The Privacy Paradox: Privacy, Surveillance, and Encryption

Karina Rider

A thesis

submitted in partial fulfillment of the

requirements for the degree of

Master of Arts

University of Washington

2016

Committee:

Sarah Quinn

Emilio Zagheni

Program Authorized to Offer Degree:

Sociology

University of Washington

Abstract

The Privacy Paradox: Privacy, Surveillance, and Encryption

Karina Rider

Chair of the Supervisory Committee:

Dr. Sarah Quinn

Department of Sociology

In most privacy studies, privacy is assumed to be antithetical to surveillance. However, some critics have warned that privacy-based criticisms may actually facilitate surveillance by narrowing the terms of the debate in such a way as to render these critiques ineffective. That being said, we do not yet have data that shows whether privacy claims were used in the past to legitimate government surveillance. This paper addresses that gap by analyzing claims made over one of the U.S.'s most controversial surveillance issues: government control over encryption technologies. A review of Congressional hearings and statements on the Congressional Record (n=112) reveals that from 1993-99, public debates were dominated by a *market liberalization* discourse in which participants supported encryption deregulation as a way to protect privacy from criminal intrusion in market transactions. Also playing a role was a strong skepticism toward government power and a preference for markets as managers of crime

prevention. Challenged by these critiques, lawmakers withdrew regulatory proposals and spent the following decade working quietly with private firms. Current debates about the FBI's "Going Dark" initiative demonstrate the *market liberalization* discourse has been fully accepted to the point that it is presumed, rather than debated. Instead, current discussions focus on court orders, rather than market policy. These findings show the *expansion* of privacy for consumers and entrepreneurs has in fact been successfully used to justify the *contraction* of privacy from law enforcement and intelligence agencies.

In February 2016, news outlets reported the FBI had ordered Apple to open an iPhone used by suspects in a shooting in San Bernadino, California. Apple refused to unlock the phone, leading to intense media attention and the possibility of a courtroom showdown. Although the FBI withdrew from proceedings after claiming it had found a method for entering the device without Apple's assistance, the public debate about the extent to which encryption should be used and regulated has continued. This dispute has a long history, however. The Clinton administration initiated the first highly publicized push to regulate encryption in 1993, sparking debates known as the "Crypto Wars." Privacy advocates have referred to the eventual withdrawal of these proposals in the 1990s as evidence of the successes possible when groups organize around privacy issues. But was the outcome of these debates an unqualified victory for civil liberties groups? What was the role of privacy critiques in deregulating encryption, and what does it tell us about how privacy critiques are mobilized in practice?

In this paper, I propose that privacy must be understood as a sociological phenomenon, rather than a legal concept that varies in degree of presence over time. Appeals to privacy – like promises of security or cost-efficiency – should be conceptualized as a political tool stakeholders deploy to achieve certain ends. As I will show, appeals to privacy protection in market contexts can be used to stimulate surveillance from law enforcement. I argue these appeals must be understood as emerging from a specific sociohistorical context, namely the American political distrust of centralized government power and reliance on market mechanisms for delivering a variety of social services. Lastly, the findings of this paper suggest the emerging field of surveillance studies would benefit from conversations with economic sociology.

Privacy: Surveillance Critique?

Surveillance studies scholars have recently questioned the effectiveness of privacy as a critique of surveillance. For some, the positioning of the right to privacy as a negative right – meaning it is always on the defensive *from* invasions and threats, rather than being something that can be achieved in and of itself – means that it is ill-equipped to check the spread of surveillance technologies. One issue that arises from mobilizing privacy critiques against surveillance programs is that what it means for privacy to be protected is often reduced to a matter of whether particular procedures of information access are in place. As Gilliom (2011:503) argues, "privacy has, for the most part, become a *procedural* order, not a substantive guarantee: if the rules are followed (consent forms, warrants, boilerplate notifications) then the objections are null." These procedures are often vague, nonenforceable, or at worst deliberately misleading. Privacy statements provided by corporations – far from protecting privacy and ensuring users are aware of the uses of their data – typically amount to no more than legal cover for surveillance activities (Fernback and Papacharissi 2007).

In their study of the development of closed-circuit television (CCTV) in Germany, Möllers and Halterlein (2013) found that privacy was the only critique mobilized against smart CCTV systems. The authors conclude that "how this discourse defined personal liberty was reduced to privacy regulations" at the expense of discussions of broader structural issues, such as the automation of labor, discriminatory outcomes for those under surveillance, and the assumption that more CCTV deters crime (Möllers and Halterlein 2013:66). Determinations as to whether privacy was threatened were based on the extent to which smart CCTV was believed to violate existing privacy statutes. However, the authors go beyond the conclusion that narrow definitions of privacy violations render privacy an inadequate critique of surveillance by

suggesting privacy critiques can legitimate surveillance systems. For example, for smart CCTV to be considered a legitimate technology in public discourse, it must meet the requirements of privacy guidelines. If these requirements are met, the technology is legitimate. Thus, by having privacy procedures in place, surveillance technologies do not appear to constitute privacy violations.

For Coll (2014), relying on narrow definitions for what constitutes a privacy violation is a logical consequence of attempts to regulate privacy. Drawing parallels to Foucault's (1985) history of sexuality – in particular the idea of the dispositive of power – Coll (2014:1260) argues privacy advocates, scholars, data protection laws, privacy policies, and the focus on educating individuals to be aware of and control their personal information constitute a form of biopower that produces subjects of privacy. Coll (2014:1260) concludes that privacy and surveillance "seem to work together in the deployment of the surveillance society. The more that is said about privacy, the more consumers focus on their individuality, reinforcing the *care of the self* … which shapes them as the subjects of control." However, in this account, the role of the state remains ambiguous. In explaining the development of *objective privacy* – that is, privacy reduced to its personal information dimension – Coll (2014) points out that governments tend to rely on this definition of privacy when debating and enacting policy. The conclusion is that "no one would blame the legislature for this tendency, as these laws are primarily intended to thwart the damage that could be produced by the increasing digitization of personal data" (p. 1252). By claiming governments are simply reflecting this definition of privacy – one that is assumed to be pushed by informational capitalists – important connections between the development of private sector privacy measures and state surveillance capabilities are hidden from analysis.

On the other hand, some researchers advocate for the continued use of privacy as a criticism of surveillance. For example, while Lyon (2015) acknowledges that privacy "is made to do much work" (p. 96) in critiques of surveillance, it still "is a robust way of questioning the growth of surveillance, and is undoubtedly the most widely used platform for mobilizing opposition to unnecessary and especially mass surveillance" (p. 98). Brown (2013) similarly acknowledges that privacy is often mobilized as a sweeping critique of surveillance, but concludes that this is not necessarily harmful. Instead, privacy acts to unify individuals around a shared concept, allowing them to build solidarity around a multitude of interconnected concerns. Bennett (2011) also takes a strong stance against common critiques of privacy as an antidote to surveillance. Citing contemporary conceptualizations of privacy (such as Nissenbaum's [2009] contextual integrity), he contends that much of the criticisms outlined above are either strawmen or based on outdated definitions of privacy. Bennett (2011) argues privacy theorists, such as Nissenbaum (2009), have moved beyond typical liberal notions of privacy that were the subject of Gilliom's (2011) critique.

I argue that such debates would benefit from a conversation with strands of research in economic sociology. Several researchers in the institutionalist tradition have interrogated the relationship between political cultures and various policy prescriptions. Dobbin (2001), for example, argues that the American political culture values a hands-off government that does not interfere in the affairs of private citizens. Policymakers drew upon this principle when designing rail policy, opting to refrain from regulating the industry. Fourcade (2009:33) makes a similar case, pointing out that an early emphasis on individual self-determination resulted in "the development of central government authority in America that has always been subject to suspicion, if not outright hostility." Fourcade (2009) further argues that in the U.S., markets are

seen as both the structure and law of the economy. Thus, "markets are not only the best mechanism, but really the only *legally admissible* mechanism for promoting economic growth and efficiency" (p. 36). How these ideas are transformed into specific policy directions can be understood as a product of existing taken-for-granted assumptions about the appropriate relationship between the state and the economy, the parsimony of a given policy prescription, and actors' efforts to legitimize these prescriptions by drawing on symbols and concepts that resonate with the public (Campbell 1998).

