Article

Security against Surveillance: IT Security as Resistance to Pervasive Surveillance

Mike Zajko

University of Alberta, Canada
zajko@ualberta.ca

Abstract

This paper examines Five Eyes surveillance programs as a threat to IT (Information Technology) security and IT security as resistance to these programs. I argue that the most significant of Snowden's disclosures have been the Five Eyes agencies' systematic compromise of the technologies, networks, and standards in use within their own countries and abroad. Attacks on domestic infrastructure contradict the defensive posture of these agencies but are consistent with the project of cyber security as defined by the Five Eyes. The cyber security project of the Five Eyes nations is expansive in scope and has proceeded along dangerous lines. By assigning signals intelligence agencies the dual role of exploiting IT systems as well as securing them, a contradiction has been baked into our evolving notion of cyber security. A comprehensive response should include political and legal reforms, disentangling the Five Eyes' offensive and defensive roles, and narrowing the scope of the cyber security project. However, the most effective forms of resistance for individuals and institutions so far have been through an increased emphasis on IT security practices.

Introduction

Edward Snowden's disclosures and the associated reporting of once-secret government programs have had a number of profound consequences. Within what might be called the internet community (the organizations involved in internet governance and the companies providing internet services), the greatest outrage has been directed at one particular subset of disclosures. These document how an international alliance of intelligence agencies systematically compromised vast private networks, technologies, and standards, and worked to keep these insecure enough to exploit. This was an affront to IT (information technology) security practitioners and those institutions in which IT security is a closely held value. In response, many of these institutions took steps to secure themselves against domestic security agencies. Snowden's disclosures stimulated discussion about taking IT security more seriously, making it easier to implement, and aligning it against a new class of threat.

Before the Snowden disclosures, Western notions of cyber security and IT security seemed to be aligned. Today, they are in tension or conflict. The technologies and services we rely upon have been exposed as the terrain for a new kind of geopolitics. The consequences are pervasive insecurity and pervasive surveillance. Resistance has come in many forms, but so far, the most effective response has been a renewed emphasis on IT security. I argue that while a broader response is necessary, this remains a long-overdue development with many potentially positive consequences. It is high time that security was

Zajko, Mike. 2018. Security against Surveillance: IT Security as Resistance to Pervasive Surveillance. *Surveillance & Society* 16(1): 39-52.

<https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2018 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#).

elevated from the status of an afterthought in the design and implementation of our digital infrastructure. However, the inherent value of privacy or improved security against state surveillance is limited. Pervasive surveillance is a threat to democracy, but resisting surveillance does not, in and of itself, promote democratic values or offer us a vision for the future.

From Cyber Security to IT Security

Immediately before Snowden's appearance on the public stage, cyber security was a dominant international political issue. Earlier in 2013, North American newspapers were full of concern over the Chinese cyber threat. The Chinese telecom company Huawei had been blocked from competing for many contracts because of worries that their technology contained surveillance backdoors. Chinese hackers were referred to as an advanced persistent threat (Achoido 2013; Fung 2013), breaking into the computer systems of various institutions: corporations, governments, and non-government organizations. The Five Eyes (US, UK, Canada, Australia, New Zealand) intelligence agencies¹ seemed the most capable forces to counter this threat. Unbeknownst to many, in their efforts to secure cyberspace these agencies had quietly been working to compromise the world's communications.

We entered the post-Snowden period in the summer of 2013, and since then, how we talk about the internet has changed. The advanced persistent threat has come to include the agencies of the Five Eyes compromising the systems of the most widely used internet services. In 2014, Snowden disclosures showed that Huawei networks had indeed been compromised, but by the NSA. The widespread deployment of Huawei technologies around the world made it a surveillance priority for the NSA to "retain access to these communications lines" (NSA 2010: 1). While Huawei's response to this news was muted, similar disclosures about US internet companies received a much more vocal reaction. Leading US firms and their engineers compared Five Eyes programs revealed by Snowden to a massive "attack"² on the internet itself.

This is essentially the conclusion arrived at by the Internet Engineering Task Force (IETF), an important standards-making body which includes employees of many top internet companies (albeit typically representing their individual views). In August 2013, participants on the IETF's mailing lists began discussing how to deal with the threat of "pervasive surveillance"—the sort of widespread passive monitoring that the Snowden documents had revealed the Five Eyes to be involved in. By September, further stories (including ones about the SIGINT Enabling Project and BULLRUN, see Perlroth, Larson, and Shane 2013) had revealed that NSA and GCHQ were doing more than engaging in bulk surveillance, but actively working to insert vulnerabilities and weaken security standards. The IETF's November 2013 technical plenary in Vancouver set a record for attendance. The outcome was strong agreement that "the current situation of pervasive surveillance represents an attack on the Internet" (IETF 2013: n.p.).

At the time, it was clear that the relationship between the internet engineering community and the security agencies had changed. Much of the talk at the IETF plenary did not specifically reference the NSA or the Five Eyes, and speakers reminded the audience that it was important to defend against pervasive surveillance regardless of who was carrying it out. But revelations of Chinese spying in the previous year had not triggered a comparable reaction. It was the actions of the Five Eyes as disclosed in the Snowden documents that had put the threat into focus.

¹ Respectively, the NSA, GCHQ, CSEC, ASD and GCSB.

² I use the term "attack" here in the technical sense favored in IT security, as generally referring to anything that subverts the intent of the communicating parties, including changing the content of the communication or compromising the intended confidentiality of a communication (see <https://www.rfc-editor.org/rfc/rfc7258.txt>).

