NEW AMERICA

OPEN TECHNOLOGY INSTITUTE

CYBERSECURITY INITIATIVE

DANIELLE KEHL, ANDI WILSON, AND KEVIN BANKSTON

DOOMED TO REPEAT HISTORY?

Lessons from the Crypto Wars of the 1990s

JUNE 2015

AUTHORS
Danielle Kehl, Senior Policy Analyst, Open Technology Institute
Andi Wilson, Program Associate, Open Technology Institute
Kevin Bankston, Director, Open Technology Institute

ABOUT THE OPEN TECHNOLOGY INSTITUTE
The Open Technology Institute at New America is committed to freedom and social justice in the digital age. To achieve these goals, it intervenes in traditional policy debates, builds technology, and deploys tools with communities. OTI brings together a unique mix of technologists, policy experts, lawyers, community organizers, and urban planners to examine the impacts of technology and policy on people, commerce, and communities. Our current focus areas include surveillance, privacy and security, network neutrality, broadband access, and Internet governance.

ABOUT THE CYBERSECURITY INITIATIVE
The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security Program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work — for the countries, for companies and for individuals.

ACKNOWLEDGEMENTS
The authors would like to thank Hal Abelson, Steven Bellovin, Jerry Berman, Matt Blaze, Alan Davidson, Joseph Hall, Lance Hoffman, Seth Schoen, and Danny Weitzner for their input and comments on an earlier draft of this paper. This paper does not necessarily reflect their views. We would also like to thank the staff and fellows at New America for their help: Jordan McCarthy, David Post, and Robert Morgus.

PHOTO CREDIT COVER PHOTO - Shutterstock

EXECUTIVE SUMMARY

In the past year, a conflict has erupted between technology companies, privacy advocates, and members of the U.S. law enforcement and intelligence communities over the right to use and distribute products that contain strong encryption technology. This debate between government actors seeking ways to preserve access to encrypted communications and a coalition of pro-encryption groups is reminiscent of an old battle that played out in the 1990s: a period that has come to be known as the "Crypto Wars." This paper tells the story of that debate and the lessons that are relevant to today. It is a story not only about policy responses to new technology, but also a sustained, coordinated effort among industry groups, privacy advocates, and technology experts from across the political spectrum to push back against government policies that threatened online innovation and fundamental human rights.

Encryption is a method by which two parties can communicate securely. Although it has been used for centuries by the military and intelligence communities to send sensitive messages, the debate over the public's right to use encryption began after the discovery of "public key cryptography" in 1976. In a seminal paper on the subject, two researchers named Whitfield Diffie and Martin Hellman demonstrated how ordinary individuals and businesses could securely communicate data over modern communications networks, challenging the government's longstanding domestic monopoly on the use of electronic ciphers and its ability to prevent encryption from spreading around the world. By the late 1970s, individuals within the U.S. government were already discussing how to solve the "problem" of the growing individual and commercial use of strong encryption. War was coming.

The act that truly launched the Crypto Wars was the White House's introduction of the "Clipper Chip" in 1993. The Clipper Chip was a state-of-the-art microchip developed by government engineers which could be inserted into consumer hardware telephones, providing the public with strong cryptographic tools without sacrificing the ability of law enforcement and intelligence agencies to access unencrypted versions of those communications. The technology relied on a system of "key escrow," in which a copy of each chip's unique encryption key would be stored by the government. Although White House officials mobilized both political and technical allies in support of the proposal, it faced immediate backlash from technical experts, privacy advocates, and industry leaders, who were concerned about the security and economic impact of the technology in addition to obvious civil liberties concerns. As the battle wore on throughout 1993 and into 1994, leaders from across the political spectrum joined the fray, supported by a broad coalition that opposed the Clipper Chip. When computer scientist Matt Blaze discovered a flaw in the system in May 1994, it proved to be the final blow: the Clipper Chip was dead.

Nonetheless, the idea that the government could find a palatable way to access the keys to encrypted communications lived on throughout the 1990s. Many policymakers held onto hopes that it was possible to securely implement what they called "software key escrow" to preserve access to phone calls, emails, and other communications and storage applications. Under key escrow schemes, a government-certified third party would keep a "key" to every device. But the government's shift in tactics ultimately proved unsuccessful; the privacy, security, and economic concerns continued to outweigh any potential benefits. By 1997, there was an overwhelming amount of evidence against moving ahead with any key escrow schemes.

While the domestic fight over key escrow wore on throughout the mid-1990s, another related battle was brewing on the international front over U.S. export controls and encryption technology. The question at the center of that debate was whether American technologies containing strong encryption should be made available overseas — which would in turn have a significant effect on the domestic availability and use of encryption tools. Until 1996, cryptographic tools were classified as munitions in the United States, with strict limits on the type of encryption that could be exported and the maximum cryptographic key length. Despite growing opposition to these restrictions, the U.S. government

had a strong incentive to maintain encryption export controls as a means to delay the spread and adoption of strong encryption technology abroad. The practical result of the policy was that many companies exported weaker versions of their encrypted products, or were kept out of foreign markets altogether. By the mid-1990s, experts projected billions of dollars in potential losses as a result of these policies. Coupled with growing evidence that foreign-made encryption was readily available around the world, the rationale behind maintaining these controls became increasingly tenuous. Many of the same organizations and individuals that rallied against the Clipper Chip came together to mobilize against encryption export controls, arguing that they undermined U.S. economic competitiveness and individual privacy, with little evidence that they were actually achieving their stated goals.

From 1996 to 1999, the Clinton Administration gradually liberalized encryption export controls, beginning with the 1996 Executive Order that moved most commercial encryption tools from the U.S. Munitions List to the Commerce Control List. The next step involved relaxing limits on the strength of encryption keys. Although these concessions were originally used as a bargaining chip in the commercial key escrow debate — companies would be allowed to export higher strength encryption if they agreed to retain the keys — those requirements were eventually abandoned after pressure from industry and public interest groups. In September 1999, the White House announced a sweeping policy change that removed virtually all restrictions on the export of retail encryption products, regardless of key length. As journalist Steven Levy put it succinctly: "It was official: public crypto was our friend."

In the decades since the resolution of the Crypto Wars, many of the predictions about how strong encryption would benefit the economy, strengthen Internet security, and protect civil liberties have been borne out. In particular, the widespread availablility of robust encryption laid the groundwork for the emergence of a vibrant marketplace of new Internet services based on secure digital communications and the widespread migration of sensitive communications online. The emergence of foundational technologies like the Secure Sockets Layer (SSL) and the Secure Shell Protocol (SSH) allowed the encrypted web to expand rapidly to include electronic banking, electronic medical records systems, online bill payment tools, home automation systems, e-filing systems for taxes, and VPNs. The evolution of the ecosystem for encrypted communications has also enhanced the protection of individual communications and improved cybersecurity, and today, strong encryption is an essential ingredient to the overall security of the modern network. And finally, the end of the Crypto Wars ushered in an age where the security and privacy protections afforded by the use of strong encryption also help promote free expression.

Unfortunately, the consensus that strong encryption is good for security, liberty, and economic growth has come under threat in recent years. The June 2013 revelations about the U.S. National Security Agency's pervasive surveillance programs — not to mention the NSA's direct attempts to thwart Internet security to facilitate its own spying — dramatically shifted the national conversation, highlighting the vulnerabilities in many of the tools and networks on which we now rely for both everyday and sensitive communications. While ordinary individuals, civil liberties advocates, and major technology companies have since embraced greater use of encryption as a necessary step to address a wide range of modern threats from both government and nongovernment actors, intelligence agencies and law enforcement officials have also become increasingly outspoken against measures to strengthen these systems through encryption. To make their case, they have revived many of the arguments they made about encryption in the 1990s, seeming to have forgotten the lessons of the past.

