International Journal of Communication 8 (2014), 2860–2878 1932–8036/20140005

The Insecurity of Innovation: A Critical Analysis of Cybersecurity in the United States

CATHERINE HART
DAL YONG JIN
ANDREW FEENBERG
Simon Fraser University, USA

This article examines the framing of U.S. debates around securitization of the Internet and questions the need for a securitizing approach. Undoubtedly the Internet could be more secure, but we stress the importance of cyberspace as an open, global commons of information that has allowed innovation and rapid technological growth. We therefore discuss how the cybersecurity issue can be reframed to take into account the importance of this openness instead of viewing it as a vulnerability, and seek solutions that do not unduly or disproportionately impact civil liberties.

Keywords: securitization, insecurity, Internet, cybersecurity, technification, cyberattacks

Introduction

Whistleblower Edward Snowden's revelations since 2013 have drawn international attention to the far-reaching, seemingly unchecked global surveillance being conducted by the U.S. National Security Agency (NSA) and equivalent agencies in countries within the "Five Eyes" alliance[1] ("Edward Snowden Interview," 2013a). In the ensuing months, many have asked how such a scheme can exist, wherein the entirety of law-abiding individuals' communications data—both Internet and cell-phone communications—can be vacuumed up indiscriminately and stored for future data mining (Poitras & Greenwald, 2013). Answers can be found by analyzing the history of networked computing and the ways in which the U.S. government has sought to influence its development and use. The interests of national security professionals and private industry, particularly technology companies, have been central to this process,

Catherine Hart: cathrynhart@gmail.com
Dal Yong Jin: djin@sfu.ca
Andrew Feenberg: feenberg@sfu.ca

[1] Snowden is an American computer specialist and a former employee of the Central Intelligence Agency. In 2013, he disclosed numerous classified NSA documents to several media outlets. The leaked documents revealed operational details of a global surveillance apparatus run by the NSA and other members of the "Five Eyes" alliance comprising the U.S., the U.K., Australia, Canada, and New Zealand, along with many commercial partners.

though their interests have not always aligned.[2]

Technically speaking, this massive surveillance program was made possible by decades of profound economic and cultural change due in part to the creation of broadband Internet and the progressive networking of the information society. The Internet's early nonhierarchical structural design facilitated its development into a relatively open medium that has been used in unexpected ways (Saco, 1999). When it began, the Internet was assumed to be an ideal cyberspace where all users are honorable (Abbate, 1999). This openness allowed new technologies to spread rapidly but also posed problems for national and personal security. Still unfinished, the Internet became accessible to the public with a tacit invitation to explore its potential, to create, and to innovate. As Zittrain noted,

> compared to the rest of the technologies we use each day, it's completely anomalous, even absurd. . . . We wouldn't want our cars, fridges, or TiVos to be altered by unknown outsiders at the touch of a button—and yet this remains the prevailing way that we load new software on our PCs. (2008, pp. ix–x)

Various sectors of society have become increasingly reliant on networked computing, increasing the potential for mass disruption should intentional interference affect these networks (Cavelty, 2008). The result, in what Saco called an ironic turn of events, is that "what began as a state-run technology intended to enhance security is now regarded as a source of insecurity" (1999, p. 270).

This parallel discussion of security and vulnerability was what paved the way for the NSA's massive spying operation, making a technical possibility into a national security necessity (Nissenbaum, 2005). The computer system, on which information and power rely, is vulnerable to intrusion and disruption. As new technologies spread, cyberattacks became more sophisticated. Attackers are now capable of shutting down network servers and cloud-based systems, affecting both companies and individuals and even raising national security concerns.

Thus, to combat what were portrayed as inevitable existential security threats, the use of extraordinary measures was justified by what Buzan, Waever, and de Wilde (1998) and Eriksson and Giacomello (2007) have called a securitizing rhetoric. It positions the Internet as a risky space where attacks on a nation can be planned via anonymous, hidden communication—or carried out directly by

[2] This article's focus is the relationship between the U.S. security establishment, civil liberties advocates, and industry, and those groups' influence on the development of the Internet. Still, it is worth noting how crucial academic institutions and nonprofits are to its governance. For example, the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN) are nonprofits that manage Internet standards, registration of domain names, and assigning of IP addresses. But they also develop international policy on Internet governance. Though based in the United States, these nonprofits do not represent U.S. interests but rather use a multi-stakeholder model that emphasizes consensus among a range of government representatives, businesspeople, academics, and individuals. They have resisted attempts to assert government or national influence over Internet governance, and prioritize global interoperability and openness (Crawford, 2012).

taking advantage of a nation's highly networked infrastructure. The U.S. government has responded by expanding its security mandate to encompass cyberspace. These colonizing efforts are geared to restrict and control certain uses of the Internet, and to remove anonymity from communications. Negative repercussions have followed for the economy and for civil liberties.

How to respond to cyber threats is one of the most pressing questions of the age. Without reliable and secure systems, users will be unable to trust that their information and finances are stored safely, and economic growth and innovation will suffer. Meanwhile, the nation's economic, social, and political reliance on these systems highlights the national security implications of safeguarding these networks. Then again, their openness and insecurity has allowed for rapid, unfettered development of networked technology, and private industry and citizens have resisted attempts to produce a greater sense of control over online activities, citing the economic and civic limitations such safety measures impose. Snowden's revelations and the public reaction to the leaked information neatly illustrate how divisive this topic is, but also how persuasive the national security argument has been among the nation's decision makers.

This article assesses the circumstances that have allowed securitizing arguments to hold such sway. Without doubting that the Internet could (and should) be more secure, the article examines how these debates are framed and questions the need for a securitizing approach (Buzan et al., 1998). Such an approach favors solutions to insecurity that increase digital controls, regulation, and surveillance; and ignores the importance of cyberspace as an open, global commons of information that has allowed innovation and rapid technological growth. The article discusses ways of reframing the cybersecurity issue to present this openness as an important advantage rather than a vulnerability, and to seek solutions that do not unduly or disproportionately impact civil liberties.