In the following months many previously willing private partners of the NSA would line up to voice their displeasure and begin implementing technical safeguards (Sanger and Perlroth 2014). They did so particularly once it became clear that the same intelligence agencies formally asking them for data (gaining access through the front door) were breaking into these same companies' systems and exfiltrating data (through the back door). Google's Eric Schmidt called the NSA's reported hacking of Google traffic "outrageous" (Lennard 2013) and the company implemented more comprehensive encryption. Brad Smith, Counsel for Microsoft, characterized this sort of hacking as an "advanced persistent threat" (Fung 2013). In doing so, he linked the recently disclosed attacks by the Five Eyes to the widely publicized Chinese hacking of a year before. Five Eyes surveillance had become a security threat of the highest order. In the course of a year, these secret services had joined the "threat model" against which industry and civil society would mount a defense.

Competing Conceptions of Security

Security is discussed so frequently, in so many different contexts, that it is difficult to pin down as an over-arching value. Individuals and organizations articulate the need to be secure against various kinds of threats. Governments provide social services, craft budgets, and start wars in the name of security. The contradictions within and between these different claims make any transcendental notion of security unintelligible (Neocleous 2008: 2). But when we examine particular discourses, or "grammars" of security (Hansen and Nissenbaum 2009), it is possible to generalize and make distinctions between them. This allows us to see how one conception of security can come to oppose, compete with, or threaten another.

Cyber security, information security, computer and network security are not discrete domains. In many cases the terms are interchangeable. Today's computers are inevitably networked, they exchange information, and they arguably constitute some sort of "cyber" domain. What is called cyber security in the West has been referred to as information security in countries including Russia and China, where censorship is treated as a legitimate means of achieving security. The distinctions I make in this section are relevant primarily in the context of the Five Eyes nations, but even there they are not universally accepted.

The concerns of both IT and cyber security can be traced back to the 1960s when networked computers created new challenges for securing sensitive data, which could now spill (or be pulled) from one machine to another (Warner 2012). In subsequent decades the concerns of state agencies and non-state actors would follow separate but frequently intertwined paths. The NSA remained an almost entirely opaque agency. With massive cryptographic and computing resources at its disposal, it was tasked with signals intelligence (SIGINT) and protecting US government systems. Private industry also came to value the security of computer systems and the need for effective IT security eventually displaced the NSA's monopoly over advanced cryptography (Diffie and Landau 2007: 229-257; Levy 2001). The early networks that handled financial and business information had the most urgent security needs, but with the commercialization of the internet in the 1990s, secure communication became necessary for anyone participating in the digital economy. IT security therefore became a specialized profession.

The closest thing that the profession of IT security has to a creed or mission statement is the "CIA triad"—to provide Confidentiality, Integrity, and Availability of information. These values have been debated, elaborated, and added to at length, but they also highlight information security's rather limited scope in dealing with threats and "attacks" against this core mission (Nissenbaum 2005: 63). IT security keeps confidential data private, prevents unauthorized modification and deletion, and ensures information meant to be accessible stays available. This is not a purely technical field, since it is often the human users of computer systems that create the greatest vulnerabilities (and must be adequately trained or monitored). Still, the objectives boil down to securing the bits of information that are not intended to be public and free, or ensuring that information meant to be public and free remains available.

In comparison, cyber security has come to encompass the discourse and practices of IT security but also to extend much further—into the realm of national security and all that this entails. IT security can be organized around individual actors and institutions, but cyber security pulls actors together, coordinates their actions, and exchanges information between them. The discourse of cyber security links networks, organizations, and individuals with societal and political referent objects. Specifically, it orients actors to the goals of national security. It asserts that digital infrastructure has become the nation's critical infrastructure and that our networks are now the terrain of geopolitics.

Cyber security ties the nation's strategic objectives to the hygiene of its networks. Its web of concern encompasses gangs of criminal hackers, infected home computers, terrorism, and cyberbullying. In the discourse of cyber security (see Barnard-Wills and Ashenden 2012; Dunn Cavelty 2013; Nissenbaum 2005), digital threats become collective threats, and the range of threats expands far beyond the computer network attacks that concern IT security. Early US approaches to cyber security were dominated by the US military and its strategic objectives (Dunn Cavelty 2007). Canada's and New Zealand's cyber security strategies include protecting citizens from cyber-bullies (Public Safety Canada 2015; New Zealand Cyber Security Strategy 2015). For the UK and Australia, cyber security is a means to further the nation's economic competitiveness (Australia's Cyber Security Strategy 2016; U.K. Cyber Security Strategy 2011).

Table 1. IT and Cyber Security

IT Security	Cyber Security
Referent objects: Computer systems and data	The nation-state and collective interests
Purpose: Confidentiality, Integrity, and Availability	National security

The distinction between IT security and cyber security given above largely follows that of Nissenbaum, who argued that there was a “technical” discourse of IT security that existed alongside a newer cyber security discourse (2005: 63). She proposed that cyber security overlapped with IT security but encompassed a greater set of concerns (2005: 64). Nissenbaum presented these as two competing and incompatible conceptions of security, entailing the need to make a choice between them (2005: 73). She warned that the “inherent differences” between these visions of security “spell tensions in future political, and technical decision-making” (Nissenbaum 2005: 61).

In a later article (Hansen and Nissenbaum 2009) the dichotomy between these two forms of security is no longer argued to be as fundamental. Instead, Hansen and Nissenbaum (2009) stress how cyber security discourse “gains its coherence from making connections between referent objects” (1163). It moves “seamlessly across distinctions” such as state and private, the economy and the military, tying these into a complex constellation of shared interests (Hansen and Nissenbaum 2009: 1162). But the earlier tension had not disappeared, even as the cyber security project steadily expanded and came to encompass IT security along with a host of other concerns.

