits that are later utilized in surveillance activities (Schneier, 2005). This is the primary reason why conflicting

reports over whether the NSA knew or exploited the Heartbleed vulnerability have caused grave alarm among cryptography experts.

For years, many analysts have expected CALEA "reform," a euphemism for expansion of the act's surveillance mandates. This expansion, which law enforcement has long pushed for, could bring new services under CALEA's umbrella, while also creating severe financial penalties for those companies that do not comply. Under such a regime, if a business were to provide encrypted peer-to-peer communication after such reform, like many services that have gained significant popularity since 2013's surveillance revelations, they would likely also need to provide law enforcement with a mechanism to intercept and decrypt them (Savage, 2010). Security expert Bruce Schneier describes the government's ambitions concisely: "What the FBI wants is the ability to eavesdrop on everything" (Schneier, 2013).

Corporate-governmental collaboration in surveillance (via CALEA and other mandates) is itself a business. As *The Washington Post* reported in August 2013, the NSA paid $394 million into the Corporate Partner Access Project in 2011, and expected to spend another $278 million in 2013 (Timberg & Gellman, 2013). Today, an option that is being floated to modify current surveillance practices would have private entities act as the surveillance data-keepers instead of the NSA—with, of course, a significant payout of tax dollars to these storage proxies.

These surveillance efforts have inspired a dramatic increase in the array of services and applications that are encrypted end-to-end (Hern, 2013). This response from privacy oriented constituencies is a response to both data discrimination and government surveillance—and also indicates that we are entering a new online era epitomized by a growing data-obfuscation arms race. Left unchecked, the relevant surveillance mechanisms will shift from network-based to device-based. That is, one can imagine a CALEA II that creates mandates that devices themselves integrate mechanisms that enable surveillance. In essence, the hardware and software integrated into our smart cars and homes—and even our bodies themselves—will be legally required to be insecure, to the financial benefit of parties seeking to control our communications.

Conclusion

The above series of events would portend frightening political pressure on lawmakers. It is difficult to imagine a politician standing up for privacy and free speech rights when opposition of this position, from both well-moneyed private industry and law enforcement, proclaim that encryption supports 'copyright infringement, child pornography, and terrorism'—all at once. This is the Crypto War II narrative.

However politically dire the current situation is, we can take heart that the key success from the first Crypto War has, in fact, withstood the test of time. Individuals everywhere can and do use tools like Pretty Good Privacy to encrypt their e-mail and other communications whenever and wherever they are. If one wishes to secure a laptop, phone, or other communication device, encryption like PGP can make it

exceedingly difficult to undermine the integrity of communications. The nearly 20 years that strong encryption has been publicly available has not led the world into disarray, nor have terrorists and criminals taken over. In fact, strong encryption has been singularly important for a variety of critical economic and political endeavors (Stecklow, Sonne, & Bradley, 2011). The online world as we know it simply would not exist without strong encryption—everything from credit card purchases to securing the passwords on our favorite social media website requires it.

Crypto War I was a long-fought affair, and eventually the forces of free speech won. But Crypto War II will be a far more grueling slog pitting privacy and free speech aficionados against both governmental and corporate interests. Losing Crypto War II would be disastrous—creating unprecedented collateral damage, dangerous precedents, and potentially game-changing implications that would fundamentally undermine participatory democracy—in particular, the free speech on which it depends—on a global scale. There are, however, several concrete actions that we can take to prevent us from heading down this trajectory. Three key tactics are discussed below.

First, ensure that the locus of control over communications is in the hands of end users and within edge devices. Today's mass surveillance is predicated upon centralized mechanisms for collecting data that are located in the core of our communications networks. But so long as we can use strong encryption and anonymizing technologies, we can still be fairly certain that our communications are secure. While we've won the right to use strong encryption, the next battles will be over who controls our edge devices—and losing now would undermine everything we won in the first Crypto War.