Constructivist Approaches to Security: Securitization and Technification

This notion of "securitizing" an issue is the foundation of Buzan et al.'s *Securitization Theory* (1998). Drawing on Austin's Speech Act Theory (1975), the Copenhagen School of security studies posits that the securitization process begins with a performative utterance that can bring about a condition by pronouncing it: A "referent object," in this case the state, is said to be threatened existentially, necessitating urgent action. This provides justification for securitizing actors to bypass normal political procedures and respond with countermeasures that may be disproportionate to the threat or infringe on civil liberties. According to the Copenhagen School, "the invocation of security has been the key to legitimizing the use of force, but more generally it has opened the way for the state to mobilize, or to take special powers, to handle existential threats" (Buzan et al., 1998, p. 21). In some cases actors may expand a securitizing move beyond a normal level by exaggerating threats and promoting excessive countermeasures, a situation that Buzan termed "hypersecuritization" (2004, p. 172). If a securitizing move is successful, an audience will tolerate violations of rules that would otherwise have to be obeyed, for example the restriction of free speech or freedom from unreasonable search and seizure.

This constructivist approach examines the framing of reality, clarifying the choices that cause issues to be characterized in certain ways. As the Copenhagen School asserts,

> actors can choose to handle a major challenge in other ways and thus not securitize it. The use of a specific conceptualization is always a choice—it is politics, it is not possible to decide by investigating the threat scientifically. (Buzan et al., 1998, p. 32)

This approach dovetails with the critical approach to technology, which argues that a technological process promotes advances of general utility, but the concrete form these advances take is determined by those with power over the technology's construction, who ensure that it also serves their interests. Taking a Marxist approach, Feenberg (1991) claimed that technological innovation has functioned to divide members of capitalist industrial societies into two groups: intellectually skilled managers or technical experts, and much larger numbers of de-skilled and less valued laborers. According to this view, technology is a dependent variable in the social system which is developed for a purpose by a dominant class and subject to reshaping for new purposes under a new technology. However, the process by which this occurs and its eventual outcome must be negotiated between relevant social groups, in this case security professionals, policy makers, private technology companies, nonprofits and academic institutions, and civil liberties advocates. Nowhere is the attempt to impose hegemonic power structures over the development of broadband Internet and related technologies clearer than at their intersection with national security concerns.

In this regard, Der Derian noted the enormous impact the ability to "speak security" can have on a population's willingness to tolerate civil liberties violations. "No other concept in international relations packs the metaphysical punch, nor commands the disciplinary power of 'security,'" he claimed (in Nissenbaum, 2005, p. 69). As Nissenbaum (2005, pp. 64–65) observed, weaknesses in networked computer systems can be framed to legitimate a specific type of response. In a technical computer security frame, protection from threats focuses on attacks that threaten a system's availability or confidentiality. This focus is arguably driven by private interests rather than moral imperative. But computer security imbued with the moral force of national security promotes different strategies of protection. Thus interested actors construct the same technical situation in radically contrasting ways.

Further cementing the influence of hegemonic power structures are cybersecurity's focus on "hypothetical futures" or estimations of risk and threat (Buzan et al., 1998), and the reliance in security and technical fields on "experts" who are not always held accountable. Bigo remarked on the "lack of precision required for threats identified by the professionals who know some secrets. Amateurs always need to prove their claims, whereas professionals, whether international, national, or local, corporate or public, can evoke without demonstrating" (2002, p. 74). Indeed, Hansen and Nissenbaum (2009, p. 1168) argue that although cybersecurity is not uniquely reliant on technical, expert discourse, it is the field where "[technifications] have been able to take on a more privileged position than in any other security sector," as computer security often requires knowledge that is unavailable to the general public. This is important because the effect of "technifications," as speech acts similar to securitization, is that "they construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda, that technology serves" (ibid., p. 1167). The simultaneous use of both securitization and technification in cybersecurity discourse is therefore significant because they "work to prevent it from being politicized in that it is precisely through rational, technical discourse that securitization may 'hide' its own political roots" (ibid., p. 1168).

Increasingly, security agencies and law enforcement advance the securitizing argument. Resultant attempts to control the development of networked computing reflect a desire to know and to secure that is central to both the security of the state and society's normalization and productive functioning. Foucault discussed this as governmentality, a method of governance that protects, controls, and fosters economic expansion, and as such is inextricable from economic liberalism (2007). Surveillance in response to insecurity is a way of knowing a population, rendering it calculable and thereby manageable. It not only informs state action but also influences the way subjects think about themselves. This is evident in Foucault's illustration of the panopticon: surveillance (or the assumption of surveillance) induces in the subject "a state of conscious and permanent visibility that assures the automatic functioning of power" (1995, p. 201). Theoretically, this produces a disciplined, ordered, productive society without the need to enforce, punish, or necessarily carry out the surveillance in the first place. Similarly, Neocleous addressed police as a form of governmental power for the administration of society and active fabrication of social order (2000, p. 14).

In today's information society, surveillance is increasingly used to achieve not only a "panoptic" effect, but also an inversion of this concept sometimes referred to as the "nonopticon," wherein effective surveillance is contingent on people being unaware and unguarded (Vaidhyanathan, 2008). Feeling anonymous while being more monitored and trackable than ever before renders them calculable and truly known. Lyon (2003) argued that the information age allows for the use of surveillance as *social sorting*, that is, using the phenomenal amount of easily compiled, tracked, and analyzed personal information to manage populations by sorting subjects into social and economic categories assigned worth or risk. Surveillance is central to the administrative function of security and law enforcement, constituting populations of individuals, organizations, and institutions in their respective risk categories to provide the security needed for economic success (Haggerty & Ericson, 2006).