Through Snowden, we have arrived back to the choice between a more limited, technical conception of security, and a more expansive notion tied to national and collective interests. The cyber security project can mobilize and coordinate IT security efforts towards a common or collective purpose, but it also opens the door to all those prerogative powers justified by national security and its endless series of emergencies (Neocleous 2008). Under this prerogative, state agencies have compromised the world's communications. They have done so in order to make us safe from adversaries. The expansion of cyber security in recent

years has offered fresh opportunities for these contradictions to develop, the most dramatic of which were cultivated in the secret world of the Five Eyes.

The Five Eyes

The Five Eyes is a SIGINT partnership that developed during and after World War II among the English-speaking allies. It includes the US NSA, UK's GCHQ, New Zealand's GCSB, Australia's ASD, and Canada's CSEC. This is not an equal partnership, as the NSA has always been the dominant force. But the Snowden documents show that while each of its member nations pursues SIGINT for their own parochial interests, these agencies routinely share information about their methods and participate in joint programs. While the NSA has many state "partners" beyond the Five Eyes (Gallagher 2014),³ these five agencies form a core trusted group operating this global surveillance system.

The Snowden documents give us an extraordinary insight in the operations of the Five Eyes. They show that these agencies have consistently worked to develop and safeguard their ability to harvest communication flows. The goal is to make these flows transparent and to ensure that no network is beyond their reach (New York Times 2013; Risen and Poitras 2013). These SIGINT efforts have developed into mass surveillance programs as well as techniques to gain access to targeted networks and individual devices (this was the particular specialty of the NSA's Tailored Access Operations group, see Spiegel 2013).

The goals towards which the Five Eyes use these capabilities are largely what you would expect from Western intelligence agencies during the perpetual post-9/11 emergency: Counter-terrorism has been an important objective and cyber threats a growing concern (see New York Times 2013). The traditional SIGINT goal of "foreign intelligence" is still fundamental and now covers an immensely broad scope. When it comes to carrying out domestic surveillance, the five agencies differ in their mandates and restrictions. However, the interconnectedness of the world's networks means that domestic and foreign traffic is often "co-mingled within the same circuits" (CSEC 2014: 24), and terrorist targets can be simultaneously domestic and foreign (Greenberg 2013).

The Snowden documents have not shown evidence of domestic abuses of power on the scale disclosed through the Church Committee's investigation of the NSA's activities in the 1960s and 70s, when the agency was targeting domestic political activity (US Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1976). However, as in the 1970s, the NSA has covertly aided law enforcement (Shiffman and Cooke 2013), and other Five Eyes agencies assist police more overtly. What is new today is the broad volume of communications that the Five Eyes have access to and the discourse of cyber security that is increasingly coming to define their mission. Given all that the cyber security project potentially entails, there is extreme danger in how the Five Eyes' capabilities will be applied.

The centrality of the five SIGINT agencies to the broader governmental project of cyber security varies across the Five Eyes. Besides their SIGINT role, these organizations are tasked with the information security needs of their respective governments, and to a lesser extent they also help secure industry and civil society from cyber threats. In the UK, GCHQ has been encouraged to form partnerships with the private sector (U.K. Cyber Security Strategy 2011), and the NSA has also recently been more public in cultivating these ties (Beinart 2017). New Zealand's GCSB is tasked with critical infrastructure protection, and this mandate has expanded to cover securing internet service providers. Telecom companies in New Zealand are obligated to have employees with security clearance who can interact with GCSB to maintain

³ Much of the argument of this paper likewise extends beyond the Five Eyes, but it is these five agencies that have been at the heart of many of the Snowden disclosures discussed herein.

surveillance-ready equipment and to submit for review their plans to purchase new equipment (Telecommunications [Interception Capability and Security] Act 2013). The SIGINT agencies of Australia and Canada have a more limited role in securing industry and civil society, with affiliated agencies taking the lead for this aspect of cyber security. Among all of the Five Eyes, the primary responsibility for non-governmental cyber security response typically falls to non-SIGINT government agencies. This means that one government agency (SIGINT) can be working to make technologies more vulnerable, while another government agency (such as US-CERT or Canada's CCIRC) has the job of alerting industry when that same vulnerability is discovered.

Strategic Insecurity in Historical Context

The most significant and concerning of the Snowden revelations has been the Five Eyes efforts to systematically compromise the digital infrastructure of their own societies in order to keep prospective targets vulnerable. The lesson to learn from these disclosures is that combining the responsibilities for SIGINT and IT security within the same agency is inherently dangerous. This was one of the conclusions of the US President's Review Group's response to the Snowden disclosures (Clarke et al. 2013), which recommended separating the two functions. The pursuit of SIGINT can easily come to contradict and supersede the more limited mandate of IT security. The consequence of this is that the communications of entire populations are made less secure in the interests of making intelligence targets more vulnerable.

These revelations were not the first instance of conflict between the goals of IT security and national security. The most notable previous episode was during the so-called "crypto wars" of the 1990s in which US intelligence agencies were concerned about the development of sophisticated encryption technologies by private industry. The fear was that advanced encryption would be adopted by US adversaries. In response, US intelligence agencies attempted to weaken these technologies, impose export restrictions, and install backdoor access by way of a mandatory "Clipper chip" (Diffie and Landau 2007: 229-257; Levy 2001). These government efforts generated a great deal of opposition from industry and critical politicians, and they ultimately failed. At the end of the conflict, the US intelligence establishment appeared to accept that it could not restrict the booming IT security trade.