Drawing on these ideas from economic sociology, this paper investigates how the privacy-surveillance relationship operates within U.S. policymaking structures. In doing so, this paper addresses a gap in the surveillance studies literature. Of the studies that identify contradictory effects of privacy critiques, many fail to take a historical approach. I argue that such an approach is necessary for identifying the effects of privacy critiques on the development of surveillance technologies because the only way to identify which arguments impact regulatory policy is to take a historical view. Furthermore, for the most part, the above studies center privacy as the ultimate object of analysis. By centering privacy, these studies miss the broader context in which privacy discourses are situated – such as neoliberal and "tough on crime" discourses – and thus fail to identify how privacy relates to broader critiques of surveillance policy. Therefore, taking my cue from Möllers and Halterlein (2013), I decenter privacy in my analysis in order to broaden the possibilities for how privacy operates. I begin by asking: what were the "Crypto Wars" *about*, and what were the main issues being debated? I then analyze how privacy functions in these arguments, in order identify the role of privacy in overall opposition to surveillance policy. This decentering ensures that privacy is not *a priori* treated as the primary critique of surveillance, and allows for more nuanced analysis regarding the role of

privacy-based opposition in checking the development of surveillance capacities. Lastly, I do not assume a definition of privacy prior to my analysis. Instead, definitions of privacy used in this paper are purely data-driven, allowing for simultaneous – and even contradictory – definitions of privacy to co-exist in the same space.

METHODS

To answer these questions, I conducted inductive qualitative content analysis (QCA). QCA was the most appropriate approach for addressing these questions because it allowed for an in-depth analysis of the construction of meaning and interpreting textual materials. One of the goals of QCA is to systematically describe the meaning of the chosen material (Schreier 2013). It does so in a way that focuses on selected aspects of the texts that are relevant in answering the research questions. Thus, due to the specific relationship investigated in this paper – privacy and surveillance – being selective in material is essential. Lastly, the systematic nature of QCA makes the approach uniquely relevant to this project. Considering the preliminary and largely non-empirical nature of many of the studies of the privacy-surveillance relationship, it is essential that in order to intervene in this debate, any empirical work should be systematic and deliberate. QCA allows for this type of analysis.

Encryption provides an ideal case study to investigate the privacy-surveillance relationship. This is because encryption is conventionally viewed as a privacy-enhancing technology, particularly in light of the Snowden disclosures. If there is any case in which privacy is likely to play a major role in securing rights, encryption appears to be that case.

In collecting data for this project, I restricted my source to public records because I am concerned with public discourses. I collected every mention of encryption on the Congressional Record from 1993 to 2015. First, I searched “encryption” on the Federal Digital System and

Hein Online databases. After filtering for non-relevant material, this yielded 77 separate statements. I then collected Congressional hearings between 1993-2015 concerning encryption regulation by searching "encryption" on the Hein Online, Federal Digital System, ProQuest Congressional, and the Government Printing Office databases. After filtering for non-relevant material, this yielded 35 Congressional hearings. A hearing was considered relevant if at least one witness answered a question about encryption policy during the hearing or if encryption was discussed for at least three sentences in a witness's written testimony. In total, I analyzed 112 Congressional documents. In addition, I used documents obtained by various organizations via Freedom of Information Act (FOIA) request for illustrative purposes in order to illuminate possible motivations behind policy decisions.

To ensure validity, I engaged in three rounds of coding in order to develop the coding frame. In the first round (December 2015), I sampled 11 Congressional hearings from the collected documents. I coded hearings according to Schreier's (2013) technique. In the first reading, I coded passages according to the topic being discussed. The most common topics included "concerns with Clipper," "problems caused by encryption," "concerns with encryption regulation," "benefits of encryption," "escrow alternatives," and "privacy." I then revisited the codes two months later (February 2016) and applied the original coding frame to a separate sample of 3 hearings. During this round, I documented the strengths and weaknesses of the coding frame and how it succeeded and failed in capturing trends in the data. For example, the first coding frame failed to account for concerns about cost, from both business representatives and law enforcement. I also began focusing on sub-codes within initial codes. For instance, under the "concerns with Clipper" code, I noticed a broad distinction between market concerns and technical concerns, and thus split the code into two separate codes. During the third round, I

applied the adjusted frame to all documents, including those that had been sampled in earlier rounds. The frame was applied evenly to all documents included in analysis, hence improving reliability through consistency. According to Schreier (2013), conducting multiple rounds of coding also improves validity in that the coding frame is allowed to evolve with the data.

The following sections will present the findings of this study. The first section will outline the emergence of two discourses – market liberalization and government skepticism – during debates about key escrow. The second section will document how these discourses continued to evolve during debates about key recovery. The final section demonstrates how the *market liberalization* discourse has become ubiquitous in the Going Dark debates of the 2010s. Table 1 summarizes the tropes used by regulation opponents in the 1990s. The left column lists the three discourses that opponents mobilized against regulatory proposals. The right column provides sub-categories of each discourse, as well as an illustrative ideal-type statement. For a timeline of encryption debates since 1993, see Figure 1.

Proposal 1: Key Escrow and the Clipper Chip

The Clinton administration announced the Clipper Chip in April 1993. Clipper was a microchip that was to be inserted into U.S.-sold cell phones. Using a classified encryption scheme ("Skipjack") and a unique key exchange method, Clipper produced copies of users' encryption keys, which were then split and held in escrow by the National Institute of Standards and Technology and the Department of Treasury. Although the administration's earlier plans were to pass legislation mandating the use of Clipper ("Encryption: The Threat, Applications, and Potential Solutions" 1993), they ultimately chose to contract with private firms to build Clipper and subsequently use the federal government's buying power to influence the market for encryption goods.

After announcing Clipper, the administration held a series of Congressional hearings, a practice that continued through subsequent phases of encryption debates. Early hearings on encryption included panels of witnesses composed of representatives from industry, law enforcement, intelligence agencies, civic society organizations, academia, and various government agencies outside law enforcement and intelligence. Table 2 summarizes the distribution of witnesses from various sectors.

Table 1. Summary of Main Discourses, Sub-categories and Ideal-type Statements.

Discourses	Sub-categories and ideal-type statements
Market liberalization	**Business participation.** Encryption ensures privacy, which is essential for US businesses to participate, lead, and dominate international markets.
	User participation. Without privacy measures, such as encryption, consumers won't feel safe enough to participate in e-commerce.
	Property protection. Encryption functions as an important security measure in that it protects the privacy of corporate trade secrets, sensitive financial information, and intellectual property.
	Innovation encouragement. Current encryption regulation creates unnecessary burdens for corporations, which are held back from innovation by big government regulation.
	Loss of market share/revenue. American companies are losing money and their share of international markets because of US encryption regulation policy.
Government skepticism	**Crime prevention.** Widespread encryption use is a good alternative to state policing in that it enrolls businesses and private citizens in crime fighting in the course of daily life.
	Bureaucracy growth. State proposals for encryption regulation would create massive government bureaucracy that would be slow, expensive, and difficult to manage.
	Market efficiency. Businesspeople are better equipped to deal with security and policing issues because markets are more flexible, quick-reacting, and efficient.
	Citizen trust. Citizens trust businesses with access to their communications more than they trust government.
	Partnerships. If the government deregulates encryption, allowing US firms to dominate global markets for encryption, businesses will cooperate with police and intelligence agencies to maintain their access to citizens' communications.

According to supporters – a group that included members of the Clinton administration, LEAs, and intelligence agencies – encryption complicated LEAs understanding of the content of

Figure 1. Timeline of Encryption Debates since 1993.