(Re)Securitizing the Internet: The Cyber-Threat Frame

It is no coincidence that the fields of security and technology both rely on privileged, expert knowledge. The origins of the Internet were closely tied to national security concerns. The first computer network, the Advanced Research Projects Agency Network (ARPANET), a U.S. military research project, was intended to ensure a robust communications system that would survive attack and be able to route around interruptions. However, as Abbate (1999) explained, the complex development of this Internet precursor involved academic networks, independent innovation by hobbyists, and military/security concerns. It was designed "to allow scientists to overcome the difficulties of running programs on remote computers" (ibid., p. 2), but evolved into something far more communication-oriented through what Abbate termed "an unusual and sometimes uneasy alliance between military and civilian interests" (ibid.). These private and economic concerns heavily influenced the direction this project would take.

In the early 1970s, few beyond the computer science community had heard of ARPANET. Economic concerns initially limited the wider, public application of such a system. As Saco (1999) noted, "because these networking concepts were radical, expensive, and untested . . . the actual development of a distributed, packet switching network posed too high an investment risk for the corporate sector" (p. 268). But over the following years, independent development of many separate networks and bulletin

board systems pointed to networked computing's wider commercial potential, not only for communication and research but also for making new friends and finding communities (Sterling, 1992). Restrictions on that commercial potential were alleviated when the military users of ARPANET, seeking greater access control to protect against malicious actors, separated from academic users, who wanted open access and information sharing (Abbate, 1999, p. 142). Once sensitive military activities were in their own separate network, ARPANET could feasibly be transferred to civilian control, where no need for similarly high levels of security was anticipated. No longer a military and, by extension, security medium, ARPANET became a public utility. This shift distanced networked computing from the idea of security.

The commercial Internet thus did not develop with security in mind. ARPANET was secure because it was a closed system with a small number of trusted users. Even after the military relinquished control and networked computing was commercially developed into the World Wide Web, its eventual use by a seemingly unlimited number of anonymous users for financial transactions, transmission of sensitive personal information, or government communications was unforeseen. In the 1980s the federal government encouraged expanded access to the Internet, and this very openness fostered the innovation and development that turned the Internet into an autonomous, anarchistic public-communications medium central to the economy, education, and culture (Sterling, 1992). As the Internet flourished, broadband service became a cutting-edge business for telecommunications companies in many countries. The development of high-speed Internet is a high priority on political-economic agendas the world over.

The computer industry's rapid growth and the resulting automation of many areas of society over the past several decades lend an element of inevitability to the military's renewed interest in the Internet and the security risks associated with networked computing. Bendrath (2003) explained how the terminology around computer security shifted in the 1990s, and drew strong connections between the threats posed to network security and historical threats to the state. But from another angle, the vulnerabilities of the Internet and related technologies are their greatest strengths, for even as the Internet's openness and flexibility make it vulnerable to manipulation and attack, they also make it resilient and effective for independent coordinated action, and for innovation. Bijker (2006) highlighted the importance of acknowledging this duality in risk assessment when he noted the need "to assess risks and benefits within one framework: risks cannot be evaluated without also evaluating the positive effects of the actions that generate them" (p. 57). Vulnerability is an objectively characterized weakness in the system, but whether it leads to good or bad outcomes depends on the interpretation and contextualization of those weaknesses—how they are constructed or framed.

As the power and potential of networked computing became apparent, controls were quickly developed to prevent uses of it that government did not intend or approve. Myriam Cavelty (2008) asserted that the resulting "cyberthreat" debate focused on reducing insecurity in two main domains: computer crime, and potential espionage involving federal computers. The former tended to focus on economic loss, the central offenses being "computer manipulation, computer sabotage, computer extortion, hacking, and computer espionage as well as software piracy and other forms of product piracy" (ibid., p. 45). The first effort to combat this kind of cyber threat resulted in the Computer Fraud and

Abuse Act (CFAA) of 1986.[3] Meanwhile, the national security domain's close link to foreign espionage and thus the debate on encryption led to the Computer Security Act of 1987 (ibid.). This would seem to suggest two discrete fields, but as we have established and will explain further, networked computing's centrality to national economic success gives computer crime a distinct national security dimension. Therefore, in the national-security-based worldview, any type of innovation or manipulation of programming that could challenge existing power structures is a threat to "the nation" that should be quashed. A few historical events illustrate how these initial legislative attempts at control in the name of national security have been used to enforce a more generalized sort of acceptable behavior in the service of capital.

Encryption and the Computer Security Act of 1987

The debate over encryption, unlike the development and use of the CFAA, has been positive for civil liberties. Arguably this is because the interests of industry have historically aligned with those of civil liberties groups in the case of encryption, whereas the latter are wary of the CFAA and its broad definitions, which could be used to protect national security and industry. The encryption debate "pitted the U.S. government against the private sector as the place where the main innovations in information technology were being made" (Cavelty, 2008, p. 52). Security agencies opposed encryption because it would create added difficulty for state surveillance, but industry encryption was prerequisite to developing e-commerce because users would need assurance of security before conducting their business online.