It seems like we may once again be on the verge of another war: a Crypto War 2.0. But it would be far wiser to maintain the peace than to begin a new and unnecessary conflict. There is no reason to repeat our previous mistakes.

TABLE OF CONTENTS

INTRODUCTION

History sometimes repeats itself.

In the past year, a conflict has erupted between technology companies, privacy advocates, and members of the U.S. law enforcement and intelligence communities over the right to use and distribute products and services that use strong encryption. In September 2014, Apple announced that it would be moving to smartphone encryption by default on all devices running its new iOS, followed a few days later by a similar announcement from Google about the latest version of the Android operating system.[1] Since the 2013 Snowden disclosures — which caused consumer trust in American technology companies to plummet[2] — a number of U.S. companies have taken greater steps to use the more secure HTTPS protocol, to encrypt end-user devices by default, and to make end-to-end encryption[3] available for their email and messaging services.[4] Although many users in the United States and around the world welcomed the changes, the Apple and Google announcements in particular prompted significant backlash from some American law enforcement and intelligence officials.[5] FBI Director James Comey argued that Apple and Google's new privacy-enhancing features will "allow people to place themselves beyond the law" and that default encryption could seriously hinder criminal investigations, calling on Congress to take action to force companies to maintain some kind of backdoor to allow government access to communications if a warrant has been obtained.[6] Former Attorney General Eric Holder also urged tech companies to leave backdoors open for police,[7] and their arguments have received support from the National Security Agency and the Office of the Director for National Intelligence.[8] The requests have ignited a public discussion about whether it is technically feasible to implement surveillance backdoors without undermining the overall security of cryptographic systems, and what the economic and civil liberties implications are.[9]

This is not a new debate. A similar policy battle over encryption happened twenty years ago: a conflict that has come to be known as the "Crypto Wars."[10] Throughout the 1990s, policymakers and advocates fiercely debated the tradeoffs related to the proliferation of encryption technology both in the United States and overseas. Although the dispute had been brewing beneath the surface for years, the beginning of the Crypto Wars can be traced back to the Clinton Administration's 1993 "Clipper Chip" proposal, which eventually evolved into a broader debate about "key escrow" technologies and whether the government or a trusted third party should hold master keys that could be used to decode any encrypted communications. By 1996, the battle was being fought on two fronts, as the conflict over the U.S. government's attempt to restrict the proliferation of strong encryption technology overseas through export controls erupted. After a groundswell of opposition from privacy advocates, industry representatives, and prominent politicians — including significant online organizing and lobbying efforts to educate the public and the highlight the technical and legal flaws in the U.S. government's policies — the Administration capitulated, abandoning the Clipper Chip and related key escrow proposals and relaxing U.S. export controls on strong encryption products.[11] By the time Vice President Al Gore finally announced sweeping changes to U.S. export restrictions in the fall of 1999, it was clear that the Crypto Wars were over, and the arguments in favor of strong encryption had won.

This paper tells the story of the original Crypto Wars and the lessons that they offer. It is a story about policy responses to new technology, but it is also a story about a sustained, coordinated effort among industry groups, privacy advocates, and technology experts from across the political spectrum to push back against government policies that threatened online innovation and fundamental human rights. Its goal is to remind us of what happened twenty years ago and why the debate reached the conclusion that it did, so that we might avoid the Crypto Wars 2.0. Unless we learn the lessons of the first Crypto Wars, we may be doomed to repeat the mistakes of the past.

I. BEFORE THE CRYPTO WARS

Contrary to what many people now believe, encryption technology is not a product of the digital age, nor something that the Founding Fathers could not have fathomed when they wrote the United States Constitution.[12] In fact, in the early 1790s, while serving as George Washington's Secretary of State, Thomas Jefferson himself relied upon encryption to securely encode and decode messages in the letters that he sent overseas, using a wooden device that he invented known as a wheel cipher.[13] Encryption methods have actually been used for centuries by diplomats, intelligence officers, and soldiers — from the ancient Romans to the likes of Benjamin Franklin, Alexander Hamilton, and John Adams — to send sensitive messages without fear that the contents could be read if they were intercepted.[14]

Modern encryption relies on mathematical algorithms to protect the security and integrity of messages and streams of data as they are transmitted electronically or when stored on devices.[15] For much of the twentieth century, these sophisticated encryption techniques were available almost exclusively to members of the government, military, and intelligence communities. Even as encryption methods became more effective and easier to use over time, they still required special technology or training that was closely guarded, and much of the cutting-edge development in the field was not visible to the public.[16] As a result, although significant advances had been made in the field by the early 1970s, sending encrypted electronic messages remained beyond the reach of ordinary individuals until 1976.

DEFINING CRYPTOGRAPHY

The term "cryptography" refers to the practice and study of theory and techniques for secure storage and communications. Encryption is the actual process of combining the contents of a message ("plaintext") with a secret value or password (the encryption "key") in such a way that scrambles the content into a totally new form ("ciphertext") that is unintelligible to unauthorized users. The goal is that only someone with the correct key can decrypt the information and convert it back into plaintext.

THE BIRTH OF PUBLIC KEY CRYPTOGRAPHY

"The crypto war is the inevitable consequence of a remarkable discovery made almost 20 years ago, a breakthrough that combined with the microelectronics revolution to thrust the once-obscure field of cryptography into the mainstream of communications policy."

- Stephen Levy, "Battle of the Clipper Chip" (1994)

"The set of algorithms, equations and arcane mathematics that make up public key cryptography are a crucial technology for preserving computer privacy in and making commerce possible on the Internet. Some hail its discovery as one of the most important accomplishments of 20th-century mathematics…Without it, there would be no privacy in cyberspace."

- Peter Wayner, "A Patent Falls, and the Internet Dances" (1997)

Everything changed with the invention of public key cryptography in 1976. Two researchers named Whitfield Diffie and Martin Hellman published a revolutionary paper on a new technology they called "public key cryptography,"[17] which demonstrated how ordinary individuals and businesses could securely communicate data over modern communications networks.[18] Diffie and Hellman described a process in which each participant in a conversation created related public and private keys, which could then be used to encrypt and decrypt plaintext conversations.[19]

Their crucial insight was that the key used to encrypt a message could be linked to, but distinct from, the key used to decrypt the message — so that anyone could create and distribute a unique "public" key, useful only for creating messages that no one but the owner of the corresponding "private" key would be able to unscramble.[20] Unlike previous methods of encryption, this approach allowed two or more parties to communicate privately and securely *even if they had never previously met*.[21]

The discovery of public key cryptography laid the foundation for a number of innovations in secure communications over the next 40 years. Not long after Diffie and Hellman's "New Directions in Cryptography" was published, three mathematicians at the Massachusetts Institute of Technology — Ronald Rivest, Adi Shamir, and Leonard Adleman — developed a system that put the split-key encryption theory into practice.[22] The technique that they created in 1977, known as "RSA" (a combination of their initials), ensured that electronic mail messages could be kept private. It also offered a means to digitally "sign" messages to show authenticity.[23] This discovery, coupled with Diffie and Hellman's paper and other research, sparked the beginning of significant academic interest in cryptography.[24]

In those early days, however, the commercial viability of technology that used public key encryption remained unclear.[25] The market for strong cryptosystems that eventually developed had two fundamental drivers: the increasing use of personal computers by large companies, and the demand for secure email technology for individual use.[26] As both became more common in the 1980s, commercial demand for encryption products exploded.[27] The increased use of networked PCs by corporations required that they use strong encryption to protect those networks, especially as more and more confidential data was computerized.[28] New markets emerged for authentication and digital signature software, antivirus software, data storage protection, firewalls, utility software, network security products, and virtual private network (VPN) software.[29]

While corporations drove much of the commercial development of cryptographic technology, a burgeoning community of privacy activists also began to create encryption tools for individual users. Computer scientist Philip Zimmermann designed one of the first major practical tools for end-to-end public key encryption of files and e-mail — a project called Pretty Good Privacy (PGP) — and released it publicly in 1991. As Zimmermann explained, "until recently, if the government wanted to violate the privacy of ordinary citizens, they had to expend a certain amount of expense and labor to intercept and steam open and read paper mail."[30] But with email, this was no longer the case — messages transmitted in plaintext were essentially postcards that could be read by anyone who intercepted them. A tool to encrypt text, emails, files, and contents of hard drives helped empower individuals to "take their privacy into their own hands."[31]

THE U.S. GOVERNMENT PREPARES FOR BATTLE

"If people had access to the means to encrypt their private communications, there could be a place to hide—and a universal means to privacy was what an agency charged with eavesdropping is hell-bent to prevent."