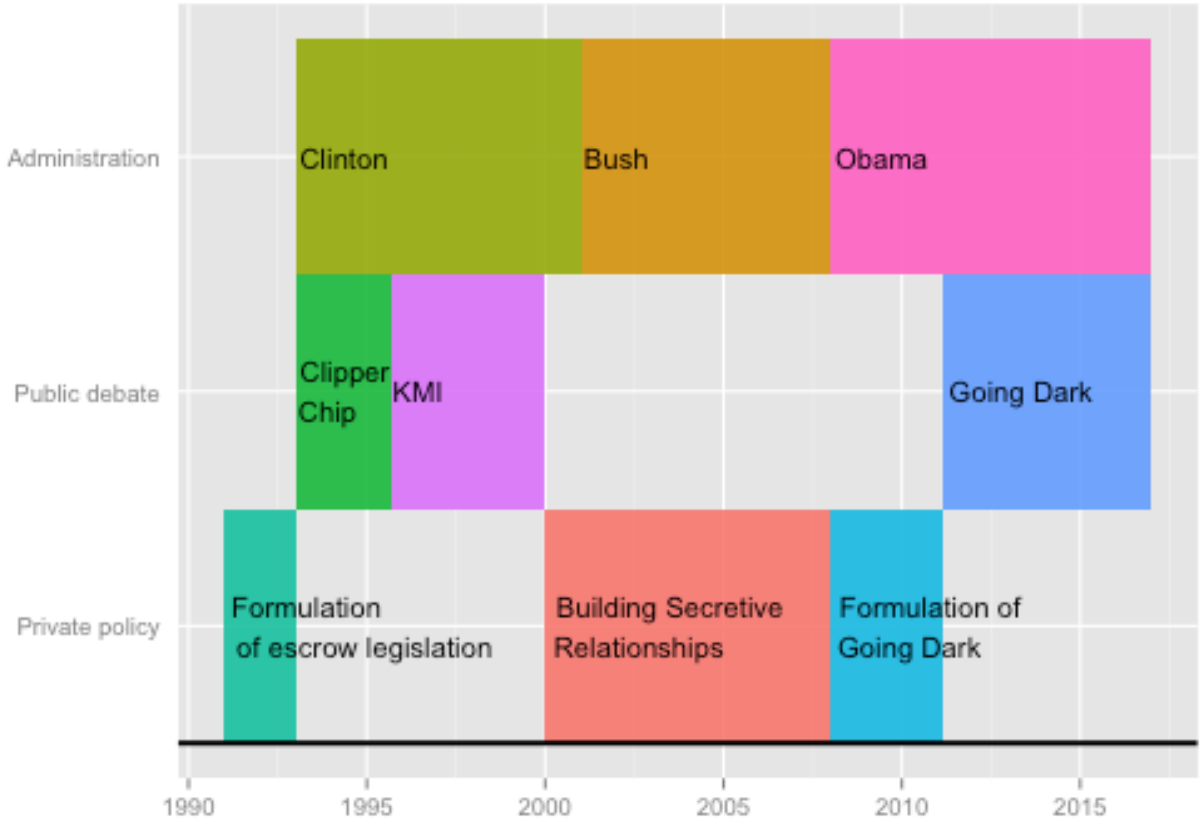

Table 2. Frequency of Witness Appearances by Sector, 1993-2016.

	1993-99	2011-16
Industry	73	0
Other government	31	2
LEAs	19	13
Civic society	17	0
Intelligence	15	1
Academia	13	3
Miscellaneous	6	0
Total	174	19

communications, or what I call the *decryption problem.* Supporters linked LEA's inability to decrypt to increases in criminal activity, particularly drug crimes. In the midst of the "tough on crime" era of the early 1990s, regulation proponents deployed sensational imagery of dangerous criminals in an effort to generate support for Clipper. Privacy also played a role in justifications for Clipper. Supporters claimed Clipper protected privacy because it included privacy safeguards

and encouraged more widespread encryption use. When asked about the privacy implications of Clipper, supporters typically referenced procedures LEAs would follow when requesting access to keys, policy regarding how and when keys would be destroyed, and the fact that LEAs would still need a warrant to access keys. Thus, for supporters, key escrow protected and enhanced privacy because it used existing statutory authority and followed specific privacy provisions that stipulated conditions for key access. Supporters constructed escrow as nothing more than adaptation of policing authority to the digital age.

Opposition to Clipper

Market Liberalization

The most common set of criticisms pushed by business representatives and privacy advocates constitute what I call the *market liberalization* discourse, which is comprised of three claims. The first claim was that Clipper had a chilling effect on private sector innovation. Opponents – including members of Congress – voiced their opinion that the best technological advancements came from a deregulated private sector, not from government or regulatory intervention. Clipper thus represented a severe commercial burden that would impede technological progress. A second claim was that privacy measures – such as encryption – were integral to international e-commerce. Encryption was necessary for American businesses' ability to compete in the growing global marketplace. Without encryption, businesses would be unable, for example, to send sensitive financial information to international banks or overseas corporate offices. Lastly, opponents claimed customers would not participate in e-commerce without assurance that their privacy was protected. In this case, opponents largely described privacy measures as a marketing tool. Without measures in place, users would be fearful of attacks from

identity thieves, criminals, and hackers, and thus would not participate in the digital economy, causing companies to lose customers.

Government Skepticism

The second discourse – *government skepticism* – focused on problems specific to federally-directed escrow systems. One concern opponents raised was with the lack of privacy procedures in place governing the use of escrow systems. In this case, key escrow systems themselves were not seen as necessarily invasive of privacy. Instead, opponents argued that weak procedural safeguards contributed to privacy invasions. Second, opponents referenced the potential for abuse as a drawback of escrow because federal agencies were untrustworthy and prone to abuse. Although some argued this abuse could be minimized with the institution of proper procedures, others believed no procedures would prevent federal excesses and abuses. Additionally, opponents cited practical difficulties implicated in federally-directed escrow systems. The existence of alternative products – including foreign products and open-source software published online and in textbooks – was an oft-cited example of why imposing any government-run system would not work. The implication was that the market was better positioned to deal with these contingencies.

Proposal 2: Key Recovery and the Administration Response to the Market Liberalization Discourse

In response to criticisms of Clipper, the Clinton administration withdrew escrow proposals and began pursuing key recovery initiatives. Key management infrastructure (KMI) represented a partial break with previous proposals in that it no longer pushed government-chosen escrow technologies. Instead, the private sector would select, build, and maintain their own recovery systems, which the federal government would permit to be exported so long as it

included a method for LEA access. Deputy Director of NSA William Crowell framed KMI as representing "significant concessions to industry" (U.S. Congress "Pro-CODE Act S. HRG. 104-617" 1996:32). Indeed, the changes in policy structure – for example, allowing firms to build and manage their own systems absent any technological mandates – suggest that the *market liberalization* and *government skepticism* discourses resonated with the administration. Many of the same justifications for Clipper were also made for KMI proposals, namely the decryption problem. Additionally, some supporters also explicitly framed KMI in opposition to Clipper in order to distance themselves from the previous proposal.

Opposition to KMI

Market Liberalization

The *market liberalization* discourse continued through debates about KMI proposals. Opponents claimed that encryption was necessary to secure user privacy, which was essential to building a global, U.S.-dominated digital economy. Without deregulation, companies would not have the freedom to choose which privacy protections were appropriate for their customers, nor the ability to develop new tools if necessary. Second, opponents made technical objections to the security of KMI, claiming it put user privacy at risk. The argument was that there were no backdoors that existed only for the "good guys." By allowing police to conduct surveillance, such regulation would permit criminals, hackers, and terrorists to invade consumers' privacy by exploiting vulnerabilities in security systems, causing consumers to avoid participating in e-commerce. Third, critiques cited the loss of revenue and market share that would result from encryption regulation. Opponents argued that encryption regulation would have the same effects as any other private sector regulation: it would hurt competition, increase costs borne by businesses, and cut into profits.

Lastly, critics of key recovery also claimed that deregulated encryption had a positive function, namely that it prevented economic espionage and intellectual property theft. In this view, encryption was actually supportive of law enforcement and private property. As Representative Goodlatte (R:VA) summarized, "the goals of ensuring the availability of strong encryption and of ensuring that law enforcement can continue to be effective are not mutually exclusive. We can do both" (U.S. Congress "SAFE Act" 1996:17). Thus, deregulation proponents made the case that encouraging widespread encryption use was not a method for protecting citizens from government surveillance, but for ensuring private property was protected.

Government Skepticism

As under criticisms of Clipper, KMI opponents claimed the system lacked sufficient privacy safeguards. The privacy threat posed by KMI was not the system itself – the bulk collection of encryption information and the requirement of LEA access to encrypted channels – but the weakness of privacy procedures. Opponents were mostly concerned about abuses of the system. For example, as Phyllis Schlafly of the Eagle Forum – a conservative interest group – explained, "are we worried about the Justice Department abusing its power to eavesdrop on our computer messages? You bet we are. The misbehavior of the FBI in so many areas and the coverups that followed have been shocking to Americans who like to support law and order" (U.S. Congress Committee on the Judiciary "SAFE Act" 1997:63). Government officials were not to be trusted with access to such a system unless there were privacy safeguards in place.