In the years that followed 9/11 came a number of disclosures relating to the NSA's bulk collection efforts. However, these were widely understood to have been carried out with the complicity and knowledge of telecom company executives. Also during this time, IT security became highly professionalized. An uneasy tension continued between hackers and government agents, but many hackers became security professionals and the NSA came to court their expertise (Spiegel 2013). Immediately prior to Snowden's disclosures, it was conceivable that IT security and the institutions of cyber security were on the same side. The threats were "out there"—foreign actors targeting domestic companies and infrastructure. Then we learned that the dream of the Clipper Chip's backdoor access had been covertly realized through an assemblage of Five Eyes programs.

I have avoided referring to backdoors when generalizing about the Five Eyes' exploitation of vulnerabilities and their attacks on infrastructure, because these programs utilize a broad range of methods. Certainly, some of the attacks of the Five Eyes are enabled by true backdoors—installed into the hardware of specifically targeted devices, hacked computer servers (Spiegel 2013), and possibly by way of compromised security standards (Perlroth, Larson, and Shane 2013). But a backdoor implies easy surreptitious access, and many of the Five Eyes' attacks are more labor-intensive and provide far less than the "direct access" that the original PRISM program document suggested (Koop 2014).

Among the vulnerabilities, weaknesses, and "attack vectors" at play, true backdoors are only a subset. The Five Eyes' programs are generally less direct but more ambitious than the 1990s proposal for the Clipper chip. Less direct, because the objective is typically to get around security instead of opening a backdoor

through it. More ambitious, because there are dozens of means of circumvention, including harvesting raw network traffic through “upstream” cable taps, breaking into computers at the end-points, or gaining the cooperation of service providers (Talbot 2013).

Much of this work is precisely what you would expect from contemporary SIGINT agencies. Nevertheless, the scope and scale of these activities has been truly shocking. These interlocking surveillance programs allow multiple collection methods to be brought to bear on a target. Any given technology can be compromised through multiple methods, and targets can be tracked across multiple systems. The consequence for those of us with only a partial insight into these efforts is distrust; we cannot know just what has been compromised and to what extent (Schneier 2014). Five Eyes governments assert they are working to promote our shared security, but this now means cleaning up the indiscriminate damage caused by their own tools and methods, which they were unable to safeguard from foreign adversaries and criminals (Shane, Perlroth, and Sanger 2017). With governments failing to demonstrate they can be credible partners in our security, we have little choice but to trust the private companies responsible for our communications networks, devices, and services. Snowden’s revelations of pervasive surveillance and strategic insecurity have made this dependence even more troubling.

The Expansion of Cyber Security

A number of the Snowden disclosures have revealed the deep contradiction between the strategic goals of cyber security and the narrower technical mission of IT security. This contradiction was not readily apparent before, and today cyber and IT security are still often interchangeable concepts. However, the open-endedness of cyber security means that it can justify subverting IT security as easily as it can strengthen it. Cyber security has traditionally meant ensuring that domestic infrastructure is protected, but according to some of its most capable practitioners (the Five Eyes intelligence agencies) it also means ensuring that the very same infrastructure is vulnerable to certain kinds of threats. When vulnerabilities are propagated in order to keep us safe, it is obvious that contradictory definitions of security are at play.

An important question to consider is whether this contradiction is inherent in cyber security or whether it is some sort of pathological development. Are the most concerning surveillance programs disclosed by Snowden really part of cyber security conduct, or is cyber security just a convenient justification for them? Sabotaging security standards, compromising networks in allied nations, and intercepting traffic are all actions carried out to further what is known as computer network exploitation. These are the sorts of activities we might expect of the NSA and GCHQ in their pursuit of SIGINT, even if these agencies did not have an explicit cyber security responsibility. The Five Eyes agencies wear two hats: one that secures computer systems and another that compromises them. Individuals within the same agency performing a computer network defense (CND) mission may operate separately from those carrying out computer network exploitation (CNE). Can this mean that both IT and cyber security are essentially defensive practices aligned against the offensive operations of CNE?

It is indeed possible to distinguish between the two hats worn by the Five Eyes, and I argue that we need to enforce this distinction in order to have any sort of meaningful state “partner” in IT security. However, as things currently stand the two are becoming even more intertwined (Nakashima 2016), and cyber security’s lofty goals and expansive scope open the door to all manner of questionable practices. The US Comprehensive National Cybersecurity Initiative (CNCI) was created as an ostensibly defensive program. However, the NSA’s massive Utah Data Center is also part of the CNCI, and it presumably aids the NSA in a variety of roles including CNE. One Snowden document reveals that the CNCI also includes the NSA’s covert SIGINT Enabling Project, which works to “insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets” (Perlroth, Larson, and Shane 2013: n.p.). The same document confidently reassures that these vulnerabilities do not weaken security for non-targets and that the goal of these vulnerabilities is

“intelligence exploitation to support network defense and cyber situational awareness” (NSA 2013: 115). According to this view, the best defense comes through ensuring all potential targets are vulnerable. Non-targets are also affected, but they are assumed to be safe, since only the agencies responsible for the vulnerabilities know to exploit them.