- Steven Levy, *Crypto* (2001)

While businesses and individuals may have been happy about the increasing use of encryption, the U.S. government was not. From the 1970s onward, intelligence and military officials in particular identified advances in cryptographic technology as a threat to U.S. security and took actions to discourage or halt research on encryption.[32] They understood that the widespread adoption of encryption — by both corporations and individuals — challenged their longstanding domestic monopoly on the use of electronic ciphers, as well as their ability to prevent encryption from spreading around the world.[33] As Jay Stowsky, a professor at UC Berkeley, explained, "[Early civilian cryptographers'] extraordinary achievements from the 1970s on were not viewed as benign by the world-class eavesdroppers at the NSA... As commercial applications developed by U.S. companies nevertheless became ever more sophisticated and widely accessible, the full weight of the federal government was brought to bear to control the pattern and pace of their diffusion."[34] But maintaining this control became increasingly difficult as a growing number of individuals and corporate actors built upon the work of early pioneers like Diffie, Hellman, and the RSA trio in the 1980s.[35]

By the early 1990s, the proliferation of personal computers, cell phones, and the Internet forced these concerns about the impact of encryption on

surveillance capabilities to the surface.[36] In January 1991, Senator Joe Biden inserted new language into the draft of an anti-terrorism bill, expressing a Sense of Congress that electronic communications service providers and equipment manufacturers "shall ensure that communications systems permit the government to obtain the plaintext contents of voice, data, and other communications when appropriately authorized by law."[37] Although the proposal did not advance, the message to companies was clear: the government was not likely to tolerate communications services offering strong encryption unless they also included "backdoors" allowing the government to lawfully obtain the decrypted contents of encrypted messages. Meanwhile, within the NSA, discussions began in earnest in 1992 about how the government might permanently address the "problem" of the widespread use of encryption.[38]

The murmurings about a possible "solution" signaled that a major conflict over encryption was inevitable. War was coming.

II. THE BATTLE OF THE CLIPPER CHIP AND THE WAR OVER KEY ESCROW

"We need the 'Clipper Chip' and other approaches that can both provide law-abiding citizens with access to the encryption they need and prevent criminals from using it to hide their illegal activities."

- White House Press Statement (April 1993)

On April 16, 1993, the White House unveiled a new initiative to address the competing challenges presented by the growing use of encryption.[39] The concept was simple: Government engineers had developed a state-of-the-art microchip, known as the "Clipper Chip," which could be inserted into consumer hardware telephones, providing the public with strong cryptographic tools without sacrificing the ability of law enforcement and intelligence agencies to access unencrypted versions of those communications.[40] The White House's official announcement called it "an important step in addressing the problem of encryption's dual-edge sword."[41]

The government offered assurances that the cryptographic algorithm used in the chips was more powerful than most available commercial encryption standards, protecting sensitive information while preserving "the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals."[42] Although adoption of the standard was technically voluntary, the government committed to purchasing a massive number of devices containing the Clipper Chip, which officials hoped would strongly influence the marketplace and result in its widespread adoption throughout the 1990s.[43]

HOW THE CLIPPER CHIP WORKED

The Clipper Chip technology relied on a system of "key escrow," in which a copy of each chip's unique encryption key would be stored by the government. In order to increase security, every key would be split in two so that no single organization had all the information necessary to conduct an unauthorized wiretap. These parts were entrusted to the Commerce Department's National Institute of Standards and Technology (NIST) and the Treasury Department. When they had "lawful authorization," the two federal agencies would jointly release them to law enforcement, providing the means to access unencrypted copies of the encrypted conversations.[44]

The NSA selected an encryption algorithm known as "Skipjack" to use in the Clipper Chip. Skipjack represented the culmination of the agency's efforts to establish a crypto standard that was ostensibly both strong and easy to compromise for legitimate law enforcement purposes. It was considerably more sophisticated and robust than any other established encryption algorithm then available.[45] But the NSA was only willing to let Skipjack be used under two conditions. First, because the algorithm itself was classified, it could only be embedded into devices (such as secure phones) that were manufactured in collaboration with the government; no one outside of the NSA was allowed to actually see how Skipjack worked, or use it for non-authorized purposes.[46] Second, the government mandated that Skipjack only be used in tandem with another system that introduced a "backdoor" into the cryptographic process — officially known as a "Law Enforcement Access Field," or LEAF — which government officials could use to gain access to the keys that protected any Skipjack-encrypted communication.[47]

The supposed strength of the Skipjack algorithm was central to the government's justification of the Clipper Chip proposal. By offering consumers encryption that was significantly more advanced than anything that had previously been

available, they hoped to build public trust and acceptance of the technology — enough to overcome concerns that it also facilitated government access through key escrow.[48] So the government convened a panel of academic and industry experts to conduct a review of Skipjack.[49] The leader of the group, a computer science professor from Georgetown named Dorothy Denning, was not only a crypto expert but had spent significant time researching and defending the positive role that the "hacker culture" could play in a modern information society.[50] In the early 1990s, she came out in favor of escrowed encryption as a means to balance individual privacy interests with overall social good.[51] In later years, Denning explained that as a participant in the panel she aimed to address concerns that the Clipper Chip was insecure and allegations that the NSA's decision to keep Skipjack classified was an attempt to hide vulnerabilities in the algorithm.[52]

The report's overall assessment of Skipjack was overwhelmingly positive. It concluded that it would be "36 years before the cost of breaking Skipjack by exhaustive search will be equal to the cost of breaking DES today," and that "there is no significant risk that Skipjack can be broken through a shortcut method of attack."[53]

In July 1993, around the same time that the expert panel's interim report on Skipjack was published, NIST initiated a public comment process on the Clipper Chip and the concept of key escrow more broadly. In a stark contrast to the affirmation expressed by Denning's group, only two of the 320 comments NIST received in response to its call were positive.[54] Experts participating in the NIST process voiced three primary sets of concerns with the proposal. First, many were wary of trusting the U.S. government as a keyholder, which would give federal agencies and law enforcement officials unprecedented access to — and power over — the private information of their citizens. Diffie, the father of public-key cryptography, argued that key escrow eliminated one of the system's key strengths: it re-introduced reliance on a third party to protect keys, a serious vulnerability.[55] To make matters worse, under the Clipper Chip scheme, this third party would be the government, which was especially troubling for privacy advocates who already questioned the government's respect for personal privacy.[56]

Relatedly, some industry commenters were concerned about how the Clipper Chip could affect future business, given the government's explicit intent to use its market power to shape the business environment and concerns that it might eventually make the technology mandatory.[57] And regardless, in the meantime, any company that wanted to do business directly with the government would be forced to adhere to the Clipper standard.[58] The chips themselves were expensive and, by design, could only be purchased from one supplier, which eliminated the potential for competition in production or pricing.[59] There was also a risk that other products might not be compatible with Clipper-enabled devices.[60] As journalist Steven Levy wrote in 1994, "the Government's stated intent is to manipulate the marketplace so that it will adopt an otherwise unpalatable scheme and make it the standard. Existing systems have to cope with... incompatibility with the new Government Clipper standard. Is it fair to call a system voluntary if the Government puts all sorts of obstacles in the way of its competitors?"[61]

Finally, there was speculation that Clipper was the first step toward prohibition of other forms of encryption that did not rely on key escrow or provide other means of backdoor access to communications.[62] Corporations and individuals that had already adopted encryption technology feared that their tools might be rendered less effective — or even declared illegal — if the Clipper Chip took off.[63]

PUBLIC MOBILIZATION AGAINST THE CLIPPER CHIP

The NIST comment process was not the only place where members of the public expressed concerns about the Clipper Chip. In fact, the proposal sparked an unprecedented wave of coordinated digital activism and lobbying efforts from a multitude of different groups.[64] Opposition to the Clipper Chip united privacy activists, technologists, academics, hackers, and industry leaders from across the political spectrum in the face of what they considered a significant threat to Internet security, economic competitiveness, and individual civil liberties.