The conflict between national security imperatives on the one hand and commerce and privacy on the other was clear from the beginning of the encryption debate. The first legislation to regulate the development of computer encryption was the Computer Security Act of 1987, which sustained the link between cryptography and national security that had tightened since the code-breaking days of the Second World War. However, conflict arose over which national security department would lead in managing commercial cryptography's development. One obvious choice was the NSA, which had been created in 1952 to continue the code-breaking work of its wartime predecessor agencies. The NSA's responsibility "for both collection and analysis of message communications and for safeguarding the security of U.S. government communications against similar agencies elsewhere" (Cavelty, 2008, p. 49) reflects its long involvement in cryptography. Surprisingly, the NSA's stiffest competition came from the

[3] The act set a penalty of a fine and/or up to 20 years in prison for anyone who, among other things, accesses a computer without authorization. It also authorized the Secret Service—the Treasury's police—to investigate computer crimes, as computing was increasingly used for transferring and managing money (Cavelty, 2008). Five times, amendments to this act (including by the Patriot Act) expanded its reach. It now effectively encompasses all computers connected to the Internet. Thus the act has inextricably linked computer crime to both national security and financial crimes. Recent proposals to reform the act (notably a "cybersecurity" bill apparently prompted by a series of major breaches of U.S. technology companies' digital infrastructure by Chinese hackers) threaten to further broaden its potential use (Martinez, 2013).

Department of Commerce, which managed the federal standard for encrypting sensitive information, and from academia. Civilian-sector approaches were favored by those with concerns about the NSA's involvement in civilian computer security, who questioned "the appropriate role of defence and intelligence agencies in civilian matters and how openness and free-market forces can coexist with secret operations and restrictions on sensitive information" (ibid., pp. 50–52).

This debate had been going on for years. Presidential directives had tended to prefer the NSA for controlling encryption, whereas Congress promoted a civilian-centered approach. By 1984 the conflict had all but been decided in favor of civilian control when Ronald Reagan authorized National Security Decision Directive (NSDD) 145 on Telecommunication and Computer Security. NSDD 145 proposed a range of expansions to NSA control over information that might adversely affect national security (Electronic Privacy Information Center [EPIC], n.d.). Jerry Berman of the American Civil Liberties Union highlighted growing criticism from academics, businesspeople, and civil libertarians who saw NSDD 145 as part of a broader campaign to control access to information. Berman (1987) asserted that

> the government is using a variety of means, from appeals to patriotism to threats of prosecution under the export control laws, to have unclassified technical papers withdrawn from scientific conferences . . . and to prevent publication of scientific and technical papers. (p. 2)

The scope of NSDD 145 was further broadened over the following years to encompass a range of "sensitive information" that might affect federal interests.

The argument for freedom of information was part of a growing civil liberties discourse promoting the view that a military organization should not be given control over the realm of civilian security. Eventually, the Computer Security Act of 1987 was used to bring government-wide security standards under the authority of a civilian department once again, thus limiting NSA involvement (ibid., p. 7). The law reaffirmed the authority of the National Institute for Standards and Technology (NIST)—a division of the Department of Commerce—over nonmilitary government computer systems, relegating the NSA to a technical assistance role (EPIC, n.d.). But despite this clear legal reframing, President George H. W. Bush continued Reagan's policy of promoting NSA authority over cybersecurity by approving National Security Directive 42 (NSD 42) in 1990. This document reiterated many points of NSDD 145 and gave the NSA authority over "national security systems," thus removing the distinction between military and civilian networks (Cavelty, 2008).

These scuffles over jurisdiction defined the terms of the cybersecurity question, thus directly affecting the outcome of the encryption debate when it culminated in the early 1990s. In 1991, then Chairman of the Senate Judiciary Committee Joe Biden introduced the Comprehensive Counter-Terrorism Act. This anti-encryption bill mandated that communications service providers possess the capability for the government to obtain the decrypted or "plain text" contents of communications when legally authorized, thus building "backdoors" into the system (Markoff, 1991). Part of a broader move toward outlawing encryption, the bill was derailed in 1991, when cryptographer Philip Zimmermann created a strong encryption program called Pretty Good Privacy (PGP) and distributed it for public use through

bulletin boards across the United States. At the time Zimmermann (1991) cited Biden's bill as one reason he had decided to publish PGP "online" for free.

Zimmermann's program was meant for personal computers and the protection of individuals' privacy, so some argued that his distribution of the program was protected under freedom of speech. But cryptography was classified as "arms" under export law, as strong encryption hampered foreign surveillance efforts. Because the Internet allows for the distribution of software across borders, "it has allowed a form of distribution that bypasses customs checkpoints, calling into question the state's capacity to regulate the flow of a different kind of strategic item (digital information) through a new distributional channel" (Saco, 1999, p. 262).

The Internet's ability to transgress national borders "challenges conventional ways of thinking about space, sovereignty, and security" (ibid.), casting doubt on state authority and causing great anxiety for security advisers. Therefore Zimmermann's act of making strong encryption openly available became constructed as a national security issue. This construction embodied the views of security experts, the Clinton administration, and government agencies like the FBI and NSA, which emphasized the need to be able to intercept and decrypt communications for public safety and national security purposes (Saco, 1999).

On the other side of the debate, civil liberties groups like the Electronic Frontier Foundation argued that strong encryption was needed to protect the individual's right to privacy. Aligned with Internet freedom groups, in these early days, were software companies concerned about losing out to foreign competitors unhampered by the state's policy on weak encryption (ibid.). The government's actions to maintain control and the sovereignty within its borders had the cumulative effect of limiting innovation. Zimmermann's situation highlighted the underlying complexity of this dynamic, as officials originally became aware of PGP when the company RSA Data Security reported Zimmermann to customs investigators, claiming the software infringed on its intellectual property rights (Diffie & Landau, 2007). Software developers were not a homogenous group. Some objected to the government's restrictive methods and favored open innovation, while others cooperated with government, using the export restrictions to enforce copyright and accepting hefty contracts to produce NSA-compliant programs.

For more than a year, the cryptography community watched carefully as a grand jury heard Zimmermann's case. Meanwhile, PGP spread internationally, and developers were improving it and reimporting the software to the United States. The intellectual property issue became moot when RSA permitted a "legal" U.S. version of PGP (Diffie & Landau, 2007).

