The Intimidation Factor: How a Surveillance State Can Affect What You Read in Professional Publications

Hal Berghel, *University of Nevada, Las Vegas*

As the world watches the continuing fallout from Edward Snowden's leaks, it's useful to reflect on the implications these leaks have on professional publications. This column is a first-hand account.

I wrote a column this past July on the NSA's PRISM database and the government surveillance apparatus that motivated it. You might recall that one central theme of my column was that while the five PowerPoint slides leaked by Edward Snowden and initially published by *The Washington Post* and *The Guardian* newspapers were pretty innocuous, the overall government surveillance apparatus that has been building for the past 40 years was far from it. We have since learned that Snowden had much more to offer the media that was exceedingly provocative (see "US Spy Network's Successes, Failures and Objectives Detailed in 'Black Budget' Summary," *The Washington Post*, 29 Aug. 2013; www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html?wpisrc=al_excl), but that's the subject of another column.

Appearing extensively in the media, the five slides remain classified even after the leaks and subsequent reproduction in the media. I included a screenshot of one of these slides in my July column. It appeared in the printed version of *Computer* but was removed from the IEEE digital library version. Pull up a chair and let me tell you a story about how our surveillance state can control what you see in your professional publications.

SPILLAGE

Spillage is government-speak for information that ends up where it shouldn't. The formal definition in the Committee on National Security Systems Glossary of April 2010 (www.cnss.gov/Assets/pdf/cnssi_4009.pdf) is a "security incident that results in the transfer of classified or CUI [controlled unclassified information] information onto an information system not accredited for it [read: authorized] for the appropriate security level…. [For example,] whenever classified data is spilled either on an unclassified information system on to an information system with a lower level of classification."

The five PRISM PowerPoint slides were examples of classified information spillage. After most of the world has seen something, it isn't secret anymore in any meaningful sense of the word, so journalists and broadcasters treat the spillage as public information. Spillage, and the whistleblowers and leakers who provide it, are a necessary by-product of investigative journalism. Spillage has always been a core component of journalists' "ground truth data."

However, Snowden's leaks were so embarrassing to the US government that the Department of

0018-9162/13/$31.00 © 2013 IEEE Published by the IEEE Computer Society

Defense's Security Service (DSS) sent out an official notice on 11 June 2013 reminding/warning contractors to avoid spillage on their networks (www.dss.mil/documents/isp/Contractor_NOTICE_posting.pdf):

> Contractors shall not, while accessing the web on Contractor's unclassified systems, access or download documents that are known or suspected to contain classified information. Classified information, whether or not already posted on public websites, disclosed to the media, or otherwise in the public domain remains classified and must be treated as such until such time it is declassified by an appropriate U.S. government authority. It is the responsibility of every Contractor to protect classified information and to follow established procedures for accessing classified information only through authorized means.
>
> Contractors who inadvertently discover potentially classified information in the public domain shall report its existence immediately to their Facility Security Officers (FSO).
>
> Companies are instructed to delete the offending material by holding down the SHIFT key while pressing the DELETE key for Windows-based systems and clearing of the internet browser cache. Subsequently, administrative inquires [sic] and adverse reports are not required. These procedures apply only to the inadvertent exposure to classified information in the public domain.

Why would the government do this? Certainly not to stem the flow of Snowden's spillage—those horses were out of the proverbial gate. The government wants federal contractors to understand by whose largesse they owe their economic fortunes. This was more than a gratuitous act—it put contractors on notice that they had better ramp up the policing of their IT infrastructure, or else.

What did this demand for network hygiene accomplish? Intimidation, pure and simple! The DSS notice provides the government with additional leverage against contractors who don't aggressively police their workforce for potential whistleblowers and leakers. The last sentence in the notice exposes the charade of using spillage as the trigger of this additional scrutiny: the notice only applies to "public domain" information—that is, yesterday's news.

Ask yourself this question: Is spillage on unclassified networks the real core of the DoD's cybersecurity problems? Not only is spillage not low-hanging fruit, from the perspective of risk, it's discarded biomass.

By the time the DSS posted this notice, newspaper copies of the original slides had already passed through contractors' offices, break rooms, and waste baskets, and no doubt prompted lively conversations in cafeterias and around water coolers. But those activities don't get audited (at least not yet!). To be compliant with this DSS notice, subcontractors had to report spillage to the FSO—and that meant creating audit trails for the government to inspect. The DSS notice was simply an Orwellian tactic to deal with thought crimes—the step before a visit to the Ministry of Love.

Similar signals were sent to the media who reported the leaks. *The Monterey County Herald* first reported an Army-wide blockade of *The Guardian*'s website to achieve a "vigilant command climate" in DoD-speak on 26 June 2013 (www.montereyherald.com/local/ci_23546947/guardian-news-website-blocked-at-presidio-monterey). *The Guardian* was the original source of Snowden's leaks, so the DoD took careful aim by blocking access from DoD computer facilities to the newspaper's website (www.theguardian.com/world/2013/jun/28/us-army-blocks-guardian-website-access). Lieutenant Colonel Damien Pickart confirmed that this also applies to all "websites that re-report information first published by *The Guardian*" (www.usnews.com/news/blogs/washington-whispers/2013/06/28/blackout-defense-department-blocks-all-articles-about-nsa-leaks-from-millions-of-computers), so the digital blockade was pervasive.