Concerns about privacy safeguards were part of a broader apprehension about centralized government power. Many business representatives and congresspersons claimed that U.S. citizens would trust corporations with encryption keys long before they would trust any

government agency. As Representative Sherman (D:CA) explained, "a lot of people want software where they can keep their own extra copy of the key. Some might even trust Bill Gates with an extra copy of the key, but none of the people who have written me want to entrust the government with the key" (U.S. Congress "Individual Right to Privacy" 1997:26). Representative Goodlatte (R:VA) cited the requirement that keys be held with government agencies as "a serious inhibiting factor" to any KMI system (U.S. Congress Committee on the Judiciary "SAFE Act" 1997:47). Representative Bono (R:CA) expressed similar concern, stating "you will never get public approval of these agencies. It's shattered … I can't support giving anything to any Federal agency … I absolutely don't trust them" (U.S. Congress "SAFE Act" 1996:47).

Lastly, opponents viewed deregulated encryption as a more efficient form of crime prevention than traditional policing methods. Encryption, in this view, was a technological method for private sector-based crime fighting. This is in stark contrast to the general assumption of the surveillance studies literature that encryption is necessarily a tool to fight law enforcement surveillance. In this discourse, encryption represented a vision of privatized law enforcement, in which crime prevention was built into private technological infrastructure. Senator Wyden (D:OR) concluded that the best way to ensure LEA access to encryption was "to unleash the genius and the creativity of the private sector, and not have the Federal Government constantly trying to stuff some sort of technological genie into the bottle" (U.S. Congress "Pro-CODE Act S. HRG. 104-624" 1996:13). Representative Goodlatte (R:VA) encouraged Congress to deregulate encryption in order to insert "heavily encrypted software into every home and every business in America to prevent crime and fight crime" (U.S. Congress "Individual Right to Privacy" 1997:37).

Counterproposals

Opponents to the administration's plans proposed several counterproposals as alternatives to federally-directed encryption regulation. These counterproposals demonstrated – both in terms of policy structure and in rhetorical framing – the continued persistence of the *market liberalization* and *government skepticism* discourses. Supporters of the counterproposals – including members of Congress, privacy advocates, and business representatives – backed these measures on the basis of three major assumptions: (1) the market was better positioned than government to respond to ubiquitous encryption because citizens trusted private business more than they trust the federal government; (2) a government-run system would require massive, unnecessary bureaucracy; and (3) achieving market interests was good for national security.

First, in response to the administration's continued efforts to drive the creation of KMI, Senators Leahy (D:VT), Burns (R:MT), Dole (R:KA), Pressler (R:SD), and Murray (D:WA) introduced the Encrypted Communications Privacy Act (ECPA) of 1996. Senator Leahy (D:VT) described the bill as "pro-business, pro-jobs, and pro-privacy" (U.S. Congress "Statement on Introduced Bills" 1996:1516). He framed the introduction of the bill as a response to two problems: the "theft of proprietary information" that resulted in the loss of billions of dollars each year by American businesses, and export controls that "tie[d] the hands of American high-technology businesses" (U.S. Congress "Statement on Introduced Bills" 1996:1516). The bill (1) prohibited government from mandating the use of one encryption system, (2) loosened export controls, (3) established privacy protections to be followed in the use of key escrow or recovery systems, and (4) criminalized encryption use in the furtherance of criminal activity. Interestingly, supporters claimed the final element – criminalization – was "privacy enhancing" because it protected the personal information of consumers. Technologists Matt Blaze and Bruce Schneier

submitted letters of support for the bill, as did the Business Software Alliance. However, the bill failed to come to a vote, even when reintroduced in 1997.

Second, a bipartisan group of Congresspersons introduced the Promotion of Commerce On-line in the Digital Era Act of 1996 (Pro-CODE Act) on May 2, 1996 in response to KMI proposals. Although similar to ECPA, this bill was narrower in scope and omitted the criminality provisions. It allowed the unrestricted export of mass market and public domain encryption software and prohibited mandatory key escrow, but did not provide guidelines for voluntary key-escrow management, as ECPA did. Senator Burns (R:MT) explained that his "primary objective with this legislation is to promote commerce both domestically and abroad … to improve the competitiveness of American software companies with their foreign competitors, the other is to protect the intellectual property and privacy of both business and individuals" (U.S. Congress "The Promotion of Commerce On-line" 1996:4624). Senator Pressler (R:SD), characterized the bill as follows:

> This bill will eliminate outdated, useless rules and regulations so that American companies can compete effectively throughout the world in the global information technology industry … The private sector is doing everything possible to expand this industry. Unfortunately, they frequently are held back by unnecessary or antiquated Government rules and regulations. Government should help, or at the very least, get out of the way … We must focus on expanding our present foreign markets and opening new ones in order to strengthen our business and maintain our economic hegemony. (U.S. Congress "The Promotion of Commerce On-line" 1996:4624)

Thus, the Pro-CODE Act was explicitly framed as a response to the market-based concerns raised by critics of the administration's encryption regulation proposals. Despite a series of hearings on the bill, it was not brought to a vote, and was never enacted.

A third counterproposal was the Security and Freedom through Encryption (SAFE) Act of 1997, introduced by Representative Goodlatte (R:VA) on February 2, 1997 with 54 co-sponsors. The goals of the bill were to aid LEAs in preventing white-collar crime, help the global

information infrastructure "reach its true potential," and loosen export controls on generally available encryption software. Representative DeLay (R:TX) supported the bill, arguing it was Congress's top priority because "if we do not take rational and effective action soon, our ability to use American ingenuity to keep at the forefront of worldwide economic growth through information technology will be irreparably harmed because of our inability to protect our Nation's primary source of strength – our citizens' knowledge and ideas" (U.S. Congress "Need for a New Policy" 1997:2243). In addition to contributing to economic growth, supporters – such as Representative Lofgren (D:CA) – argued it allowed "Americans to have complete protection from hackers and others who would steal and invade their privacy" (U.S. Congress "Support the SAFE Act" 1998:1702). Thus, opponents framed counterproposals as protecting privacy by stopping hackers and thieves, while encouraging the domination of U.S. firms in the global encryption market. Although the SAFE Act eventually accumulated 294 cosponsors and was endorsed by various organizations such as the U.S. Chamber of Commerce, the National Association of Manufacturers, the American Civil Liberties Union, and the National Rifle Association, it was never brought to a vote.

Although none of the counterproposals passed Congress, the debates surrounding these bills are instructive for considering the effects of privacy critiques on the development of surveillance technology. For example, the *government skepticism* discourse was a central component in efforts to pass the above counterproposals. For supporters of counterproposals, what made their bills superior to the administration's proposals was the fact that they enrolled the private sector in crime-fighting activities, thus lessening the policing power of the state, while also easing the regulatory burden on companies. For example, Ed Black, President of the Computer Communications Industry Association, claimed "the administration's approach is, in

essence, top-down industrial policy. Key recovery should not, and we do not think can be, government driven. It needs to be market driven" (U.S. Congress "Encryption" 1997:61). Similarly, James Lucier of Americans for Tax Reform supported the Pro-CODE Act because it was market-focused, leading to growth in technology markets and "increase the private sector and allow us to hold the government sector stable and basically decrease the Government sector in relative terms (U.S. Congress "Pro-CODE Act S. HRG. 104-617" 1996:75). Representative Goodlatte (R:VA) expressed similar sentiment, posing the question of "whether a free market system of this country and the very, very capable computer software industry should manage the development of that system or whether big government should be involved … in such a way that causes competitive disadvantages and severe mistrust on the part of a great many Americans" (U.S. Congress "Individual Right to Privacy" 1997:17). Thus, for critics of the administration's proposals, shifting control of decryption capabilities from the government to the market was a preferable alternative to centralized encryption access for law enforcement. This is reflective of the broader American political culture, which emphasizes self-determination, free enterprise, and skepticism of centralized government (Dobbin 2001; Fourcade 2009).

Counterproposal supporters also pushed the argument that market-based decryption capabilities were good for national security. They claimed it was in national interests to encourage widespread adoption of U.S. encryption products because American companies were more willing than foreign businesses to work with LEAs and intelligence agencies. As Roel Piper – President and CEO of Tandem Computers Inc.[1] – stated, "U.S. companies must be able to compete. If we can compete, you can trust us that we will work with all the established security agencies around the world to then allow them to do their job with those technologies"

[1] Tandem Computers was a U.S.-based computer manufacturing company.