In May 1993, a few weeks after the Clipper Chip proposal was announced, Whit Diffie testified before Congress on "The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology."[65] Diffie's testimony offered a window into the significance of the issue. "[S]uch a proposal is at best premature and at worst will have a damaging effect on both business

security and civil rights without making any improvement in law enforcement," he told the chamber.

Two weeks later, 26 of the nation's largest computer companies issued a statement through their trade organization, the Computer and Business Equipment Manufacturers Association, criticizing the economic viability of the Clipper plan. The group, which included Apple, AT&T, Hewlett Packard, IBM, and Xerox, told the Computer System Security and Privacy Advisory Board[66] that "encryption issues no longer can be treated as the province of only a small circle of national security, law-enforcement and technology experts."[67]

These efforts were only the beginning of a sustained effort by a diverse, loose-knit coalition of companies and activists to demonstrate the potential harms of the government's key escrow proposal. Key to that movement were the Cypherpunks, a "confederation of computer hackers, hardware engineers and high-tech rabble-rousers" who saw the proposal as a fundamental threat to electronic privacy.[68] As one of the Cypherpunk founders, Eric Hughes, said not long after the Clipper Chip was announced, "This plan creates the ears of Big Brother, just as Orwell warned."[69] The introduction of the Chip confirmed their fears that the government's mission was to cripple strong cryptography and keep it out of the public's hands.[70] Comprised mainly of technologists, the Cypherpunks embraced electronic mailing lists and online newsgroups to organize and disseminate their message.[71] They planned boycotts of AT&T — which had agreed to include the Clipper Chip in its new encrypted phone — and organized media campaigns, cooperating with new digital rights advocacy groups as part of their strategy to protect encryption.[72]

A wide range of individuals and organizations joined the Cypherpunks in the public campaign against the Clipper Chip. Recognizing the clear threat to the right to privacy, nascent digital rights groups like the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC) rallied against the proposal.[73] They organized experts to speak on panels, testified before Congress, and circulated electronic petitions, including one that garnered over 50,000 signatures — an unprecedented number in the early days of Internet activism.[74] Decades before popular online advocacy campaigns like the one that stopped the Protect IP Act (PIPA) and Stop Online Piracy Act (SOPA) in 2012,[75] these groups used Internet-enabled tools like email and online forums to spread and amplify their messages and force a public conversation about the merits of the Clipper proposal.[76]

A key part of the organizing strategy involved bringing together diverse groups of constituents to articulate the threats posed by the Clipper Chip. A group called the Computer Professionals for Social Responsibility (CPSR), which was founded in 1981 to "promote the responsible use of computer technology,"[77] coordinated many of these efforts, organizing letters and online petitions to demonstrate both widespread and expert opposition to the proposal. In January 1994, for example, CPSR brought together more than three dozen leading cryptographers, security experts, and privacy advocates in a letter to the Clinton Administration urging it to abandon the Clipper Chip scheme.[78] The signatories included many of the fathers of public cryptography — Diffie, Hellman, Rivest, Zimmermann, and Ralph Merkle among them — as well as trusted privacy and security experts like Bruce Schneier and Jerry Berman. The letter contained an ominous warning: "If the plan goes forward, commercial firms that hope to develop new products will face extensive government obstacles. Cryptographers who wish to develop new privacy enhancing technologies will be discouraged. Citizens who anticipate that the progress of technology will enhance personal privacy will find their expectations unfulfilled."[79]

Privacy advocates also teamed up with allies in industry to highlight the economic ramifications of the proposal. In May 1993, the Digital Privacy and Security Working Group — a coalition that included both privacy advocates and communications and computer companies like Apple, AT&T, Hewlett-Packard, IBM, Lotus Development Corporation, Microsoft, RSA Data Security, and Sun Microsystems — submitted a letter to President Clinton expressing concerns about the Clipper program. "While we recognize the importance of authorized national security and law enforcement needs," the letter stated, "we believe that there are fundamental privacy and other constitutional rights that must be taken into account."[80] These were some of the country's most powerful tech companies telling the White House that they were concerned about its sweeping new policies — the same companies who were expected to build products that employed key escrow systems.

Finally, a number of prominent politicians from both sides of the political spectrum joined the fray, including Senators John Kerry and Patrick Leahy and Representatives Maria Cantwell, Sam Gejdenson, and Ed Markey.[81] As Senator Patrick Leahy, one of the most vocal critics of Clipper, pointed out, one had to wonder if it would even be effective given the existence of alternatives like PGP. "I have serious questions about whether any sophisticated criminal or terrorist organization is going to use the one code endorsed by the U.S. Government and for which U.S. Government agents hold the decoding keys," he said in a 1994 hearing. "There are a multitude of alternative encryption methods commercially available."[82]

THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA)

It is difficult to tell the history of the Crypto Wars without telling the story of the Communications Assistance for Law Enforcement Act (CALEA), which Congress passed in 1994. CALEA was written in response to concerns from the FBI that, as telecommunications services were transitioning from analog to digital systems, they needed to preserve and enhance their ability to access communications transmitted by those services when they had lawful wiretap demands. After fierce debate between privacy advocates and law enforcement officials, both sides came to a compromise which included key concessions related to the use of encryption and pro-privacy updates to the Electronic Communications Privacy Act (ECPA). In particular, law enforcement, under heavy pressure from privacy advocates, had to accept that the law's mandate of intercept capability neither prevented telecommunications users from employing encryption nor required service providers to block or break such user-generated encryption. The law, at 47 USC § 1002(b)(3), explicitly states that a "telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." Further clarification can be found in the legislative history, which explicitly notes that "nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access" and "Nothing in the bill is intended to limit or otherwise prevent the use of any type of encryption within the United States."[83] The insertion of this language was a key win for the pro-encryption side in the Crypto Wars.

MARCHING TOWARD CLIPPER'S DEMISE

Despite growing opposition to the proposal, officials seemed intent on moving forward with it. In February 1994, the federal government officially adopted the technology behind the Clipper Chip as a Federal Information Processing Standard. Formally known as the Escrowed Encryption Standard (EES), its stated goal was to "facilitate the acquisition of devices that implement escrowed encryption techniques by Federal government agencies."[84]

The decision to move forward did little to reassure a skeptical public. By March 1994, according to a *CNN/TIME* poll, eighty percent of Americans opposed the Clipper Chip.[85] So the government went into public relations overdrive. In an attempt to engage directly with the opposition, the NSA's Chief Counsel Stewart Baker published an article in Wired, a tech-focused magazine, called "Don't Worry Be Happy: Why Clipper Is Good For You."[86] He also participated in an online Q&A on the subject, attempting to address the most pervasive myths about the Clipper Chip. Dorothy Denning also went on the offensive to advocate for the program, writing journal articles and op-eds, debating prominent critics online, and becoming one of the government's most vociferous advocates.[87] But these spirited defenses gained little traction in comparison to the diverse coalition of groups that had come together opposing Clipper.