Any tactics that might confer an advantage over threats and strategic adversaries can be considered part of the Five Eyes’ cyber security project. CSEC appears to have helped the NSA covertly author a weak encryption standard which then became widely adopted (Perlroth 2013). Before 2013, intelligence agencies helped drive up a lucrative market in “zero-day” vulnerabilities—seeking out and buying exclusive knowledge of security flaws for potential exploitation (Menn 2013). A purely defensive orientation to IT security would find this practice unacceptable (as did the President’s Review Group, see Clarke et al. 2013), but the post-Snowden improvements in encryption have actually increased the value of these zero-day exploits for SIGINT and cyber offense (Ranger 2017). In recent years we have become acutely aware of the dangers of such strategic insecurity, as adversaries and criminals have used some of the vulnerabilities cultivated by the Five Eyes to cause harm on an enormous scale around the world (Shane, Perlroth, and Sanger 2017). However, there are additional reasons for concern as the Five Eyes pursue their nebulous mission of cyber security.

On the basis of the Snowden documents, it is GCHQ’s capabilities and mission scope within the Five Eyes that has been the most concerning. The UK agency has a bulk collections and processing capacity that rivals or exceeds the NSA, and it also works to make IT security technologies more vulnerable (Perlroth, Larson, and Shane 2013). GCHQ’s mission includes operating “in the interests of national security... in the interests of the economic wellbeing of the United Kingdom; and in support of the prevention and the detection of serious crime.” According to one memo, GCHQ’s targets “boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors” (MacAskill et al. 2013). The agency pursues “full-spectrum cyber effects” as a “major part of business.” These effects can range from computer network attack (CNA) to “propaganda, deception, mass messaging, pushing stories,” creating “viral” media content, and psychological operations (GCHQ 2010: 4, 9).

GCHQ is a central part of the UK Cyber Security Strategy (2011), acting in a defensive capacity and as an economic enabler. But according to documents released through Snowden, it has also been developing techniques of covert intervention at the scale of populations (Dhami 2011: 8). This is an agency pursuing the ability to hack networks, analyze populations, and manipulate masses of people towards ill-defined ends. If the other Five Eyes are not currently pursuing similar efforts, it is important to prevent these agencies from metastasizing in a similar fashion.

Pervasive surveillance and strategic insecurity have the consequences of making us more vulnerable, eroding trust, and chilling freedom. There are even greater perils to democracy when these secretive capabilities are combined with a will to police crime, promote business, and manipulate public sentiment. The open-ended discourse of cyber security can apparently accommodate such a dangerous mode of government. To what extent, then, can privacy be a safeguard?

IT Security and Privacy

In debates over the appropriateness of surveillance, many have talked about finding some sort of balance between privacy and security. The pursuit of national security often assumes some compromise of individual privacy and liberty. However, personal IT security can be privacy-enabling because it provides individuals greater control over their information and its confidentiality. Nevertheless, there are approaches to IT security at the institutional level that compromise personal privacy, such as when a company monitors its employees to ensure that they are not leaking trade secrets. Google may have

improved IT security for its users following the Snowden disclosures, but it did so to safeguard its own business model of harvesting personal information for targeted advertising.

It is in this relationship between institutions and individuals where the goals of IT security and privacy may conflict, since individual actions can be a threat to institutional goals. Therefore, I prefer to speak about IT security rather than privacy-enabling technologies as a form of resistance. Both individuals and institutions have strengthened IT security in response to Five Eyes surveillance. However, it makes less sense to speak of Google taking steps to protect its organizational privacy, and the extent to which the company values the privacy of its users remains debatable.

In the end, both privacy and IT security are valuable to the extent that they allow other values to flourish. Likewise, it is difficult to put a value on resistance to surveillance without considering what we lose by not resisting. Privacy safeguards, IT security, and resistance to surveillance overlap with one another. They are linked through the values that these practices can enable and will be discussed together below. However, my focus will remain on IT security as resistance to pervasive surveillance, since this is the clearest way of describing post-Snowden resistance at both the individual and institutional level.

IT Security as Resistance to Pervasive Surveillance

As security scholars are aware, recent decades have seen a proliferation of new kinds of security problems (Hansen and Nissenbaum 2009: 1156-1160; Neocleous 2008: 1-3). The word “security” is now appended to various kinds of referents: human security, environmental security, and cyber security. Contemporary notions of security tend to be oriented against threats to these referent objects, and so it is possible for one kind of security to threaten another. The pursuit of national security and cyber security threats has come to threaten the more clearly delimited value of IT security. Surveillance in the name of national and cyber security has become a threat to IT security, and in response, IT security has become a means of resistance.

The Snowden disclosures generated a great deal of discussion about how best to counter or “rein in” the Five Eyes (although the vast majority of the public debate has focused on the NSA and taken place in the American context). Political and legal approaches gained limited traction and were complicated by the international nature of Five Eyes programs. A more immediate response came from individuals and organizations strengthening IT security. This was resistance through encryption, a greater emphasis on security and privacy in the development of new technologies and more security education. Encryption tools such as Signal and SecureDrop became more widely used to protect confidential sources and communications, and businesses took greater control over their data. A 2015 study by Forrester Research estimated a loss in potential revenues of \$47 billion for US-based companies serving international clients, after the Snowden disclosures led clients to lose confidence in US providers. However, this figure was far below the initial projections, as many international businesses had chosen to remain clients of US providers but with greater control of their own security and encryption (Dignan 2015). In the consumer market, Apple’s release of iOS 8 in 2014 improved encryption for iPhones, leading to major legal conflict in 2016, with US agencies demanding backdoor access (Satarino and Strohm 2016). In that fight, Apple’s CEO “made it clear that he will spend whatever it takes to demonstrate to the world that the company’s products cannot be pierced by the NSA” (Sanger 2017: n.p.).⁴

Such acts of resistance are all “blocking moves” (Marx 2003: 379). They make surveillance less effective by blocking the Five Eyes’ access to certain technologies or blocking these agencies’ ability to easily read communications. But the unilateral nature of these blocking moves—the fact that any individual or organization can pursue them of their own accord—also limits any broader systemic effect. Yes, we can

⁴ While the FBI did eventually break into the iPhone that was at the center of the dispute, it did so without Apple’s assistance.

all encrypt, but that does nothing to address the sprawling assemblage of surveillance programs that are designed to circumvent any single point of blockage.