Of course, this behavior isn't new: the DoD does the same for WikiLeaks and presumably for any other news source that provides access to embarrassing or classified stories. According to Pickart, one of the primary rationales for the blackout is economic—server hygiene is costly, so it's preferable to simply block access. Think about this for a while.

As intimidating as these DoD shots across the bow were, they pale in comparison to the British government's reaction to the Snowden leaks. It actually raided *The Guardian*'s offices. You see, the Brits lack a First Amendment and apparently have much more latitude when it comes to imposing prior restraint on free speech than the US. It demanded the hard drives that contained Snowden's materials from *The Guardian* (www.theguardian.com/world/2013/aug/20/nsa-david-miranda-guardian-hard-drives). Rather than turn over the hard drives, *Guardian* editor Alan Rusbridger chose to destroy them. According to Rusbridger, two UK

Government Communications Headquarters (GCHQ) security experts witnessed the physical destruction. "Whitehall was satisfied, but it felt like a peculiarly pointless piece of symbolism that understood nothing about the digital age," Rusbridger commented.

Reuters reported that the request to hand over or destroy the hard drives came directly from British Prime Minister David Cameron (www.reuters.com/article/2013/08/21/us-usa-security-snowden-britain-idUSBRE97K0G920130821). The choice, as *The Guardian* saw it, was to comply or risk the British government's closure of the newspaper.

Technology service companies were included in the wave of government intimidation as well. This past August, encrypted email service provider Lavabit abruptly shut down its operation after the FBI obtained a search warrant for metadata (a so-called pen register) for a specific account. It has been reported that the account holder of interest was Edward Snowden, who used the account to advertise press conferences he held in the Moscow airport. Lavabit refused to hand over the data and was threatened with criminal contempt. Lavabit appealed, but the FBI served a search warrant for "all information necessary to decrypt communication sent to or from all Lavabit email accounts including encryption keys and SSL keys" (www.wired.com/threatlevel/2013/10/lavabit_unsealed).

Understanding that an anonymous email service that gives up authentication keys is, for all intents and purposes, out of business anyway, Lavabit owner Ladar Levison simply closed the doors rather than comply with the order (http://techcrunch.com/2013/10/03/lavabit-founder-details-government-surveillance-of-secure-email-while-documents-disclose-epic-trolling-of-fed/). Levison remains under a gag order. How far the government will push the contempt case against him is still an open question. In reaction to the Lavabit closure, another email anonymizing service, Silent Mail, preemptively followed suit (http://silentcircle.wordpress.com/2013/08/09/to-our-customers).

It appears that the newest target of government wrath might be academic freedom. In early September, a professor of computer science at Johns Hopkins was instructed by his dean to remove a blog post critical of the NSA from the university's mirror site. Why the dean did this is unclear at this writing (www.theatlanticwire.com/politics/2013/09/johns-hopkins-university-falls-victim-nsa-chilling-effect/69219; www.propublica.org/article/johns-hopkins-and-the-case-of-the-missing-nsa-blog-post), but it's likely that he was externally motivated, as faculty blog oversight isn't normally within the purview of an academic dean. The offending blog post is reproduced at http://arstechnica.com/security/2013/09/crypto-prof-asked-to-remove-nsa-related-blog-post.

Not-for-profit professional societies aren't the best perches from which to launch First Amendment test cases.

THE REST OF THE STORY

So that's the backdrop against which the rest of this story must be placed. I submitted my column on 14 July, unaware of the latest DoD DSS missive three days before and the subsequent implications that would have for at least one corporate subscriber to the IEEE digital library. An attentive facility security officer of a beltway government contractor sent a spillage security alert to employees concerning the PRISM screenshot that appeared in my column (specifically, in the digital library version of my column to which IEEE members had access).

This security alert took on a life of its own, eventually landing in the office of the IEEE General Counsel and Chief Compliance Officer. Although legal precedent might not allow the government to prevent the publication of leaked, classified, or otherwise restricted government information that's protected under the First Amendment, the government can in certain cases still prosecute a publisher for possession or publication of such materials.

The legal precedent includes *The New York Times v. US* and the subsequent prosecution of Daniel Ellsberg and Anthony Russo under the Espionage Act of 1917. The Supreme Court held in that case in 1971 that the US government failed to satisfy the burden of proof required for a prior restraint injunction discussed above, and that *The Times* was free to continue to publish the Pentagon Papers, but (and this is a critical conjunction) that the government was free to prosecute Ellsberg and Russo after the fact. As it turned out, the resulting Ellsberg and Russo prosecution resulted in a mistrial because of misconduct in the Nixon administration's prosecution (such as the White House Plumbers operations). Hence, Ellsberg and Russo weren't acquitted, there was no definitive Supreme Court ruling, and therefore nothing added to the body of case law.