In the end, the Department of Justice let the case drop. It is unclear if this related to the central issue of whether publishing to the Internet can actually be considered an "export," rather than the simple exercise of free speech. But significantly, Zimmermann's publication was not the only one at issue: The MIT Press had published the PGP code as a 600-page book and proceeded to sell it to its international market. As Diffie and Landau noted, "had the government prosecuted Zimmermann and not gone after MIT, it would have invited scorn. But MIT was three times as old as NSA, just as well funded, and even more influential in the military-industrial complex" (ibid., p. 230). Apparently even the national security

argument was no match for the financial might of the publishing industry. This power struggle over the interests of security agencies, technology companies, and groups promoting open access became even more complex as the "Crypto Wars" raged on.

The Clipper Chip (1995)

The Crypto Wars were the setting for the debate over the "Clipper Chip." In the early 1990s, export restrictions and the general lack of direction in national encryption policy were significantly impeding innovation and the development of secure systems (Diffie & Landau, 2007). The NSA's position was complicated by its dual responsibility to secure and to break into information systems. Attempting to meet the growing economic and governmental need for secure communications with a solution that also heeded the national security imperative of easy access to foreign communications, the Clinton administration advocated use of the NSA-developed scheme known as Capstone. Relying on a telephone encryption technology called the "Clipper chip," Capstone attempted to secure phone conversations while still allowing for surveillance: "If both callers used a special phone, anyone with a wiretap on either end of the call would hear garbled noise, unless the key for lawful intercept by authorities was used" (Duggan, 2013, para. 5). With a warrant, government entities could access the two corresponding wiretap "keys," held in two separate locations, which would decode the messages or data. The Capstone computer adaptation would allow communications to be encrypted, thus providing privacy, but the government would keep a decryption key in case this privacy was abused for criminal or terrorist activity (the NIST would hold this key, illustrating once more the continuing closely coupled interests of national security and commerce) (ibid.). Unsurprisingly, solving the encryption debate by giving the government a key to decode private data was an unpopular approach that was criticized in the media. Saco (1999) noted that "instead of the breachable 'privacy' that key-escrow programs offer, opponents favor the 'Pretty Good Privacy' that Zimmerman's program promises and, by all accounts, delivers" (p. 271).

The reception within the software industry was not positive overall, as the NSA's plan limited developers, who would be given tamper-resistant chips to use rather than having full control over their products and designing them to meet a standard. Furthermore, algorithms could not be exported without government approval, which would limit the market and thereby constrain innovation around cryptography. In addition, the government would decide which companies would have access to the approved encryption. As Diffie and Landau (2007) noted, "the computer industry had been characterized by rapid and nimble developments; to many observers, this federal standard seemed to bode steep bureaucratic hurdles for any product that included security" (p. 237).

Media coverage of the proposed project revealed the public and private spheres' highly critical reactions to government regulations purporting to increase cybersecurity while having the side effect of limiting the economy. For example, a *USA Today* editorial (Editorial, 1995) defined cybersecurity not in national security terms, but as the degree to which the Internet is "safe for business" (para. 1), something to be achieved through powerful encryption. Yet such encryption was "blocked by government export regulations that make the programs difficult if not impossible to market, even for domestic purposes" (ibid., para. 4). Framed as the antithesis of successful business, government regulation was proclaimed to be "not right," and moreover "not necessary" (ibid., para. 5–6). Media criticisms incorporated civil liberties

concerns, implying that the regulation would primarily damage citizens' right to privacy.

The opposition to the state's encryption policy pushed the government to do discursive work of its own in an attempt to reframe the debate. It thus presented the Clipper chip as a choice, which, Saco (1999) argued, "reinforces the liberal assumption that private persons (both individual and corporate) can and should be able to make choices" (p. 273); as a result "the liberal state appears more neutral on the issue of surveillance than it might otherwise seem if it made key escrow compulsory" (ibid.). Escrow proponents also conducted a largely unsuccessful public relations campaign to reframe the issue as one of "data recovery," arguing that if an encryption key is lost, the information becomes useless without a spare. This argument lost force when applied to communications, which are less likely to require data recovery after the fact (although e-mail does blur this distinction) (Diffie & Landau, 2007). The attempt to create the illusion of choice went a step further in 1995, when the Clinton administration established a joint defense–civilian board that tried to protect electronic transactions by combining commercial and federal methods: Private entities would hold a "commercial escrow," and software companies willing to build wiretap escrow keys into their products were offered export privileges (Saco, 1999, p. 282).

By 1996, though, the debate over encryption seemed decided. The Clipper debate had prompted Congress to task the National Research Council with producing a report on cryptography. Despite the many defense and security agency professionals on the research team, the report concluded that cryptography should be broadly available to all legitimate elements of U.S. society, that current U.S. policy was "inadequate for the security requirements of an information society," and that "current export policy hampered the domestic use of strong cryptosystems" (Diffie & Landau, 2007, p. 243).

In the mid-late 1990s the government's approach to cryptography began to shift. Congress was divided, but significant factions within government were interested in having strong encryption. The NSA's algorithm had been cracked several times, proving far from foolproof. So as of 1997, when the aging Data Encryption Standard was slated for replacement by what would be called the Advanced Encryption Standard, the process of determining criteria, accepting submissions, and testing encryption was far more stringent than in the past, and many submissions (including the winner) came from non-U.S. programmers. All the while, the government was trying to cut costs by buying "off-the-shelf" equipment, as it was economically untenable to pay industry to create a secure government version and a Clipper-chipped, export-friendly public version. In addition, some cryptographers simply ignored export rules and published their codes anyway. One programmer—Daniel Bernstein at the University of California, Berkeley—used the free speech argument to challenge the export rules and won in the District Court and the Appeals Court for the Ninth Circuit. Then in 1998, the global spying apparatus ECHELON became public knowledge. Europeans' realization that the United States was spying on its allies for commercial purposes prompted them to develop stronger encryption while relaxing their export laws, thereby pressuring the United States to do likewise. Finally, after the Security and Freedom Through Encryption Act—which called for relaxing export controls, promoting strong encryption, and prohibiting mandatory key escrow—passed through several committees in 1999, the White House kept control of the situation by relaxing export restrictions on its own. Meanwhile the Clipper chip projects quietly disappeared from public view (Diffie & Landau, 2007).