The final death blow for the Clipper Chip came in June 1994 from Matt Blaze, a computer scientist at AT&T Bell Laboratories. In a technical paper titled "Protocol Failure in the Escrowed Encryption Standard," Blaze revealed that he had found a serious flaw in the Clipper Chip's security.[88] Simply put, Blaze demonstrated that the technology did not work as advertised: with the help of a brute force attack, a user could avoid transmitting the LEAF and circumvent the law-enforcement surveillance mechanism entirely.[89] Consequently, "some communications... can be encoded so that not even the government, decrypting keys in hand, can unscramble them."[90] The circumvention of Clipper's "backdoor" was the most damning evidence

yet, confirming fears that the encryption standard had significant unforeseen vulnerabilities.[91] What's more, the fact that the government could be shut out of its own surveillance protocol suggested that it was not qualified to be dictating technical mandates like the Clipper Chip at all. *The New York Times* headline about Blaze's research simply read: "Flaw Discovered in Federal Plan for Wiretapping."[92]

Blaze's discovery, coupled with the growing wave of public opposition, proved fatal to the original Clipper Chip proposal. In a January 1995 *Wall Street Journal* article about a new, much stronger chip being developed by AT&T and a semiconductor manufacturer, one analyst called the Clipper Chip "dead." As James Bidzos, the president of RSA Data Security, suggested, "the NSA must see that they're losing the battle."[93]

THE CLIPPER CHIP IS DEAD! LONG LIVE KEY ESCROW!

"This convergence of technology — cheap ubiquitous PCs, modems, FAX, digital phones, information superhighways, et cetera — is all part of the information revolution... All these devices will be using encryption...Trying to stop this is like trying to legislate the tides and the weather...even with the NSA and the FBI on their side, it's still impossible." [94]

Although the initial Clipper proposal flopped, the idea that the government could find a compromise that would allow it to access the keys to a widely implemented encryption standard lived on throughout the 1990s. Many policymakers clung to hopes that it was possible to securely implement a key escrow system for phone calls, emails, and other communications and storage applications.[95] In short, the government did not abandon its attempts to control cryptography after 1994 — it simply changed tactics. The evolution shifted toward the concept of "software key escrow," sometimes called "commercial key escrow" (CKE).[96] Later, some would also refer to these as "key recovery" schemes.[97]

Commercial key escrow was different from the Clipper Chip in a number of respects. Rather than focusing on the inclusion of a physical chip in hardware, the idea was to convince companies to implement a key escrow system themselves, a much more flexible alternative which could also be used for software products containing strong encryption. Instead of requiring the use of a single cryptographic algorithm, like the government had tried with Skipjack, new proposals simply limited the key length to 64 bits.[98] Under the new scheme, private escrow agents — certified by the government, of course — would hold the keys, rather than simply putting everything in the hands of the Treasury Department and NIST.[99] To sweeten the deal, the government offered the software industry a significant carrot: they would relax encryption export controls in exchange for agreeing to these criteria (a debate which we will discuss in greater depth in the next part of this paper).

Subsequent iterations of the proposal, introduced in 1995 and 1996, attempted to use the new commercial key escrow model to address the concerns of U.S. companies.[100] However, although marginally improved and repackaged, these key escrow proposals were ultimately no more palatable than the original Clipper Chip (and some even referred to them dismissively as "Clipper II" and "Clipper III"). Opponents maintained serious reservations about the potential abuse of power by the trusted third party in the absence of a strong mechanism for oversight and concerns about the security of the escrow system.[101] In May 1996, Senator Conrad Burns lambasted the Administration's third, and ultimately final, attempt: "[T]he third version of the administration's Clipper Chip proposal is a swing and a miss. It's time to quit relying on government mandates for what is truly a matter of great concern to the private sector: the expansion of commerce on the Internet and other computer networks."[102]

COMMERCIAL KEY ESCROW: "A SWING AND A MISS"

During the first Clipper debate there had been a vocal, if small, group of lawmakers opposing to the proposal in both the House and Senate. But as the debate expanded to more complex attempts to regulate encryption, those concerns grew and began to encompass broader value questions. How should privacy be protected in the digital age? How could the United States balance its interest in national security with its commitment to economic development and strong civil liberties when dealing encryption technology? Congress held hearings on the merits of key escrow, often led by Clipper opponents like Senator Leahy, Senator Ashcroft, Senator Burns, and Representative Bob Goodlatte.[103] None of them seemed

willing to accept the Administration's software key escrow proposals.

Some, like Senator Burns, argued that decisions about the use of encryption should be left up to businesses. In a letter to "the Internet community" in May 1996, he criticized the Administration for acting "without regard to the harm this policy has on American businesses' ability to compete in the global marketplace or the ability of American citizens to protect their privacy online. Until we get the federal government out of the way and encourage the development of strong cryptography for the global market, electronic commerce and the potential of the Internet will not be realized."[104] At the same time, Burns introduced legislation that would, among other things, prohibit mandatory key escrow and limit the Commerce Department's ability to impose encryption standards on non-government entities, as they had attempted to do with the Clipper Chip.[105] The Promotion of Commerce Online in the Digital Era (Pro-CODE) Act, along with similar proposed legislation like the Security and Freedom Through Encryption (SAFE) Act (which we discuss in detail in Part III) demonstrated the lengths to which some members of Congress were willing to go to stop the Administration's quest for key escrow.[106]

Other lawmakers stressed the importance of civil liberties in the digital era, clearly concerned about the impact of mandatory backdoors on those fundamental rights. In 1997, for example, John Ashcroft made an impassioned defense of online privacy, arguing that, "There is a concern that the Internet could be used to commit crimes and that advanced encryption could disguise such activity. However, we do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant government the Orwellian capability to listen at will and in real time to our communications across the Web?"[107]

Meanwhile, additional evidence against the adoption of these proposals continued to pile up. After an extensive study, the National Research Council (NRC) issued a 700-plus page report in 1996 on the policy challenges that encryption posed, strongly endorsing its availability. The report's primary recommendation stated that:

> No law should bar the manufacture, sale, or use of any form of encryption within the United States. Specifically, a legislative ban on the use of unescrowed encryption would raise both technical and legal or constitutional issues. Technically, many methods are available to circumvent such a ban; legally, constitutional issues, especially those related to free speech, would be almost certain to arise, issues that are not trivial to resolve.[108]

The report also found that the "debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis," undermining the claims made by those who invoked classified information to bolster their arguments.[109] Overall, the NRC's conclusions were overwhelmingly pro-encryption and had a powerful impact on the debate.