In this way, an image that had already appeared in virtually every news outlet was removed from the electronic copy of my column in the IEEE digital library, along with all references thereto. How did one of our cherished professional societies become intimidated by the government in this way? The answer is to

be found somewhere in the intersection of uncertain case law, DoD digital blackouts of media, intimidation of government contractors, and pressure on journalists and authors who might be critical of the government and the surveillance state.

STUFF HAPPENS

Computer authors receive feedback continuously—but generally not from their publisher's attorneys. In my case, I received a call from the office of the IEEE Legal and Compliance Department on 18 July concerning unsettled case law regarding spillage. Sympathetic to concerns about the image, I recommended, without hesitation, that the image simply be removed, leaving behind the text and caption as is, and substituting for the image something like the spillage alert or a URL to the image available on Wikipedia. I felt that in so doing we would simultaneously ameliorate any legal concerns while remaining on the right side of history.

In my opinion, the removal of all textual references to the image as if to pretend that the image never appeared in the first place will be judged poorly by history. However, this is an area over which intelligent people may disagree. Distinguished not-for-profit media organizations such as NPR (www.indiewire.com/article/outrage_review_spiked_for_naming_names) and the Public Broadcasting Service (PBS) (www.policymic.com/articles/43793/citizen-koch-pbs-kills-koch-brothers-critical-documentary-for-fear-of-offending-them) have been pressured to pull controversial content occasionally, and have done so without permanent damage to their reputations. Although the motivations might have been different (protect privacy [NPR] versus economic pressure [PBS] versus threat of litigation [IEEE]), not-for-profit organizations are of necessity risk averse. In fact, commercial television isn't immune—for example, ABC's pulling of a 20/20 episode that was critical of parent Disney Corporation's hiring policies (www.ajr.org/article.asp?id=237). First Amendment zealots will wish that professional media organizations have complete editorial license over what they decide to release, but wishing won't make it so.

Although I don't think for a moment that the government would ever prosecute an academic professional society on a spillage charge, professional societies cannot survive if large numbers of government employees and contractors cancel their memberships. That's where the intimidation factor comes in, and it's one of the reasons that the spillage notice was posted in the first place. From a historical perspective, the more dangerous threat isn't spillage of classified information, but the spillage of government intimidation. No publisher, media outlet, professional society, NGO, corporation, or individual is immune from this. The government will go to any length to maintain its appearance of control.

By the way, my response to all parties involved was to encourage all not-for-profit professional societies and scholarly publishing companies to raise the issue of how they might all stand together to encourage legislative reform in the area of classified information that's inadvertently divulged into the public space (in other words, spillage). The current atmosphere where the government is unwilling to declassify such information—while it simultaneously increases the risk to government subcontractors, publishers, and media outlets (such as with the DSS notice of 11 June 2013)—is hard to reconcile with the need to advance scholarly and scientific inquiry. This problem can only get worse as the information needs increase in such critical areas as digital security and privacy, genetics, and cloud control—not to mention the thorny constitutional issues involved. I would hope that through combined lobbying efforts, effective and meaningful change might take place.

History has shown that the velocity of innovation usually exceeds our ability to manage it for the public good.

THE VELOCITY OF INNOVATION

As Henry David Thoreau said, "Our inventions are wont to be pretty toys which distract our attention from serious things. They are but improved means to an unimproved end, an end which it was already but too easy to arrive at" (http://thoreau.library.ucsb.edu/thoreau_life.html).

In his own way, Snowden was calling attention to the fact that it's far easier to create and deploy surveillance technology than to responsibly use it. So it is with the advance of weaponry, pesticides, the exploration and use of fossil fuels and nuclear energy, misuse of pharmaceuticals, non-FDA-approved medical compounding, and so on. Phrases like the Cutter Incident, the thalidomide crisis, Love Canal, Bhopal, Chernobyl, Fukushima Daiichi, Deepwater Horizon, *Exxon Valdez*, and the Johnstown Flood effortlessly slide into our vocabulary as silent witness to our technological immaturity. Western society has always had a problem with technology stewardship, often deferring to unbridled technology change for its own sake.

Excising innocuous spillage from a digital library is understandable for a professional society that relies on member dues and subscriptions for revenue and lacks the resources for lengthy court cases.

Stanford law professor Lawrence Lessig is well known for his poignant observation that software code might actually provide more regulation over our behavior in cyberspace than the law (codev2.cc/download+remix/Lessig-Codev2.pdf). This introduces a unique spin on cyberdystopia: where the government's code acts as its agent whenever Constitutional protections become too burdensome. This isn't regulation by code, but oppression by code. In Lessig's terms, government regulates the code directly to better regulate behavior indirectly: if code is power, government code is absolute power. We don't have to look overseas to see how a government can use Internet technology against its citizens.

***Hal Berghel**, Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@computer.org.*