Together with the failure of the Clipper chip and the push for stronger encryption standards, the eventual relaxation of export controls in the late 1990s looked like a major victory for civil rights activists, advocates of openness and innovation, and proponents of strong encryption. Now, in the wake of the Snowden disclosures, this outcome of the Crypto Wars seems less a victory than a change of tack in which the NSA shifted from controlling encryption by legal methods to exploring ways to circumvent cryptography.

Legislating Surveillance

The large security products market that many had presumed would emerge after restrictions on cryptographic innovation were eased was not forthcoming, and adoption of encryption was much slower than expected. But the gradual uptake of strong encryption has not kept the government from gathering massive amounts of communications data. In fact, even as opposition to the Clipper chip was opening up the debate over civil liberties and cryptography, legislators were drafting the foundation of the modern state surveillance system: the 1994 Communications Assistance to Law Enforcement Act (CALEA). After several years of campaigning, the FBI managed to get CALEA passed, citing complications posed to wiretapping by the non-standardized telephone systems and new technologies proliferating after the Bell System telephone monopoly breakup (Landau, 2003). The encouragement of strong encryption did present difficulties for intercepting digital communications. But more crucially, as Marc Rotenberg et al. noted, "CALEA established for the first time the premise that the government had the authority to require by law that new communication services be designed to enable surveillance by the state" (in Landau, 2003, pp. 112–113).

Again, government efforts to expand surveillance powers had to be framed carefully, especially regarding private industry. The abysmal failure of the military and Department of Homeland Security initiative known as Total Information Awareness (TIA) is an example of the importance of perception on the success or failure of an information initiative. Developed in 2002 in response to 9/11, TIA was described by the Cato Institute as "a colossal effort to assemble and 'mine' massive databases of our credit-card purchases, car rentals, airline tickets, official records, and the like" with the aim of monitoring "the public's whereabouts, movements, and transactions to glean suspicious patterns that indicate terrorist planning and other shenanigans" (Crews, 2002, para. 1). With its unflinchingly honest title, its Orwellian logo of the Great Seal of the United States topped by an all-seeing eye, and the slogan "knowledge is power," TIA was a hard sell, even in the wake of the patriotic fervor and paranoia created by the 9/11 terrorist attacks. Significantly, however, it was not only privacy advocates who took umbrage but members of industry too. Companies that flourished in the information economy and relied on electronic commerce feared that TIA would destroy corporate America's ability to credibly assure customers' privacy and security (ibid.). Further, as a Cato Institute critique noted about this national security effort's potentially limiting impact on the economy,

> if the TIA project ends up routinely requiring banks, airlines, hotels, Internet-service providers, and other businesses to hand over such private information, it will undermine evolving commercial-privacy standards, drive transactions underground, and make criminals out of ordinary people who simply want to be left alone. (ibid., para. 6).

Congress defunded the controversial project in 2003, but many of its functions were redistributed to classified programs (Electronic Frontier Foundation, 2003).

Facing an insurmountable public relations battle that pitted privacy and industry concerns against the national security imperative, TIA lost—or at least quietly withdrew. But intelligence agencies still strive toward the ideal of developing a massive database of information to be mined. Amendments to CALEA have greatly expanded the types of domestic communications data accessible to the FBI, allowing for the use of "subpoenas, warrants, and National Security Letters to get email; pen registers, traditional wiretaps, and cell-phone eavesdropping tools to get telephone data; and all the powers set forth in the original CALEA to monitor most Internet communications" (Duggan, 2013, para. 6). The development of strong encryption has complicated this effort but does not impede it. In fact, Ryan Singel (2010) reported in *Wired* that despite the oft-repeated argument that strong encryption allows criminals and terrorists to hide their unlawful activities, "investigators encountered encrypted communications only one time during 2009's wiretaps [and the] state investigators told the [Administrative Office of the U.S. Courts] that the encryption did not prevent them from getting the plain text of the messages" (para. 6). In short, encryption has not greatly diminished the intelligence community's drive to accumulate data on U.S. citizens in the name of national security, though the opposition of privacy groups and private industry has forced it underground.

Even so, encryption has complicated this surveillance effort enough that in 2010 the cryptography debate was rekindled when the Obama administration introduced a bill that, much like Joe Biden's bill in 1991, would require all service providers—including encrypted e-mail services like Blackberry, social networking sites like Facebook, and VOIP services like Skype—to have the capacity to intercept and decrypt communications when required by court order (Savage, 2010). Following the pattern of earlier encryption debates, the bill would have made it illegal to offer completely secure encrypted communications whose decryption key was held by the customer but not also by the service provider (McCullagh, 2010). Similarly, the insidious TIA project evidently has survived Congressional defunding because the money was redistributed to the "black budget" used to fund classified operations like the strikingly similar PRISM (Harris, 2013), supported by a massive state-of-the-art facility in Utah (Bamford, 2012).

But surveillance is only useful when equipped with the concomitant ability to understand and analyze that information. As Snowden claimed, "encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on" (in Schneier, 2013, para. 14). So besides pursuing decryption capabilities, the NSA has developed a range of alternate methods for gathering information. For example, much can be learned simply by looking at communications metadata, which is not encrypted and indicates who spoke to whom, when, from where, for how long, how often, and using what programs. Snowden's documents also highlighted a program called Tailored Access Operations that has given a team of skilled hackers an almost unlimited budget to develop innovative methods of targeting "end point devices" ("Inside TAO," 2013b). Likewise, when targeting the contents of communications, the most effective way to gather data may be to tap directly into communications networks by secret agreement with telecommunications companies; or attack network devices; or ensure that surveillance capabilities

are already built into routers, switches, and firewalls; or collude with encryption software developers to intentionally weaken cryptographic systems by ensuring backdoors are built into code itself (Schneier, 2013).