(U.S. Congress "Pro-CODE Act S. HRG. 104-617" 1996:71). Similarly, Representative White (R:WA) concluded that "if we do not produce it [encryption] here and if our government does not understand and have relationships with the people who produce it, we are going to be less able, rather than more able, to decrypt encoded messages in the future" (U.S. Congress Committee on Commerce "SAFE Act" 1997:36). Two years later Representative White (R:WA) pointed out that if "all the people developing this technology happen to be located in Israel, Singapore, Japan, Ireland, and Germany, it is going to be pretty tough for the U.S. Government to interact with them and learn and understand and develop products that meet the needs of worldwide industry" (U.S. Congress "PROTECT Act" 1999:129). Ira Rubenstein – senior corporate attorney with Microsoft Corporation and representative of the Business Software Alliance – made a similar claim, stating that "industry is in a position to assist law enforcement and national security in achieving their objectives because we are able to sell U.S. products in mass volume" (U.S. Congress Committee on the Judiciary "SAFE Act" 1997:95). This discourse was well summarized by Representative Kennedy (D:RI):

> I think we need to co-opt, if you will, American high technology … if we are going to intend to be leaders in the world for our national security purposes, it seems to me we want to work with them and make sure that this stuff is going to be sold anyway, why not make sure they are on our side. If the product is being sold all over the world, why not make sure it is our product, domestic companies that have some allegiance and some interest in this country because they know about and appreciate the value of this great country of ours. (U.S. Congress "Encryption Policy: Part I" 1999:15)

Thus, opponents of KMI proposals countered the plans with a proposal for market-run decryption that would still allow LEA access. The ability to ensure privacy for consumers in market transactions against criminals was therefore paired with offers to work cooperatively with government to ensure LEAs and intelligence agencies obtained decrypted communications.

Privacy from criminals in the market had the paradoxical effect of facilitating the contraction of privacy from police surveillance.

Interim Period: 2000-2010

There is evidence that this was more than a rhetorical strategy. Documents released by whistleblower Edward Snowden, a former NSA contractor, demonstrate that beginning in the year 2000 – the same year that public debates about encryption rapidly dissipated, dropping from 4 public hearings and 17 statements on the Congressional Record in 1999 to zero in 2000 – NSA began investing billions of dollars in secret efforts to break commercial encryption systems (Appelbaum et. al. 2014). Since 2000, NSA has been working with Internet companies "by getting their voluntary collaboration, forcing their cooperation with court orders or surreptitiously stealing their encryption keys or altering their software or hardware" (Larson, Perlroth, and Shane 2013). Various leaked documents state that the goal of the project – known as BULLRUN – is to make "commercial encryption software 'more tractable' to NSA attacks by 'shaping' the worldwide marketplace and continuing efforts to break into the encryption used by the next generation of 4G phones" (Ball, Borger, and Greenwald 2013). Most important to this discussion, a classified NSA document claimed that "NSA makes modifications to commercial encryption software and devices 'to make them exploitable,' and that NSA 'obtains cryptographic details of commercial cryptographic information security systems through industry relationships" (Ball, Borger, and Greenwald 2013). Although the precise mechanisms of this cooperation remain unclear, one possibility is through the NSA's Commercial Solutions Center, which is used by NSA to "leverage sensitive, co-operative relationships with specific industry partners" (Ball, Borger, and Greenwald 2013). Additional documents show that Microsoft cooperated with NSA to help the agency "circumvent its encryption to address concerns that the

agency would be unable to intercept web chats on the new Outlook.com portal" (Greenwald et. al. 2013). Hence, there is evidence that industry cooperation and dialogue were indeed used by LEAs and intelligence agencies in their response to criticisms of KMI proposals.

Crypto Wars Redux: Going Dark, 2011-16

Following the interim period, the FBI launched the "Going Dark" initiative in 2011. The FBI framed Going Dark as addressing the gap between the legal authority of LEAs – such as warrants and subpoenas – and their technical capability to execute such authorities. Although Going Dark shares many similarities with the first Crypto Wars, there are significant differences. For example, whereas in the 1990s LEAs cited the *decryption problem* as the primary justification for regulating encryption, this issue faded in importance during the most recent reincarnation of the Crypto Wars. Instead, LEAs now stress companies' lack of compliance with court orders – what I call the *warrant problem.* Assistant Attorney General Sally Yates summarized the problem in these terms:

> Increasingly, we're finding that even when we have the authority to search certain types of digital communications, we can't get the information that we need, because encryption is being designed so that the information is only available to the user and the providers are simply unable to comply with a court order or warrant. The need and the justification for the evidence has been established, and yet that evidence can't be accessed. Critical information becomes, in effect, warrant proof. (U.S. Congress "Going Dark" 2015)

The central issue, then, is no longer concerns associated with the *market liberalization* discourse, which I argue is evidence that the *market liberalization* discourse has become fully accepted as legitimate by encryption stakeholders in public discussions. The primary obstacle facing LEAs in this phase is lack of cooperation from companies. As an FBI Situational Information Report dated June 2011 states, the "problems highlighted by the Going Dark initiative include LE's difficulty in receiving information from some technology companies." The report later elaborates that "some companies are unable to comply … due to a lack of knowledge regarding LE

authority, a belief that they are not subject to the laws providing LE intercept authority, or a lack of technical capability to provide the requested information." LEAs now claim the main issues they face are related to companies' compliance in relationships that were built in the wake of the first Crypto Wars.

It is also interesting to note the absence of business representatives from the witness panels at Congressional hearings. This represents a shift from panel composition in the first Crypto Wars. Table 2 above summarizes the distribution of witnesses from different sectors in all phases of public debates about encryption. The steep drop in number of business representatives is further evidence of the acceptance of the *market liberalization* discourse in that the distribution of responsibility for maintaining surveillance systems is no longer being debated. Instead, discussions are between congresspersons and LEA representatives, and focus on how the court system should respond to ubiquitous encryption.

Further evidence of the acceptance of the *market liberalization* discourse is the way in which LEAs and congresspersons discuss the possibilities for regulation. Rather than restricting the use or export of encryption as in the past, proponents begin by assuming businesses' encryption use and then move to regulate use in a way similar to any other corporate activity that impacts public interest. For example, Deputy Attorney General Yates contrasted the current approach with those of the past:

> This is not the situation of the 90's, where it was discussed at that time that the government actually would retain keys and would have an ability to access consumer information. What we're talking about is the individual companies, many of which are already doing this now for their own business purposes or other security purposes while still maintaining strong encryption. What we're asking is that public safety and national security also be one of the factors that industry considers in determining what type of encryption to use. (U.S. Congress "Going Dark" 2015)

Senator Whitehouse (D:RI) accused companies of "privatizing value" by using encryption as a marketing tool while "socializing the costs" among victims and their families. Drawing parallels to lawsuits over pollution, Whitehouse suggested that "when we see corporations privatizing value and socializing cost so that other people have to bear the cost, one of the ways that we get back to that and try to put some balance into it, is through the civil courts, through a liability system" (U.S. Congress "Going Dark" 2015). Thus, we see a full shift from solutions anchored in the market to those situated in the court system.

Discussion

What, then, can we say was the effect of how privacy discourses were mobilized in practice? The history presented above demonstrates that rather than stopping the spread of surveillance technologies, privacy critiques facilitated their development. Specifically, privacy critiques were embedded within the *market liberalization* and *government skepticism* discourses, in which privacy was either conceptualized as (1) the foundation for U.S. market hegemony and for protecting consumers from hackers, criminals, and terrorists, or (2) a procedural requirement that could be achieved with construction of proper technological and organizational safeguards. In the latter case, this study finds that privacy critiques facilitate the development of state surveillance capacities, although through slightly different mechanisms than those identified by Möllers and Halterlein (2013) and Coll (2014). Whereas these authors focus on the narrowing of privacy as a concept to a procedural order subjected to regulation and bureaucracy – thus, for Coll (2014), creating subjects of privacy via a dispositive of power – this study concludes that the focus on privacy from identity theft and economic espionage in the market facilitated the development of LEA surveillance capacity.

In the *market liberalization* discourse, privacy was bound up in concerns about American economic hegemony in emerging global markets, as well as broader neoliberal discourses. Deregulation proponents saw encryption as a means for ensuring informational privacy, an essential component in building U.S.-dominated global markets. Furthermore, deregulation backers saw encryption as compatible with law-and-order concerns in that it presented an opportunity to enroll technology corporations in law enforcement activities. Rather than checking policing powers, deregulation proponents argued encryption helped police by building crime-fighting techniques in private sector-run technical infrastructure. For some, this method of crime-fighting was actually preferable to traditional approaches because it signified a decrease in the size of the federal government and a privatization of law enforcement functions, without sacrificing the law-and-order goals of the 1990s. This is reflective of the broader American political culture, which holds a strong skepticism of centralized government power and prefers market mechanisms for distribution of goods (Dobbin 2001, Fourcade 2009). Understanding the trajectory of LEA access to encrypted communications requires a consideration of the relationship between American political culture and economic policy. This understanding, I argue, can be gained via conversations between surveillance studies and economic sociology.