Around that time, the foreign governments whom the U.S. had been lobbying to adopt a key recovery approach overseas also rejected the idea. In early 1997, the U.S. had attempted to get the Organisation for Economic Co-operation and Development (OECD) to adopt a recommendation supporting key escrow and key recovery. But instead of supporting it, the OECD's final recommendation turned into a statement against the idea.[110] A European Commission report later that year went even further, declaring that, "In order to make good use of the commercial opportunities offered by electronic communication via open networks, a secure and trustworthy environment is... necessary. Cryptographic technologies are nowadays widely recognised as the essential tool for security and trust in electronic communication."[111] The Commission rejected the American proposals for key recovery on the basis that they undermined privacy, threatened economic growth, and were likely to be simply ineffective. "The report appears to all but doom efforts by the Clinton Administration and the Federal Bureau of Investigation to establish a global system in which people who use cryptography would have to deposit a 'key' for unlocking their codes with an independent outside organization," explained the *The New York Times* in October 1997.[112]

One of the final nails in the coffin for key escrow proposals came from a group of almost a dozen technical experts convened by the Center for Democracy & Technology that included Matt Blaze, Whit Diffie, Ronald Rivest, Bruce Schneier, John Gilmore, and Steve Bellovin.[113] In a paper examining a range of proposals for key recovery, key escrow and "trusted third party" encryption, they

concluded that the "deployment of key-recovery-based encryption infrastructures to meet law enforcement's stated specifications will result in substantial sacrifices in security and greatly increased costs to the end user." Their analysis suggested that the task would be "enormously complex" and "far beyond the experience and current competency of the field." What's more, they argued that, "Even if such infrastructures could be built, the risks and costs of such an operating environment may ultimately prove unacceptable."[114] The paper concluded that: "Key recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature. The massive deployment of key-recovery-based infrastructures to meet law enforcement's specifications will require significant sacrifices in security and convenience and substantially increased costs to all users of encryption."[115]

This final barrage of reports condemning the very idea of key escrow represented the closing shots in the battle that began with the Clipper Chip. However, by that point the Crypto Wars were also raging on another front, as pro- and anti-encryption forces battled over the government's role in restricting the availability of encryption overseas.

III. THE BATTLE OVER ENCRYPTION EXPORT CONTROLS

As the domestic fight over key escrow wore on, another battle was brewing on the international front over U.S. export controls and encryption technology. The question at the center of that debate was whether American technologies containing strong encryption should be made available overseas — which would in turn have a significant effect on the domestic availability and use of encryption tools as well.

TESTING THE WATERS: THE CASES OF KARN, BERNSTEIN, AND ZIMMERMANN

In 1994, an engineer named Phil Karn tried to send a copy of Bruce Schneier's book, Applied Cryptography,[116] and an accompanying floppy disk containing an electronic copy of the book text, outside of the United States.[117] At the time, products containing encryption were regulated as munitions exports under the International Traffic in Arms Regulations (ITAR), so Karn submitted a request to the Department of State to find out if the book was subject to any restrictions. The verdict that came back seemed paradoxical: although the book could be freely exported without restriction, the disks — which included the same encryption source code printed in Part Five of the physical book — were designated under a defense category subject to strict export controls.[118] Karn appealed the decision on the basis that the export restriction violated his First Amendment rights.

Although a judge ultimately dismissed Karn's claims in 1996, other high-profile legal incidents related to the export restrictions on encryption technology arose in the mid-1990s as well — part of a loosely coordinated effort to highlight growing concerns with the U.S. regulations as commercial encryption spread. For example, many are familiar with the case of Daniel Bernstein, a PhD candidate at UC Berkeley who fought a series of court challenges after he attempted to publish his public key encryption algorithm, "Snuffle," in both paper and online format.[119] Or Phil Zimmermann, the creator of PGP, who found himself under a three year investigation by the Justice Department for possible export violations because his cryptographic software program ended up in the hands of foreign Internet users, even though it was only uploaded to sites based in the United States.[120] The simple act of posting software to the Internet (or otherwise publishing source code) was considered an export, creating substantial legal hurdles for any individual or company that wished to sell products containing strong encryption abroad, or even make them freely available.

ENCRYPTION SOURCE CODE AS A WEAPON

"For the past two decades or more, a major goal of U.S. cryptography policy... has been to prevent strong mass-market cryptography from becoming widely available abroad, with export controls being the primary tool used to achieve this end."

- Michael Froomkin, "It Came from Planet Clipper" (1996)

Because they had historically been used by military and intelligence agencies almost exclusively, cryptographic tools were originally classified as munitions. Prior to 1996, all products using encryption were controlled under the International Traffic in Arms Regulations (ITAR) and listed on the U.S. Munitions List (USML).[121] Products with strong encryption were considered "dual use" technologies, meaning that they had both civilian and military applications, akin to nuclear technology or chemicals that could be weaponized. The export controls were based on the strength of the encryption — that is, the cryptographic key length[122] — and applied not only to hardware but also to encryption software and source code. In 1994, for example, products with "strong encryption" were those with key lengths greater

than 40 bits.[123] Under the ITAR regime, most applications to export cryptographic software with longer keys would be denied, although the restrictions were more lax when it came to "special" categories of applications like those that protected financial information.[124] Notably, the restrictions did not prevent people from sending encrypted messages abroad, but they prohibited the export of tools that provided the means to encrypt and decrypt those messages.

By the mid-1990s, as commercial use of encryption was taking off, the place of these tools on the USML became increasingly difficult to justify. Yet the U.S. government had a strong incentive to maintain strict encryption export controls. Limiting the ability of American companies to sell certain cryptographic products in foreign markets allowed the government to delay the spread and adoption of strong encryption technology abroad, which many officials feared could reduce their ability to gather intelligence on foreign targets.[125] Big companies like Apple, Microsoft, and Lotus knew that they often could not get licenses to sell strong cryptography overseas, so they were forced to make separate versions of their products for foreign markets. In these products, the encryption features were either stripped out entirely or relied on a weaker, "export-grade" version that was easier to crack. Journalist Steven Levy described export-grade encryption as "crypto lite": it was "strong enough to protect communications from casual intruders but not from the [g]overnment itself."[126] Or, as EFF put it in a 1997 bulletin, "the government has limited the key size of encryption to be exported to that which the NSA could crack."[127]

The implications of such a policy on the development of the worldwide cryptographic market were far-reaching. As a report by EPIC explained, export controls could reduce or weaken the availability of encryption in common programs, make it difficult to develop international encryption standards and build interoperable programs, and weaken the security of the Internet overall by forcing the development of local encryption alternatives that may not have gone through extensive peer review.[128]

Although export controls are generally not meant to have a direct impact on domestic economic activity — they are, after all, aimed at foreign sales — the encryption restrictions had broader consequences as well. By requiring American companies to seek approval before exporting cryptographic technologies, the U.S. government could continue to monitor and indirectly influence the development of commercial cryptography. The government could decide, for example, that it looked favorably on licenses for a particular tool or algorithm (perhaps, one might cynically suggest, because they already knew how to crack it) and thus create an incentive for U.S. companies to integrate that tool into their products instead of another method for which it might be harder to obtain a license. And while some large companies had enough of a business interest to produce different domestic and export versions of their products, for many it was too costly. Consequently, preventing the export of strong cryptography could actually restrict domestic use, forcing customers inside the United States to use the same weaker, export-grade cryptography that was required for foreign products.[129]

THE CAMPAIGN FOR CRYPTO WITHOUT BORDERS

By the mid-1990s, industry opposition to these restrictions had grown fairly strong. The computer industry argued that encryption export controls hampered technological development because the policies forced them to develop two distinct products for every piece of software — one for domestic use, and another for foreign consumption.[130] In the long term, business analysts also worried that the restrictions would hinder the American tech industry's overall competitiveness, given increasing demand for strong cryptography overseas as e-commerce spread and the development of foreign encryption alternatives expanded. A report from the U.S. Department of Commerce and the National Security Agency in 1996 acknowledged that some American businesses "believe that not being able to participate at the early stage of market development will be a tremendous obstacle to their future international competitiveness" and predicted that "export sales could increase significantly if allowed to export stronger algorithms — some by orders of magnitude."[131]

A separate study by the Economic Strategy Institute in 1998 translated the predictions into specific numbers, projecting anywhere between $35 billion and $95 billion in losses over the next five years as a result of encryption export controls.[132] "The record shows that these controls have had no discernible impact on national security, but have demonstrably compromised America's economic

security," the report concluded. "Foreign encryption products are present in the free international market, their competitiveness is increasing at the expense of American companies, and their products are outside U.S. regulatory authority. In this light, export controls are indefensible."[133]

Overall, the economic stakes were clear: encryption export controls were hurting U.S. businesses and undermining America's economic interests.