It is easy to argue that Five Eyes surveillance is essentially a political problem. As long as these institutions endeavor to make the world's IT systems exploitable, there can be no proper solution. Furthermore, we limit the chances for an effective political response by viewing this as a technical problem and believing there can be a technical fix. The same geopolitical blind spot that got Silicon Valley into this mess would be repeated if we believed we could simply invent our way out of it with better IT security technologies.

Morozov (2013) has made the argument that privacy is a weak value when we consider it as an end in itself. If pervasive surveillance is a threat to democracy, privacy is valuable to the extent that it furthers democratic engagement and participation. This value is lost when privacy is equated with an individual's right to control personal information and decide what data is accessible. Encryption can help organize a labor union and a political party, or it can distribute child pornography and coordinate a terrorist attack. Some form of anonymity (including the ability to read anonymously) may be necessary for democratic politics (Moglen 2014), but there is nothing inherently democratic about anonymity. A world where everyone is anonymous or has the benefit of perfect IT security is neither a utopia nor a dystopia but simply a world in which the Five Eyes are forced to work much harder.

By extension, a similar critique can highlight the limited value of resistance. We should ask, is resisting state surveillance valuable in and of itself? What is the value of making Five Eyes surveillance programs more expensive and technically challenging? Even if every act of resistance can be considered to be a political act, many of us are interested in staying out of Five Eyes databases for reasons of self-interest. Like privacy, resistance should be a means to an end. That end can be limited to the peace of mind we gain from not being data-mined by our governments, or we can aspire to change more than our own personal insecurity.

Improving IT security for individuals and institutions is therefore an indirect good; it is the most immediate form of resistance to pervasive surveillance. Politics are slow and uncertain (Moglen 2014), and individual responses can be taken unilaterally. However, we do not have to choose between a technical or political response to pervasive surveillance. Bruce Schneier (2013), in calling upon the engineers at the IETF to "take back" the internet, admitted that even though this is primarily a political problem, it does not make the need for better IT security any less pressing. It seems patently obvious that a greater emphasis on information security will be part of any effective response to the Five Eyes, just as it is clear that there must be a political answer to these institutions (Moglen 2014).

As the arms race between exploitation and IT security continues, each new threat must be countered by a new defensive technique. Perhaps this is inevitable. It is how IT security has always functioned—one step behind the attackers, patching holes as they are discovered. After the Snowden disclosures, greater use of encryption made it more difficult and expensive to harvest communications in bulk. Institutions responsible for "the cloud" can provide even better security for these networks but as individuals we can work to lessen our dependence on cloud infrastructure managed by vulnerable parties. In the longer term we must contend with the cyber security state's taste for offense, which will inevitably be turned inwards as well as outwards.

Personal IT Security and Institutional IT Security

At times in this paper I have made a distinction between personal and institutional IT security and it is necessary to reflect on these two forms and their respective capacities for resistance. Both individuals and organizations have taken defensive measures in response to the surveillance threats disclosed by Snowden.

However, their interests are not necessarily aligned. Individuals must often be treated as potential threats to the IT security of institutions, and users' privacy can be compromised in order to enable an institution's business practices (such as data mining). Institutions are also particularly susceptible to state pressures and may be forced to participate in surveillance programs simply to operate in a given territory (Margolis 2013).

On the other hand, an internet giant like Google can resist state power in ways that exceed the capability of individuals. The company has plenty of money, expertise, and the ability to shape global information flows. Google can unilaterally provide a level of protection to its users that isolated individuals would likely not be able to manage on their own. When protecting one's inbox from an "advanced persistent threat," it pays to have Google's security team in your corner.

The dependent relationships we maintain with our service providers should be troubling to all, but individual or personal IT security is never an independent pursuit. We cannot personally verify every device or line of code, or completely trust anyone else to do so for us. The best way forward is some kind of distributed security (Deibert 2012) involving multiple actors and some overlapping responsibilities. Individuals, companies, and state agencies can all play a part but not as the sort of coordinated assemblage envisioned in cyber security discourse. Rather, distributed security needs to nurture a certain amount of chaos and tolerate disorder—a mixture of actors and approaches, as well as restraint in its scope and interventions.

Conclusion

The slogan of the Australian Signals Directorate is to "reveal their secrets—protect our own." This is an orientation shared among the Five Eyes, and the Snowden documents have revealed just how dangerous this mission statement becomes when the same services and technologies are used broadly across nations. The objective of revealing "their" secrets easily translates into the argument that everyone's information must be transparent to the agents of national security.

Liberalism's traditional means of resisting the state's authoritarian prerogative has been to insist on the rule of law. But we know that the conduct of the Five Eyes agencies has been shaped and limited by these nations' respective legal regimes, and it appears that many of the most concerning of the programs disclosed by Snowden are (or were) "fully legal." This demonstrates the need for political and legal reform, but the blocking moves of IT security can be enacted independent of changes to legal regimes. This is why the most effective reforms to date have been technical and why individuals and institutions have been making pervasive surveillance more difficult as courts deliberate.