Thus, the Crypto Wars should not be characterized as "privacy versus law enforcement," as commonly done. Rather, these debates were about matching neoliberal and law-and-order principles: how could informational privacy in the market be assured so that American technology firms could dominate world markets, all while securing avenues for LEA surveillance? How could LEA surveillance be assured without activating the American skepticism toward centralized government power? In the first phase, the Clinton administration eventually loosened export controls and withdrew regulatory proposals. Although it appeared

privacy advocates had won the Crypto Wars, in reality discussions about LEA access shifted to non-public and non-democratic channels. The result of these debates, then, were that LEAs and intelligence agencies were able to dialogue with U.S. firms – who now faced fewer regulatory barriers to exporting their products worldwide – behind closed doors to coordinate individualized solutions, all while keeping the public unaware of these activities. Therefore, this study finds that when privacy is conceptualized as protection from criminals, hackers, and identity thieves, privacy critiques can actually facilitate the development of surveillance technologies. Privacy, in this sense, is not at all antagonistic to law enforcement. Instead, increased privacy from criminals in the private sector can be used as a means for contracting privacy from law enforcement.

References

Appelbaum, Jacob, Aaron Gibson, Christian Grothoff, Andy Muler-Maguhn, Laura Poitras, Michael Sontheimer, and Christian Stocker. 2014. “Prying Eyes: Inside the NSA’s War on Internet Security.” *Der Spiegel* Retrieved December 1, 2015 from [http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html].

Ball, James, Julian Borger, and Glenn Greenwald. 2013. “Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security.” *The Guardian.* Retrieved May 1, 2016 from [http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security].

Bennett, Colin J. 2011. “In Defence of Privacy: The Concept and the Regime.” *Surveillance and Society* 8(4): 485-496.

Brown, Brian A. 2013. “Primitive Digital Accumulation: Privacy, Social Networks, and Biopolitical Exploitation.” *Rethinking Marxism: A Journal of Economics, Culture and Society* 25(3): 385-403.

Campbell, John L. 1998. “Institutional Analysis and the Role of Ideas in Political Economy.” *Theory and Society* 27(3): 377-409.

Coll, Sami. 2014. “Power, Knowledge, and the Subjects of Privacy: Understanding Privacy as the Ally of Surveillance.” *Information, Communication and Society* 17(10): 1250-1263.

Dobbin, Frank. 2001. “Why the Economy Reflects the Polity: Early Rail Policy in Britain, France, and the United States.” Pp. 397-418 in *The Sociology of Economic Life*, edited by Mark Granovetter and Richard Swedberg. Westview Press: Cambridge.

Fernback, Jan and Zizi Papacharissi. 2007. “Online Privacy as Legal Safeguard: The Relationship among Consumer, Online Portal, and Privacy Policies.” *New Media and Society* 9(5): 715-734.

Foucault, Michel. 1985. *The Historical of Sexuality Vol. 2: The Use of Pleasure.* New York, NY: Vintage.

Fourcade, Marion. 2009. *Economists and Societies: Discipline and Profession in the United States, Britain, and France, 1890s to 1990s.* Princeton University Press: Princeton.

Gilliom, John. 2011. “A Response to Bennett’s ‘In Defence of Privacy.’” *Surveillance and Society* 8(4): 500-504.

Greenwald, Glenn, Ewen MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe. 2013. “Microsoft Handed the NSA Access to Encrypted Messages.” *The Guardian*. Retrieved May 1, 2016 from [http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data].

Larson, Jeff, Nicole Perlroth, and Scott Shane. 2013. “Revealed: The NSA’s Secret Campaign to Crack, Undermine Internet Security.” *ProPublica.* Retrieved May 1, 2016 from [https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption].

Lyon, David. 2015. *Surveillance after Snowden*. Polity Press: Cambridge.

Mollers, Norma and Jens Halterlein. 2013. “Privacy Issues in Public Discourse: The Case of ‘Smart’ CCTV in Germany.” *Innovation: The European Journal of Social Science Research* 26(1): 57-70.

Nissenbaum, Helen. 2009. *Privacy in Context.* Palo Alto: Stanford University Press.

Schreier, Margrit. 2012. *Qualitative Content Analysis in Practice.* SAGE Publications: Thousand Oaks, CA.

Sessions, William. 1993. "Encryption: The Threat, Applications, and Potential Solutions." Top Secret briefing document obtained by the Electronic Privacy Information Center via FOIA. Retrieved December 1, 2015 from [https://epic.org/crypto/clipper/foia/crypto_threat_2_19_93.html].

Appendix A: Congressional Hearings Used in QCA. Chronological Order.

U.S. Congress. 1993. House Subcommittee on Economic Policy, Trade, and Environment of the Committee on Foreign Affairs. *Export Controls on Mass Market Software:* Hearing. 103rd Congress, 1st Session, pp. 1-139.

U.S. Congress. 1993. House Subcommittee on Telecommunications and Finance of the Committee on Energy and Commerce. *Telecommunications Network Security: Part I:* Hearing. 103rd Congress, 1st Session, pp. 1-100.

U.S. Congress. 1993. House Subcommittee on Telecommunications and Finance of the Committee on Energy and Commerce. *Telecommunications Network Security: Part II:* Hearing. 103rd Congress, 1st Session, pp. 101-260.

U.S. Congress. 1994. Senate Subcommittee on Technology and the Law of the Committee on the Judiciary. *The Administration's Clipper Chip Key Escrow Encryption Program:* Hearing. 103rd Congress, 2nd Session, pp. 1-155.

U.S. Congress. 1994. House Subcommittee on Technology, Environment, and Aviation of the Committee on Science, Space, and Technology. *Communications and Computer Surveillance, Privacy and Security*: Hearing. 103rd Congress, 2nd Session, pp. 1-195.

U.S. Congress. 1995. House Subcommittee on Crime of the Committee on the Judiciary. *Combating Domestic Terrorism:* Hearing. 104th Congress, 1st Session, pp. 1-189.

U.S. Congress. 1995. House Subcommittee on Crime of the Committee on the Judiciary. *Enforcement of Federal Drug Laws: Strategies and Policies of the FBI and DEA:* Hearing. 104th Congress, 1st Session, pp. 1-66.

U.S. Congress. 1996. Senate Subcommittee on Science, Technology, and Space of the Committee on Commerce, Science, and Transportation. *S. 1726, Promotion of Commerce*

Online in the Digital Era Act of 1996, or 'PRO-CODE' Act [S. HRG. 104-624]: Hearing. 104th Congress, 2nd Session, pp. 1-299.

U.S. Congress. 1996. Senate Subcommittee on Science, Technology, and Space of the Committee on Commerce, Science, and Transportation. *S. 1726, Promotion of Commerce Online in the Digital Era Act of 1996, or 'PRO-CODE' Act [S. HRG. 104-621]:* Hearing. 104th Congress, 2nd Session, pp. 1-138.

U.S. Congress. 1996. Senate Subcommittee on Science, Technology, and Space of the Committee on Commerce, Science, and Transportation. *S. 1726, Promotion of Commerce Online in the Digital Era Act of 1996, or 'PRO-CODE' Act [S. HRG. 104-617]:* Hearing. 104th Congress, 2nd Session, pp. 1-161.

U.S. Congress. 1996. House Committee on the Judiciary. *Security and Freedom through Encryption (SAFE) Act:* Hearing. 104th Congress, 2nd Session, pp. 1-102.

U.S. Congress. 1997. Senate Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary. *The Encryption Debate: Criminals, Terrorists, and the Security Needs of Business and Industry:* Hearing. 105th Congress, 1st Session, pp. 1-116.

U.S. Congress. 1997. Senate Committee on Commerce, Science, and Transportation. *Encryption:* Hearing. 105th Congress, 1st Session, pp. 1-185.

U.S. Congress. 1997. Senate Committee on the Judiciary. *Encryption, Key Recovery, and Privacy Protection in the Information Age:* Hearing. 105th Congress, 1st Session, pp. 1-130.