It seems significant that, rather than engage in yet another public relations battle over national security agencies' need for decryption capabilities, organizations like the NSA can now draw on the greatly expanded powers facilitated by the Patriot Act to bypass debate entirely. By concealing its development of more advanced code-breaking capabilities, undermining strong encryption, and infiltrating communications networks—all with the assistance of private industry—the NSA has managed to avoid the censure of privacy advocates and work with the technology industry, giving it the freedom to continue innovating instead of placing limits on it (Schneier, 2013).

Conclusion

This history of networked computing has attempted to illuminate how the interests of national security professionals and private industry—particularly technology companies—have influenced its governance. Yet the argument for protecting civil liberties cannot be dismissed, for it becomes a powerful rhetorical force when aligned with the interests of private industry. Early on, the comparative lack of regulation allowed the Internet to spread rapidly. The popularity of networked computing and its potential for economic growth spurred its rapid development and the innovation of all kinds of new communications technologies. But with its mass uptake and integration into all areas of society, the Internet has also presented areas of vulnerability that malicious actors could exploit. It has also presented government with access to a wellspring of data on individuals throughout the United States and worldwide, and opportunity to surveil potentially malicious actors. The reaction to the September 11, 2001 terrorist attacks exacerbated this state of affairs by promoting a new conceptualization of security in which everyone is a potential threat and therefore everyone is suspect, an attitude strongly reminiscent of anti-Communist fears and initiatives (Lyon, 2003). As Chandler (2008) observed, "since terrorism (particularly suicide terrorism) is not easily deterred by punishment after the fact, the pressure to detect and preempt terrorist plots is strong. Increased surveillance is therefore a predictable response to a dramatic terrorist attack" (p. 125). Computerization and the extensive incorporation of digital technologies into everyday life have made it increasingly possible to process and analyze huge amounts of digital information, providing opportunity for surveillance as never before (Haggerty & Ericson, 2006).

Therefore security professionals, as "experts" with access to special knowledge, have heavily influenced decisions around the development and governance of this technology. How well these actors "speak security" has an enormous impact on the population's willingness to tolerate violations of its civil liberties and more, for safety's sake. This understanding that safety comes at a price suggests that security is mainly about sacrifice: of people, through determinations of whose survival is needed; and of values, as violence and coercion are legitimized as an inevitable side effect of security (Bigo & Tsoukala, 2008). Yet the Internet is still a contested technology, and decisions about its development and governance are made through a process of negotiation. Though the rhetoric of security may hold sway, the input of private industry and civil libertarians will influence the success of security arguments.

Snowden's revelations may have tilted the balance back in favor of civil liberties as the realities of mass surveillance give citizens, businesses, and foreign governments pause. The NSA's surveillance system was justified with the rhetoric of security, which insisted it was necessary to protect law-abiding citizens by targeting criminals and terrorists. Now security professionals are struggling to use this rhetoric to justify indiscriminate surveillance of all communications that pass through U.S. networks.

As Der Derain, the Copenhagen School, and many others have noted, national security is a powerful ideological motivator. But the massive U.S. surveillance effort facilitated by securitizing rhetoric has a troubled relationship with private corporations, particularly in the technology industry on which it depends. A group of concerned cryptologists recently responded to Snowden's revelations with an open letter that illustrates the weakening of the national security argument when it remarks that "the value of society-wide surveillance in preventing terrorism is unclear, but the threat that such surveillance poses to privacy, democracy, and the US technology sector is readily apparent" (Abadi et al., 2014, para. 3). However, some are uneasy about grouping civil liberties together with private industry concerns. Though the interests of civil libertarians and private businesses have strategically aligned at times to combat securitizing arguments, their ultimate goals have not always been compatible. The renewed interest in privacy concerns in the context of international trade may be giving the U.S. government pause as it attempts to allay fears over the surveillance it conducts, but some are hesitant to forge ahead with a discussion of privacy within a foreign trade framework, questioning whether trade negotiations are an appropriate site for discussion of international standards for privacy legislation (Millán, 2013). Once again, Snowden's revelations have exposed how intimately the decision making in the development and governance of networked technologies relates to national security or economic arguments. How closely these positions align with civil liberties concerns will make all the difference in how much privacy and openness are built into these technologies by design.

References

Abadi, M., Abelson, H., Acquisti, A., Barak, B., Bellare, M., Bellovin, S. et al. (2014, January 24). An open letter from US researchers in cryptography and information security. Retrieved from http://masssurveillance.info

Abbate, J. (1999). *Inventing the Internet.* Cambridge, MA: MIT Press.

Austin, J. (1975). *How to do things with words*. Cambridge, MA: Harvard University Press.

Bamford, J. (2012, March 15). The NSA is building the country's biggest spy center. *Wired.* Retrieved from http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter

Bendrath, R. (2003). The American cyber-angst and the real world: Any link? In R. Latham (Ed.), *Bombs and bandwidth: The emerging relationship between information technology and security* (pp. 49–73). New York, NY: The New Press.

Berman, J. (1987). National security vs. access to computer databases: A new threat to freedom of information. *First Principles*, *12*(3), 1–7.

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. *Alternatives*, *27*, 63–92.

Bigo, D., & Tsoukala, A. (2008). *Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11*. London, UK: Routledge.

Bijker, W. (2006). The vulnerability of technological culture. In H. Nowotny (Ed.), *Cultures of technology and the quest for innovation* (pp. 52–69). New York, NY: Berghahn Books.