One of my arguments has been that the IT security response to the Five Eyes is more than just resistance to pervasive surveillance, but that this demonstrates a conflict between the expanding scope of cyber security and the delimited mission of IT security. Some efforts to secure cyberspace constitute an "attack" in the technical sense of IT security. Cyber security encompasses overt programs to strengthen encryption and covert programs to weaken it.

For state actors, cyber security is an extension of the goals of national security, so it is no surprise that it encompasses the same sorts of offensive and threatening practices that have historically been pursued under the aegis of national security. For the good of the collective, various sorts of people and organizations have been made insecure. Surveillance capabilities are often prioritized over trust and social cohesion. Some of the lead agencies responsible for cyber security (the Five Eyes), have a clear mandate to collect intelligence, and a murkier mandate to conduct offensive operations. As the Snowden documents reveal, they are not above compromising domestic infrastructure in pursuit of these goals or attacking domestic organizations if these include services that are potentially used by adversaries. Cyber

security by way of strategic insecurity may not seem like a sensible approach, but it is entirely reasonable when maximizing surveillance is seen as essential to national security.

One way forward is to better define and delimit cyber security before secrecy and state prerogatives further extend and twist it. This would move cyber security away from concerns such as social control and inter-state competition, and back towards its main focus with controlling access and the integrity of computer systems. Cyberspace is not a referent object that can be secured—it has always been a collective fantasy. The danger is that in a digitally mediated society, efforts to secure cyberspace turn a broader sphere of social life into cyber security's referent object.

The more practical option, given how widely the discourse of cyber security has already dispersed, is to emphasize the value of more delimited concepts like IT security, computer security, and data privacy. To this end, the Snowden disclosures have increased skepticism towards state-backed cyber security efforts and renewed emphasis on the long-neglected value of IT security. But it is precisely because IT security is so delimited and technical that it cannot provide the values we need to go beyond resistance. IT security has nothing to say about democratic politics; it has no inherent preference for openness or walled gardens. The challenge going forward is to make sure that privacy and security are not limited to being ends in themselves but are positioned in service of some higher values.

Acknowledgments

This paper benefited from the mentorship and comments of Kevin Haggerty.

References

- Achido, Byron. 2013. Chinese Military Hackers Were “Noisy.” *USA Today*, February 19. <https://www.usatoday.com/story/news/world/2013/02/19/chinese-military-hacking-group-us-attacks-cyberspying/1930307/>.
- Australia's Cyber Security Strategy. 2016. <https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf>
- Barnard-Wills, David, and Debi Ashenden. 2012. Securing Virtual Space Cyber War, Cyber Terror, and Risk. *Space and Culture* 15 (2): 110–23.
- Beinart, Matthew. 2017. NSA To Share More Unclassified Information on Cyber Threats To Build Industry Partnerships. *Defense Daily*, November 15. <http://www.defensedaily.com/nsa-share-unclassified-information-cyber-threats-build-industry-partnerships/>
- Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. 2013. *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*. https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
- CSEC. 2014. *A-2014-0012*. <https://drive.google.com/file/d/0B0wdLKxvw1xsYzhKWVFJenlNWE0/edit>
- Deibert, Ron. 2012. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. Canadian Defence & Foreign Affairs Institute Research Paper. <https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf>
- Dhami, Mandeep K. 2011. *Behavioural Science Support for JTRIG'S Effects and Online HUMINT Operations*. <https://theintercept.com/document/2015/06/22/behavioural-science-support-jtrig/>
- Diffie, Whitfield, and Susan Landau. 2007. *Privacy on the Line: The Politics of Wiretapping and Encryption* (updated and expanded edition). Cambridge, MA: MIT Press.
- Dignan, Larry. 2015. Snowden, PRISM fallout will cost U.S. tech vendors \$47 billion, less than expected. *ZDNet*, April 2. <http://www.zdnet.com/article/snowden-prism-fallout-will-cost-u-s-tech-vendors-47-billion-less-than-expected/>
- Dunn Cavelty, Myriam. 2007. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge.
- Dunn Cavelty, Myriam. 2013. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review* 15 (1): 105–22.
- Fung, Brian. 2013. Microsoft: U.S. Government Is a Potential Security Threat *Washington Post*, December 5. <http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/05/microsoft-u-s-government-is-a-potential-security-threat/>
- Gallagher, Ryan. 2014. How Secret Partners Expand NSA's Surveillance Dragnet. *The Intercept*, June 18. <https://firstlook.org/theintercept/article/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/>
- GCHQ. 2010. *Full Spectrum Cyber Effects*. <https://www.aclu.org/files/natsec/nsa/Full%20Spectrum%20Cyber%20Effects.pdf>