"Prohibiting the use of a particular form of cryptography for the express purpose of making communication intelligible to law enforcement officers is akin to prohibiting someone from speaking a language not understood by law enforcement officers." [134]

Export controls were also being legally challenged through a series of court cases which focused on the question of whether encryption source code should be recognized as "speech" subject to the protections of the First Amendment. The challenges mounted by Daniel Bernstein[135] and Phil Karn[136] in the mid-1990s — along with a third case, *Junger v. Daley*[137] — were premised on the argument that if code was speech, requiring an individual to register and obtain a license to publish code outside of the United States was an unconstitutional prior restraint on that speech.

Although two of the three cases were resolved much later — and with mixed rulings[138] — the debate about whether software code was speech shed light on some of the broader civil liberties issues at stake. As EFF's John Gilmore explained in an interview in 1994:

> There's a whole continuum between a book about cryptography, a book listing source code, an on-line copy of that book, a piece of actual source code, a piece of binary code stored on diskette, a piece of binary code loaded into a general-purpose computer, and a machine that does nothing but encoding and decoding. Somewhere along that continuum, you go from having full rights to anything you want, to having no export rights. It's not clear where the line should be drawn. The government benefits from leaving this line fuzzy, since people who actually have the right to export are afraid that they don't, and don't do it.[139]

Beyond the free speech issues, encryption export controls raised significant privacy questions. Many of the concerns voiced by privacy advocates were quite similar to those brought up in the domestic Clipper Chip debate (which we describe in the previous section of this paper) but a few were unique to the export controls conflict. In particular, some argued that restrictions on the export of encryption worldwide effectively created two different standards for privacy, providing a higher degree of protection for communications between Americans within the United States. This essentially meant that the Fourth Amendment right to be secure in one's digital "papers and effects" stopped at the U.S. border, even for American citizens communicating with colleagues and loved ones abroad.[140] These concerns were exacerbated by the fact that there had been several high-profile demonstrations of how easy it had become to crack export-grade crypto by the late 1990s.[141]

Finally, a growing body of evidence suggested that by the end of the twentieth century, encryption export controls were no longer very effective at stopping the spread of strong encryption overseas. "Strong cryptography only gets easier to implement — and harder to regulate — over time," wrote Ron Rivest, one of the developers of the RSA algorithm, in 1998.[142] A comprehensive report from the Cyberspace Policy Institute at George Washington University in June 1999 noted that there were over 500 foreign companies manufacturing or distributing foreign cryptographic products in nearly 70 countries outside the United States.[143] Furthermore, the report found that on average the quality of the foreign encryption products was comparable to those built in the United States.[144] As Alan Davidson, a staff attorney at the Center for Democracy & Technology, explained to Congress, "world-class strong cryptography is now widely available outside the United States. The result is that criminals, terrorist organizations, and rogue governments all have access to the strongest encryption, while law-abiding individuals around the world still do not have strong encryption in the mass-market products they use."[145] The logic of Davidson's argument echoed the famous statement by Phil Zimmermann in his explanation of why he created PGP: "If privacy is outlawed, only outlaws will have privacy."[146]

FROM WEAKENING CRYPTO TO WEAKENED RESTRICTIONS: THE LIBERALIZATION PROCESS

"The vigorous application of cryptography may also improve national security: the encryption of communications, for example, protects U.S. businesses from industrial espionage. Paradoxically, we may create a safer society by promoting a technology that somewhat hampers law enforcement."

In the fall of 1996, the Clinton Administration took a small but significant first step toward recognizing the challenges that export controls presented for the spread of commercial encryption products. Vice President Al Gore, who had championed the Clipper Chip just a few years earlier, delivered the news on October 1, 1996, as part of a broader encryption-related initiative. In a statement, Gore acknowledged the value of encryption in protecting privacy and enabling secure online transactions, as well as the overall benefits to Internet security and American competitiveness in the technology sector:

> The Administration's initiative will make it easier for Americans to use stronger encryption products — whether at home or abroad — to protect their privacy, intellectual property, and other valuable information. It will support the growth of electronic commerce, increase the security of the global information, and sustain the economic competitiveness of U.S. encryption product manufacturers during the transition to a key management infrastructure.[147]

Gore went on to describe a temporary relaxation of export controls as "part of a broader encryption policy effort designed to promote electronic information security and public safety." The change meant that commercial encryption products would no longer be considered munitions, and would instead become part of the more extensive push by the administration to implement commercial key recovery legislation. He described the policy change as "broadly consistent with the recent recommendations of the National Research Council"[148] and suggested that it addressed "many of the objectives of pending Congressional legislation."

Six weeks later, the White House issued Executive Order 13026, which officially transferred the control of the export of non-military encryption items on the USML from the Department of State to the Department of Commerce's Export Administration Regulations (EAR) and placed them on the Commerce Control List (CCL).[149] Commerce created a new category of foreign policy and national security controls for "encryption items" (EI), which would allow the commercial distribution of several classes of software, including products used in financial transactions, encryption software that employed key lengths of less than 64 bits, and retail products exported to individual consumers.[150] The shift was generally met with support by privacy advocates and companies alike, who saw this as a first step in a broader liberalization of encryption export controls. But because these items still required a license — and because they came as part of a broader effort to implement key recovery proposals — the change left a number of the concerns expressed by industry, civil liberties advocates, and technical experts unresolved.[151]

"Only by allowing the use of strong encryption, not only domestically but internationally as well, can we hope to make the Internet a safe and secure environment."

Around the same time that the Clinton Administration was tentatively taking its first steps toward liberalization, a broader legislative effort — which Vice President Gore referred to in his October 1996 speech — was underway to shift U.S. policy more dramatically in the direction of a positive encryption agenda. Representative Bob Goodlatte first introduced the Security and Freedom Through Encryption (SAFE) Act in Congress in March 1996. The bill's overall goal was simple: "to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption."[152] It aimed to prevent the government from creating a mandatory key-escrow system[153] and remove export restrictions on most encryption, including lifting the existing limits on key length.[154] Multiple versions of the legislation were re-introduced in the House and Senate throughout the late 1990s. Eventually, the SAFE Act garnered sponsorship from a majority of the members of the House of Representatives — 258, to be exact — reflecting a broad and bipartisan consensus on the importance of

promoting and protecting access to strong encryption tools. A similar effort was undertaken by Senator Conrad Burns in the Pro-CODE Act (which we describe in Part II).

With the pressure to relax encryption export controls growing on the Hill, in the courts, and in the court of public opinion, a vigorous debate was underway within the Clinton Administration in 1997 and 1998 about how to adapt while still protecting the interests of law enforcement. In September 1998, after "several months of intensive dialogue between the government and U.S. industry, the law enforcement community and privacy groups," Vice President Gore announced additional concessions relating to the export of strong encryption for purposes like financial transactions, electronic banking, and health records.[155] Under the new policy, hardware and software products containing 56-bit encryption could be exported without a license, and the requirement that companies submit key recovery plans in exchange for permission export those products was removed.[156] But as a CNET reporter described it, "The plan announced today continues the administration's piecemeal strategy of easing some of the export controls without fully lifting the limits as many high-tech companies and civil liberties groups would like."[157] They continued to fight for more significant export control relief.