Buzan, B. (Ed.). (2004). *The United States and the great powers: World politics in the twenty-first century*. Cambridge, UK: Polity Press.

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner.

Cavelty, M. D. (2008). *Cyber-security and threat politics: U.S. efforts to secure the information age*. London, UK: Routledge.

Chandler, J. (2008). Privacy versus national security: Clarifying the trade-off. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *On the identity trail: Anonymity, privacy and identity in a networked society* (pp. 121–138). Oxford, UK: Oxford University Press.

Crawford, S. (2012, January 9). Name-calling on the Internet is serious business. *Bloomberg*

Businessweek. Retrieved from http://www.businessweek.com/news/2012-01-09/name-calling-on-the-internet-is-serious-business-susan-crawford.html

Crews, C. W. (2002, November 26). The Pentagon's total information awareness project: Americans under the microscope? *Cato Institute.* Retrieved from http://www.cato.org/publications/techknowledge/pentagons-total-information-awareness-project-americans-under-microscope

Diffie, W., & Landau, E. (1998). *Privacy on the line: The politics of wiretapping and encryption*. Cambridge, MA: MIT Press.

Duggan, B. (2013, May 23). Government plan to build "back doors" for online surveillance could create dangerous vulnerabilities. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2013/05/23/calea_reform_to_build_back_doors_into_online_communications_could_create.html

Editorial: One little change could end cyber-security woes [Editorial]. (1995, October 24). *USA Today*, p. 12A.

Edward Snowden interview: The NSA and its willing helpers. (2013a, July 8). *Der Spiegel*. Retrieved from http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html

Electronic Frontier Foundation (2003, September 30). Total/terrorism information awareness (TIA): Is it truly dead? *Electronic Frontier Foundation.* Retrieved from https://w2.eff.org/Privacy/TIA/20031003_comments.php

Electronic Privacy Information Center (EPIC). (n.d.) Computer Security Act of 1987. *Epic.org*. Retrieved from http://epic.org/crypto/csa

Eriksson, J., & Giacomello, G. (2007). *Introduction: Closing the gap between international relations theory and studies of digital-age security*. In J. Eriksson & G. Giacomello (Eds.), *International relations and security in the digital age* (pp. 1–29). New York, NY: Routledge.

Feenberg, A. (1991). Critical theory of technology. Oxford, UK: Oxford University Press.

Foucault, M. (1995). *Discipline and punish: The birth of the prison*. New York, NY: Vintage.

Foucault, M. (2007). *Security, territory, population: Lectures at the College de France 1977–1978* (Graham Burchell, Trans.). New York, NY: Palgrave Macmillan.

Haggerty, K., & Ericson, R. (2006). *The new politics of surveillance and visibility*. Toronto, Canada: University of Toronto Press.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53(4)*, 1155–1175.

Harris, S. (2013, June 19). Total recall. *Foreign Policy*. Retrieved from http://www.foreignpolicy.com/articles/2013/06/19/total_information_awareness_prism_nsa_bush_poindexter

Inside TAO: Documents reveal top NSA hacking unit. (2013b, December 29). *Der Spiegel*. Retrieved from http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

Landau, S. (2003). *The transformation of global surveillance*. In R. Latham (Ed.), *Bombs and bandwidth: The emerging relationship between information technology and security* (pp. 49–73). New York, NY: The New Press.

Lyon, D. (2003). *Surveillance after September 11*. Cambridge, UK: Polity Press.

Markoff, J. (1991, April 17). Move on unscrambling of messages is assailed. *The New York Times*. Retrieved from http://www.nytimes.com/1991/04/17/business/move-on-unscrambling-of-messages-is-assailed.html

Martinez, J. (2013, March 25). Draft house judiciary cybersecurity bill would stiffen anti-hacking law. *The Hill*. Retrieved from http://thehill.com/blogs/hillicon-valley/technology/290103-draft-cybersecurity-bill-aims-to-stiffen-computer-hacking-law

McCullagh, D. (2010, September 27). Report: Feds to push for net encryption backdoors. *CNET.* Retrieved from http://news.cnet.com/8301-31921_3-20017671-281.html

Millán, L. (2013, September 30). Regulating the flow of data. *National Magazine*. Retrieved from http://www.nationalmagazine.ca/Articles/Sept-Oct-2013/Privacy-and-the-digital-economy.aspx

Neocleous, M. (2000). *The fabrication of social order*. London, UK: Pluto Press.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology, 7*(2), 61–73.

Poitras, L., & Greenwald, G. (2013, June 9). NSA whistleblower Edward Snowden: "I don't want to live in a society that does these sort of things"—video [Online broadcast]. *The Guardian*. Retrieved from http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

Saco, D. (1999). Colonizing cyberspace: National security and the Internet. In J. Weldes, M. Laffey, H. Gusterson, & R. Duvall (Eds.), *Cultures of insecurity: States, communities, and the production of*

danger (pp. 261–292). Minneapolis: University of Minnesota Press.

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?pagewanted=all&_r=0

Schneier, B. (2013, September 15). How to remain secure against the NSA. *Schneier on security*. Retrieved from https://www.schneier.com/blog/archives/2013/09/how_to_remain_s.html

Singel, R. (2010, April 30). Police wiretapping jumps 26 percent. *Wired.* Retrieved from http://www.wired.com/threatlevel/2010/04/wiretapping

Sterling, B. (1992). *The hacker crackdown*. New York, NY: Bantam Books.

Vaidhyanathan, S. (2008, February 15). Naked in the "Nonopticon." *The Chronicle of Higher Education*. Retrieved from http://chronicle.com/article/Naked-in-the-Nonopticon-/6197

Zimmermann, P. (1991). Why I wrote PGP. *Philip Zimmerman.* Retrieved from http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven, CT: Yale University Press.