U.S. Congress. 1997. House Subcommittee on International Economic Policy and Trade of the Committee on International Relations. *Encryption: Individual Right to Privacy vs. National Security:* Hearing. 105th Congress, 1st Session, pp. 1-116.

U.S. Congress. 1997. House Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce. *The Security and Freedom through Encryption (SAFE) Act:* Hearing. 105th Congress, 1st Session, pp. 1-121.

U.S. Congress. 1997. House Subcommittee on Courts and Intellectual Property of the Committee on the Judiciary. *Security and Freedom through Encryption (SAFE) Act:* Hearing. 105th Congress, 1st Session, pp. 1-166.

U.S. Congress. 1997. House Committee on National Security. *H.R. 695, The Security and Freedom through Encryption Act:* Hearing. 105th Congress, 1st Session, pp. 1-127.

U.S. Congress. 1998. Senate Subcommittee on the Constitution, Federalism, and Property Rights of the Committee on the Judiciary. *Privacy in the Digital Age: Encryption and Mandatory Access:* Hearing. 105th Congress, 2nd Session, pp. 1-121.

U.S. Congress. 1998. Senate Subcommittee on Commerce, Justice, and State, the Judiciary, and Related Agencies of the Committee on Appropriations. Counterterrorism: Evaluating the 5-Year Plan: Hearing. 105th Congress, 2nd Session, pp. 1-53.

U.S. Congress. 1998. Senate Select Committee on Intelligence. *Current and Projected National Security Threats to the United States:* Hearing. 105th Congress, 2nd Session, pp. 1-177.

U.S. Congress. 1999. House Committee on Armed Services. *U.S. Encryption Policy: Part I:* Hearing. 106th Congress, 1st Session, pp.1-65.

U.S. Congress. 1999. House Committee on Armed Services. *U.S. Encryption Policy: Part II:* Hearing. 106th Congress, 1st Session, pp. 67-195.

U.S. Congress. 1999. House Subcommittee on International Economic Policy and Trade of the Committee on International Relations. *Encryption Security in a High Tech Era:* Hearing. 106th Congress, 1st Session, pp. 1-60.

U.S. Congress. 1999. Senate Committee on Commerce, Science, and Transportation. *S. 798, The Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999:* Hearing. 106th Congress, 1st Session, pp. 1-129.

U.S. Congress. 1999. House Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce. *The Security and Freedom through Encryption (SAFE) Act:* Hearing. 106th Congress, 1st Session, pp. 1-89.

U.S. Congress. 2011. House Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary. *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies:* Hearing. 112th Congress, 1st Session, pp. 1-79.

U.S. Congress. 2011. House Committee on the Judiciary. *Federal Bureau of Investigation:* Hearing. 112th Congress, 1st Session, pp. 1-68.

U.S. Congress. 2015. House Committee on Homeland Security. *Countering Violent Islamist Extremism: The Urgent Threat of Foreign Fighters and Home-Grown Terror:* Hearing. 114th Congress, 1st Session, pp. 1-58.

U.S. Congress. 2015. House Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security. *Addressing Remaining Gaps in Federal, State, and Local Information Sharing:* Hearing. 114th Congress, 1st Session, pp. 1-31.

U.S. Congress. 2015. House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations of the Committee on the Judiciary. *ISIL in America: Domestic Terror and Radicalization:* Hearing. 114th Congress, 1st Session, pp. 1-59.

U.S. Congress. 2015. House Committee on Homeland Security. *Terrorism Gone Viral: The Attack in Garland, Texas, and Beyond:* Hearing. 114th Congress, 1st Session, pp. 1-53.

U.S. Congress. 2015. Senate Committee on the Judiciary. Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy: Hearing. 114th Congress, 1st Session.

U.S. Congress. 2015. Senate Select Committee on Intelligence. *Counterterrorism, Counterintelligence, and the Challenges of 'Going Dark':* Hearing. 114th Congress, 1st Session.

U.S. Congress. 2016. House Committee on the Judiciary. *Encryption Tightrope: Balancing Americans' Security and Privacy:* Hearing. 114th Congress, 1st Session.

Appendix B: Statements on Congressional Record Used in QCA. Chronological Order.

U.S. Congress. 1993. *Legislation to Amend the Export Administration Act of 1979:* Extension of Remarks on the House Congressional Record. 103rd Congress, 1st Session, 139(22):32192-32193.

U.S. Congress. 1994. *Encryption Standards and Procedures Act of 1994:* Extension of Remarks on the House Congressional Record. 103rd Congress, 1st Session, 140(20):28704-28705.

U.S. Congress. 1994. *Encryption Policy Endangers U.S. Competitiveness in Global Marketplace:* Extension of Remarks on House Congressional Record. 103rd Congress, 2nd Session, 140(9):13127-13128.

U.S. Congress. 1995. *Comprehensive Terrorism Prevention Act:* Statement on the Senate Congressional Record. 104th Congress, 1st Session, 141(89):7599-7607.

U.S. Congress. 1995. *Computer Privacy:* Extension of Remarks on the House Congressional Record. 104th Congress, 1st Session, 141(194):2307-2309.

U.S. Congress. 1996. *Statements on Introduced Bills and Joint Resolutions: The Encrypted Communications Privacy Act of 1996:* Statement on the Senate Congressional Record. 104th Congress, 2nd Session, 142(28):1516-1522.

U.S. Congress. 1996. *The Promotion of Commerce On-Line in the Digital Era Act of 1996:* Statement on the Senate Congressional Record. 104th Congress, 2nd Session, 142(59):4624-4627.

U.S. Congress. 1996. *Encryption Reform Needed Now:* Statement on the Senate Congressional Record, 104th Congress, 2nd Session, 142(86):6153-6155.

U.S. Congress. 1996. *FBI Files at the White House:* Statement on the Senate Congressional Record. 104th Congress, 2nd Session, 142(99):7358-7366.

U.S. Congress. 1996. *Trust:* Statement on the Senate Congressional Record. 104th Congress, 2nd Session, 142(101):7505-7508.

U.S. Congress. 1996. *Encryption:* Extension of Remarks on House Congressional Record. 104th Congress, 2nd Session, 142(105):1305.

U.S. Congress. 1996. *Our Flawed Encryption Policies:* Extension of Remarks on House Congressional Record. 104th Congress, 2nd Session, 142(105):1295.

U.S. Congress. 1997. *The Introduction of the Security and Freedom through Encryption (SAFE) Act:* Extension of Remarks on House Congressional Record. 105th Congress, 1st Session, 143(18):245-247.

U.S. Congress. 1997. *Proposed Encryption Legislation:* Statement on Senate Congressional Record. 195th Congress, 1st Session, 143(26):1930.

U.S. Congress. 1997. *The Secure Public Networks Act:* Statement on Senate Congressional Record. 105th Congress, 1st Session, 143(66): 4684-4686.

U.S. Congress. 1997. *The Computer Security Enhancement Act of 1997:* Extension of Remarks on House Congressional Record. 105th Congress, 1st Session, 143(84):1232.

U.S. Congress. 1997. *Encryption Bill: An Exercise in Deception:* Extension of Remarks on House Congressional Record. 105th Congress, 1st Session, 143(91): 1320.

U.S. Congress. 1997. *Encryption Policy Reform:* Statement on the Senate Congressional Record. 105th Congress, 1st Session, 143(93): 6724-6726.

U.S. Congress. 1997. *National Security and Defense Issues:* Statement on the House Congressional Record. 105th Congress, 1st Session, 143(115): 6909-6914.

U.S. Congress. 1997. *Computer Security Enhancement Act of 1997:* Statement on the House Congressional Record. 105th Congress, 1st Session, 143(123):7293-7298.

U.S. Congress. 1997. *Encryption:* Statement on the Senate Congressional Record. 105th Congress, 1st Session, 143(142):10879-10881.

U.S. Congress. 1997. *Encryption Policy: America's Police Oppose the SAFE Act (H.R. 695):* Extension of Remarks on the House Congressional Record. 143(147):2108.

U.S. Congress. 1997. *Encryption:* Statement on the Senate Congressional Record. 105th Congress, 1st Session, 143(155):11959-11960.

U.S. Congress. 1997. *Support U.S. Encryption Exports:* Statement on Senate Congressional Record. 105th Congress, 1st Session, 143(156):12195-12196.

U.S. Congress. 1997. *Need for a New Policy on Encryption:* Extension of Remarks on House Congressional Record. 105th Congress, 1st Session, 143(156):2243-2244.