- Greenberg, Andy. 2013. NSA's Verizon Spying Order Specifically Targeted Americans, Not Foreigners. *Forbes*, June 5. <http://www.forbes.com/sites/andygreenberg/2013/06/05/nsas-verizon-spying-order-specifically-targeted-americans-not-foreigners/>
- Hansen, Lene, and Helen Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53 (4): 1155–75.
- IETF. 2013. Leading Engineers Agree to Upgrade Standards to Improve Internet Privacy and Security. *IETF*. <http://www.ietf.org/blog/leading-engineers-agree-upgrade-standards-improve-internet-privacy-and-security/>
- Koop, Peter. 2014. Top Level Telecommunications: What Is Known about NSA's PRISM Program. *Top Level Telecommunications*. <http://electrospace.blogspot.ca/2014/04/what-is-known-about-nas-prism-program.html>
- Lennard, Natasha. 2013. Google's NSA Outrage: Correct and Hypocritical. *Salon*, November 4. http://www.salon.com/2013/11/04/googles_nsa_outrage_correct_and_hypocritical/
- Levy, Steven. 2001. *Crypto: Secrecy and Privacy in the New Code War*. London, England: Allen Lane.
- MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. 2013. Mastering the Internet: How GCHQ Set out to Spy on the World Wide Web. *The Guardian*, June 21. <http://www.guardian.co.uk/uk/2013/jun/21/gchq-mastering-the-internet>
- Margolis, Joel. 2013. Reader Forum: Team Telecom, the Softbank/Sprint Deal and the Impact on CALEA Obligations. *RCR Wireless News*, June 10. <http://www.rcrwireless.com/article/20130610/opinion/reader-forum-team-telecom-softbanksprint-deal-impact-calea-obligations/>
- Marx, Gary T. 2003. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues* 59 (2): 369–390.
- Menn, Joseph. 2013. U.S. Cyberwar Strategy Stokes Fear of Blowback. *Reuters*, May 10. <http://in.reuters.com/article/2013/05/10/usa-cyberweapons-idINDEE9490AX20130510>
- Moglen, Eben. 2014. Privacy under Attack: The NSA Files Revealed New Threats to Democracy. *The Guardian*, May 27. <http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy>
- Morozov, Evgeny. 2013. Evgeny Morozov on Why Our Privacy Problem Is a Democracy Problem in Disguise. *MIT Technology Review*. <http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/>
- Nakashima, Ellen. 2016. National Security Agency Plans Major Reorganization. *The Washington Post*, February 2.
- Neocleous, Mark. 2008. *Critique of Security*. Edinburgh, UK: Edinburgh University Press.
- New York Times. 2013. Documents Show N.S.A. Efforts to Spy on Both Enemies and Allies. *New York Times*, November 3. <http://www.nytimes.com/interactive/2013/11/03/world/documents-show-nsa-efforts-to-spy-on-both-enemies-and-allies.html>
- New Zealand Cyber Security Strategy 2015. <https://www.dPMC.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf>
- Nissenbaum, Helen. 2005. Where Computer Security Meets National Security. *Ethics and Information Technology* 7 (2): 61–73.
- NSA. 2010. *Huawei Powerpoint Slides*. <https://www.aclu.org/sites/default/files/assets/huawei-powerpoint-slides.pdf>
- NSA. 2013. *Intelligence Budget Request*. <http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html>
- Perlroth, Nicole. 2013. Government Announces Steps to Restore Confidence on Encryption Standards. *New York Times—Bits* September 10. <http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/>
- Perlroth, Nicole, Jeff Larson, and Scott Shane. 2013. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*, September 5. <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>
- Public Safety Canada. 2015. Information on Cyberbullying. <https://www.getcybersafe.gc.ca/cnt/cbrbllng/index-en.aspx>
- Ranger, Steve. 2017. Why the CIA's iOS, Android and Windows Hack Stockpile Puts Zero-Day Hoards in the Spotlight. *ZDNet*, March 8. <http://www.zdnet.com/article/cias-ios-android-windows-hack-stockpile-puts-zero-day-hoards-in-the-spotlight/>
- Risen, James, and Laura Poitras. 2013. N.S.A. Report Outlined Goals for More Power. *New York Times*, November 22. <http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html>
- Sanger, David E., and Nicole Perlroth. 2014. Internet Giants Erect Barriers to Spy Agencies. *New York Times*, June 6. <http://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html>
- Sanger, David E. 2017. Journalism after Snowden: A New Age of Cyberwarfare. *Columbia Journalism Review*, March 7. <https://www.cjr.org/opinion/edward-snowden-cyberwarfare.php>
- Satarino, Adam, and Chris Strohm. 2016. The Behind-the-Scenes Fight Between Apple and the FBI. *Bloomberg*, March 20. <https://www.bloomberg.com/news/features/2016-03-20/the-behind-the-scenes-fight-between-apple-and-the-fbi>
- Schneier, Bruce. 2013. The NSA Is Commandeering the Internet. *The Atlantic*, August 12. <http://www.theatlantic.com/technology/archive/2013/08/the-nsa-is-commandeering-the-internet/278572/>
- Schneier, Bruce. 2014. Internet Subversion. *Schneier on Security*. https://www.schneier.com/blog/archives/2014/05/internet_subver.html
- Shane, Scott, Nicole Perlroth, and David E. Sanger. 2017. Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core. *The New York Times*, November 12. <https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html>
- Shiffman, John, and Kristina Cooke. 2013. Exclusive: U.S. Directs Agents to Cover up Program Used to Investigate Americans. *Reuters*, August 5. <http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>

- Spiegel. 2013. The NSA Uses Powerful Toolbox in Effort to Spy on Global Networks. *Spiegel Online*, December 29. <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>
- Talbot, David. 2013. Bruce Schneier: NSA Spying Is Making Us Less Safe. *MIT Technology Review*. <http://www.technologyreview.com/news/519336/bruce-schneier-nsa-spying-is-making-us-less-safe/>
- Telecommunications (Interception Capability and Security) Act 2013. (New Zealand). <http://www.legislation.govt.nz/act/public/2013/0091/latest/whole.html>
- UK Cyber Security Strategy. 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
- US Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. 1976. National Security Agency Activity Concerning Americans. In *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*. http://www.aarclibrary.org/publib/church/reports/book3/pdf/ChurchB3_10_NSA.pdf
- Warner, Michael. 2012. Cybersecurity: A Pre-History. *Intelligence and National Security* 27 (5): 781–99.