Second, we must enshrine Internet Freedom and open internet rules and ensure that discriminatory practices do not become the new norm. End users are perfectly capable of deciding when they want to prioritize streaming video or an outgoing upload. Today, a legal battle is raging inside the Beltway about how the Federal Communications Commission will oversee the internet—and it is up to the FCC to disrupt the data obfuscation arms race that is certain to occur if ISPs begin to prioritize and degrade services.

Third, reiterate that the right to privacy is sacrosanct and includes the right to use strong encryption, steganographic communications, and anonymizing technologies. Anonymity has been a foundational part of U.S. culture, from Publius, the pseudonym used by some Founding Fathers when publishing the Federalist Papers, to anonymous comments in online forums. It is essential to free speech and a free society.

Taken together, these reforms would change a trajectory that is rapidly hurling us toward Crypto War II and help ensure that Democracy in the 21st century remains true to the inalienable rights it is predicated upon. To accomplish this peace, we need to overcome both entrenched business interests as well as the ever-prevalent fear of the unknown. Our privacy and free speech rights will not survive if we lose these coming battles—and with this corporate-government alignment against encryption, the fight will be harder than ever before.

References

Brodkin, J. (2014, February 21). Netflix packets being dropped every day because Verizon wants more money. Ars Technica. Retrieved from http://arstechnica.com/information-technology/2014/02/netflix-packets-being-dropped-every-day-because-verizon-wants-more-money/

Brooks, D. (2013, June 10). The solitary leaker. *The New York Times*. Retrieved from http://www.nytimes.com/2013/06/11/opinion/brooks-the-solitary-leaker.html

Clapper, J.R. Office of the Director of National Intelligence. (2013). DNI statement: Why the intelligence community seeks to understand online communication tools & technologies. *IC on the Record*. Retrieved from http://icontherecord.tumblr.com/post/58838654347/welcome-to-ic-on-the-record

Fitzgerald, D., & Ramachandran, S. (2014, February 18). Netflix-traffic feud leads to video slowdown. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424052702304899704579391223249896550

Goodin, D. (2013, June 20). Use of Tor and e-mail crypto could increase chances that NSA keeps your data. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2013/06/use-of-tor-and-e-mail-crypto-could-increase-chances-that-nsa-keeps-your-data/

Hern, A. (2013, December 31). Email is broken—but Dark Mail Alliance is aiming to fix it. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2013/dec/31/email-broken-dark-mail-alliance-fix-silent-sircle-snowden

Robinson, F. (2013, August 8). U.S. surveillance programs spur EU efforts to tighten data protection rules. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424127887324522504579000702411343532

Savage, C. (2010, September 27). U.S. tries to make it easier to wiretap the internet. *The New York Times*. Retrieved from http://www.nytimes.com/2010/09/27/us/27wiretap.html

Schneier, B. (2005, February 18). Cryptanalysis of sha-1. *Schneier on Security*. Retrieved from http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html

Schneier, B. (2013, June 4). The problems with CALEA-II. *Schneier on Security*. Retrieved from https://www.schneier.com/blog/archives/2013/06/the_problems_wi_3.html

Simonite, T. (2013, October 8). NSA's own hardware backdoors may still be a "problem from hell." *MIT Technology Review*. Retrieved from http://www.technologyreview.com/news/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/

Stecklow, S., Sonne, P., & Bradley, M. (2011, June 1). Mideast uses Western tools to battle the Skype rebellion. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424052702304520804576345970862420038

Timberg, C., & Gellman, B. (2013, August 29). NSA paying U.S. companies for access to communications networks. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html

Walters, J. (2013, December 29). NSA "hacking unit" infiltrates computers around the world—report. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao

Zajac, A., & Shields, T. (2014, January 14). Verizon wins net neutrality court ruling against FCC. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/2014-01-14/verizon-wins-net-neutrality-court-ruling-against-fcc.html