U.S. Congress. 1997. *Keep High Technology Free from Washington Interference:* Statement on the Senate Congressional Record. 105th Congress, 1st Session, 143(156):12078-12080.

U.S. Congress, 1997. *Strong Encryption Needed to Protect National Security:* Extension of Remarks on House Congressional Record. 105th Congress, 1st Session, 143(157):2276.

U.S. Congress. 1997. *Concern about Exports and Domestic Controls:* Extension of Remarks on House Congressional Record. 105th Congress, 1st Session, 143(157):2289-2290.

U.S. Congress. 1997. *Encryption Exports Need Liberalization:* Statement on the Senate Congressional Record. 105th Congress, 1st Session, 143(158):12480.

U.S. Congress. 1997. *On Lifting the Encryption Export Ban:* Extension of Remarks on House Congressional Record. 105th Congress, 1st Session, 143(160):2370-2371.

U.S. Congress. 1998. *The Security and Freedom through Encryption Act:* Statement on the House Congressional Record. 105th Congress, 2nd Session, 144(38):1701-1702.

U.S. Congress. 1998. *The SAFE Act (H.R. 695) is Detrimental to Israel's National Security:* Extension of Remarks on House Congressional Record. 105th Congress, 2nd Session, 144(39):532-533.

U.S. Congress. 1998. *America's Police Oppose the SAFE Act (H.R. 695):* Extension of Remarks on House Congressional Record. 105th Congress, 2nd Session, 144(39):529.

U.S. Congress. 1998. *The American Legion Opposes H.R. 695, the SAFE Act:* Extension of Remarks on House Congressional Record. 105th Congress, 2nd Session, 144(39):531.

U.S. Congress. 1998. *The SAFE Act Jeopardizes Israel's Security:* Extension of Remarks on House Congressional Record. 105th Congress, 2nd Session, 144(40):542.

U.S. Congress. 1998. *Veterans of Foreign Wars of the United States Opposes H.R. 695, the SAFE Act:* Extension of Remarks on House Congressional Record. 105th Congress, 2nd Session, 144(40):540.

U.S. Congress. 1998. *Wake-Up Call on Encryption:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(41):3114-3116.

U.S. Congress. 1998. *Statements on Introduced Bills and Joint Resolutions:* Statement on Senate Congressional Record. 105th Congress, 2nd Session, 144(59):4713-4727.

U.S. Congress. 1998. *Sense of House Concerning President's Assertions of Executive Privilege:* Statement on House Congressional Record. 105th Congress, 2nd Session, 144(66):3640-3646.

U.S. Congress. 1998. *It's Official, the SAFE Act, (H.R. 695) Jeopardizes Israel's Security!:* Extension of Remarks on House Congressional Record. 105th Congress, 2nd Session, 144(67):973-974.

U.S. Congress. 1998. *The Unnecessary Legislative Fight over Encryption:* Extension of Remarks on House Congressional Record. 105th Congress, 2nd Session, 144(71):1032.

U.S. Congress. 1998. *Encryption:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(79):6437-6440.

U.S. Congress. 1998. *Congress needs to Act on Encryption Legislation:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(94):8236-8238.

U.S. Congress. 1998. *Encryption Legislation:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(95):8376-8377.

U.S. Congress. 1998. *Media Campaign Helps Inform Congressional Action on Encryption:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(105):9419-9420.

U.S. Congress. 1998. *Administration's Updated Encryption Policy:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(124):10515.

U.S. Congress. 1998. *56 Bit Encryption is a Good Start, but is not Enough:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(141):12151-12152.

U.S. Congress. 1998. *National Security and Information Technology:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(144):12359-12362.

U.S. Congress. 1998. *International Crime and Anti-Terrorism Amendments of 1998:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(147):12612-12620.

U.S. Congress. 1998. *Encryption Challenge in the Next Congress:* Statement on the Senate Congressional Record. 105th Congress, 2nd Session, 144(151):12851.

U.S. Congress. 1999. *Wireless Privacy Enhancement Act of 1999:* Statement on the House Congressional Record. 106th Congress, 1st Session, 145(30):800-806.

U.S. Congress. 1999. *Security and Freedom through Encryption (SAFE) Act:* Extension of Remarks on House Congressional Record. 106th Congress, 1st Session, 145(31):297.

U.S. Congress. 1999. *Statements on Introduced Bills and Joint Resolutions:* Statement on the Senate Congressional Record. 106th Congress, 1st Session, 145(51):3705-3707.

U.S. Congress. 1999. *The PROTECT Act:* Statement on the Senate Congressional Record. 106th Congress, 1st Session, 145(52):3771-3772.

U.S. Congress. 1999. *U.S. Policies Restrict Growth of Certain Exports:* Statement on House Congressional Record. 106th Congress, 1st Session, 145(55):2242-2243.

U.S. Congress. 1999. *The High Tech Economy:* Statement on the House Congressional Record. 106th Congress, 1st Session, 145(60):2527-2528.

U.S. Congress. 1999. *High-Tech Industry Export Laws:* Extension of Remarks on House Congressional Record. 106th Congress, 1st Session, 145(62):827.

U.S. Congress. 1999. *Research and Development of the 21st Century:* Statement on House Congressional Record. 106th Congress, 1st Session, 145(73):3379-3382.

U.S. Congress. 1999. *In Support of Security and Freedom through Encryption (SAFE) Act:* Statement on House Congressional Record. 106th Congress, 1st Session, 145(81):3999.

U.S. Congress. 1999. *Controls on Exportation of Technology in America:* Statement on the House Congressional Record. 106th Congress, 1st Session, 145(81)3997-3998.

U.S. Congress. 1999. *PROTECT Act:* Statement on the Senate Congressional Record. 106th Congress, 1st Session, 145(104):8949-8950.

U.S. Congress. 1999. *Security Issues Facing our County:* Statement on the House Congressional Record. 106th Congress, 1st Session, 145(120):8356-8366.

U.S. Congress. 1999. *Petitions and Memorials:* Statement on the Senate Congressional Record. 106th Congress, 1st Session, 145(121):11051-11053.

U.S. Congress. 1999. *Cyberspace Electronic Security Act of 1999: Message from the President of the United States (H. DOC. No. 106-123):* Statement on the House Congressional Record. 106th Congress, 1st Session, 145(123):8390-8391.

U.S. Congress. 1999. *Technology in our Society:* Statement on the House Congressional Record. 106th Congress, 1st Session, 145(125):8624-8625.

U.S. Congress. 1999. *Exportation of Technology Regarding Supercomputers and Encryption Software:* Statement on the House Congressional Record. 106th Congress, 1st Session, 145(148):10906-10907.

U.S. Congress. 1999. *Continued Reporting of Intercepted Wire, Oral, and Electronic Communications Act:* Statement on the Senate Congressional Record. 106th Congress, 1st Session, 145(155):14222-14223.

U.S. Congress. 2001. *Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 2002:* Statement on the Senate Congressional Record. 107th Congress, 1st Session, 147(119):9354-9359.

U.S. Congress. 2001. *How to Address the Threat that Confronts Us Today:* Statement on the Senate Congressional Record. 107th Congress, 1st Session, 147(122):9468-9469.

U.S. Congress. 2014. *USA FREEDOM Act:* Extension of Remarks on Senate Congressional Record. 113th Congress, 2nd Session, 160(79):835-836.

U.S. Congress. 2014. *FISA:* Statement on the Senate Congressional Record. 113th Congress, 2nd Session, 160(141):6027-6029.

U.S. Congress. 2015. *Statements on Introduced Bills and Joint Resolutions:* Statement on the Senate Congressional Record. 114th Congress, 1st Session, 161(3):101-108.

U.S. Congress. 2015. *USA Freedom Act of 2015: Motion to Proceed:* Statement on the Senate Congressional Record. 114th Congress, 1st Session, 161(85):3331-3340.

U.S. Congress. 2015. *Terrorist Attacks against France:* Statement on the Senate Congressional Record. 114th Congress, 1st Session, 161(169)7976-7977.

U.S. Congress. 2015. *Fighting ISIS:* Statement on the Senate Congressional Record. 114th Congress, 1st Session, 161(176):8427-8428.

U.S. Congress. 2015. *Presidential Strategy to Defeat ISIS:* Statement on the Senate Congressional Record. 114th Congress, 1st Session, 161(178):8529-8531.

U.S. Congress. 2015. *President's Strategy to Defeat ISIS:* Statement on the Senate Congressional Record. 114th Congress, 1st Session, 161(182):8663-8665.