In August 1999, the President's Export Council Subcommittee on Encryption[158] made a number of more aggressive recommendations related to revising encryption export regulations, including raising the key length limit for mass market hardware and software to 128 bits, which had become the standard for electronic commerce at that point. The report was unequivocal in its arguments that,

> The U.S. government should recognize market realities... [and] the difficulty of controlling mass-market products once they are allowed to be exported even to limited sectors. Furthermore, mass-market products play an important role in protecting the communications and data of individuals—a segment of the encryption user community that has been neglected in recent liberalizations to the U.S. export policy.[159]

Shortly thereafter, on September 16, 1999, the White House made a major announcement: in the coming months, it would update its encryption policies to remove virtually all restrictions on the export of retail encryption products, regardless of key length.[160] The government's intent was to "significantly update and simplify export controls on encryption," and it emphasized that, "The updated guidelines will allow U.S. companies new opportunities to sell their products to most end users in global markets." Guidance published by the Commerce Department that same day offered additional details, including the fact that they would continue to restrict exports to sanctioned countries and foreign government and military end users.[161]

The announcement caught many encryption advocates by surprise, but they nonetheless quickly leapt to support it. *The New York Times* called the new policy change a "reversal," declaring: "Bucking pressure from the Justice Department, the F.B.I. and intelligence agencies, the White House yesterday essentially eliminated its complex controls on the export of data-scrambling hardware and software, handing a surprise victory to Congressional, high-technology and privacy groups that have spent years fighting for the change."[162]

Representative Bob Goodlatte, who had championed the SAFE Act for a number of years, called it "huge news" and a "tremendous victory."[163] As Steven Levy put it succinctly: "It was official: public crypto was our friend."[164]

The following January, the Commerce Department officially released the revised regulations, which amended the EAR "to allow the export and reexport of any encryption commodity or software to individuals, commercial firms, and other non-government end-users in all destinations."[165] Although a handful of prohibitions remained in place, the change swept away the vast majority of the restrictions that had been the focus of the debate in the previous decade.

One of the key steps in this liberalization process was the creation of an exemption for the export of free and open source cryptography. The January 2000 changes made "unrestricted encryption source code" exportable under License Exception TSU, which covers a range of generally available and mass-market technology and software.[166] This eliminated the ambiguity surrounding the export of products like PGP, removing them from legal limbo in which it was uncertain whether they met the criteria included in the free and open source exemption.

Although the truce declared at the end of 1999 took many encryption proponents by surprise,[167] both industry and civil liberties advocates got virtually everything for which they had asked. As Rubinstein and Hintze summarize, American "export policy [had] evolved from case-by-case licensing of individual encryption exports, to policies designed to encourage 'key escrow' or 'key recovery' encryption systems, to broad approvals for exports to certain preferred industry sectors, and finally to nearly free exportability of most products."[168]

After the last shots had been fired, the Crypto Wars ended with a broad policy consensus: ensuring Americans' ability to use and distribute strong encryption free of government backdoors was critical to maintaining the nation's economic security and information security, as well as maintaining Americans' constitutional rights to privacy and free speech.

IV. POST-WAR: HOW THE CRYPTO WARRIORS WERE PROVEN RIGHT

The Crypto Wars of the 1990s offer a compelling tale about the convergence of technical experts, business interests, civil liberties advocates, and political leaders to articulate why encryption benefits Internet security, the information economy, and civil liberties. In the decades since the conflict ended, many of the crypto warriors' predictions have been proven right, while new arguments in favor of strong encryption have also emerged as the technology continues to change.

THE INTERNET AND THE INFORMATION ECONOMY HAVE GROWN EXPONENTIALLY SINCE THE CRYPTO WARS

The resolution of Crypto Wars in favor of robust encryption for everyone played a significant role in jumpstarting the nascent Internet economy in the early 21st century. In 1996, the National Research Council wrote that it was "widely believed that encryption [would] be broadly adopted and embedded in most electronic communications products and applications for handling potentially valuable data."[169] Just as they predicted, the late 1990s and early 2000s witnessed the emergence of a vibrant marketplace of new Internet services based on secure digital communications and the widespread migration of sensitive communications online. Many of the major titans of the Internet economy were founded in the five-year period immediately following the demise of the Clipper Chip proposal, including Ebay, Paypal, and Amazon. Their business models depended on their customers' ability to conduct secure transactions online and to trust that connections advertised as secure actually were.[170] Indeed, since the Crypto Wars ended, electronic commerce in the United States has risen steadily.[171]

One of the most important protocols to emerge during this period was the Secure Sockets Layer (SSL) specification, which eventually became "the secure communications protocol of choice for a large part of the Internet community."[172] SSL and its successor, Transport Layer Security (TLS), rely on encryption to provide, among other things, secure connections between Internet browsers and the websites with which they communicate.[173] The Secure Shell Protocol (SSH), although lesser known, quickly became an equally indispensable tool for remotely administering large numbers of servers — an essential prerequisite for the rise of the modern data-center.[174] At the same time as these protocols were being refined, entirely new industries were being formed to both support and leverage the new ecosystem of secure digital communications. Companies like VeriSign[175] (a spinoff of RSA Security) and Comodo[176] were formed to manage public key infrastructure, issuing the digital certificates used for encryption. Their products provide independent verification to consumers that the secure sites they are visiting have not been tampered with and are not being impersonated by malicious actors. In addition to bolstering consumer confidence, the added protection provided by encryption also prevents a substantial number of real attacks that would otherwise be extremely easy to carry out.

In the early 21st century, the emergence of these foundational technologies allowed the encrypted web to expand rapidly to include electronic banking, electronic medical records systems, online bill payment tools, home automation systems, e-filing systems for taxes, and VPNs. Additionally, SSL was embedded in a huge number of physical products, including smartphones, home routers, and media streaming devices — products and services that now represent billion dollar industries unto themselves. Those who argued during the Crypto Wars that encryption would be a foundational technology for the growth of the digital economy have undeniably been proven right.

STRONG ENCRYPTION HAS BECOME A BEDROCK TECHNOLOGY THAT PROTECTS THE SECURITY OF THE INTERNET

The evolution of the ecosystem for encrypted communications has also enhanced the protection of individual communications and improved cybersecurity. Today, strong encryption is an essential ingredient in the overall security of the modern network, and adopting technologies like HTTPS is increasingly considered an industry best-practice among major technology companies.[177] Even the report of the President's Review Group on Intelligence and Communications Technologies, the panel of experts appointed by President Barack Obama to review the NSA's surveillance activities after the 2013 Snowden leaks, was unequivocal in its emphasis on the importance of strong encryption to protect data in transit and at rest. The Review Group wrote that:

> Encryption is an essential basis for trust on the Internet; without such trust, valuable communications would not be possible. For the entire system to work, encryption software itself must be trustworthy. Users of encryption must be confident, and justifiably confident, that only those people they designate can decrypt their data.... Indeed, in light of the massive increase in cyber-crime and intellectual property theft on-line, the use of encryption should be greatly expanded to protect not only data in transit, but also data at rest on networks, in storage, and in the cloud.[178]

The report further recommended that the U.S. government should:

> Promote security[] by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.[179]

Moreover, there is now a significant body of evidence that, as Bob Goodlatte argued back in 1997, "Strong encryption *prevents* crime."[180] This has become particularly true as smartphones and other personal devices that store vast amount of user data have risen in popularity over the past decade. Encryption can stop or mitigate the damage from crimes like identity theft and fraud targeted at smartphone users.[181]

Meanwhile, recent incidents have confirmed the dangers of promoting policies that weaken encryption. In March 2015, a team of researchers discovered a bug that "for more than a decade has made it possible for attackers to decrypt HTTPS-protected traffic passing between Android or Apple devices and hundreds of thousands or millions of websites."[182] The researchers called it a "FREAK" attack, which stands for "Factoring attack on RSA-EXPORT Keys," a deliberate reference to the export-grade encryption that was developed by some companies in the 1990s to comply with encryption export controls. An attack occurs when an attacker forces a vulnerable browser to use weak 512-bit RSA keys,[183] which can now be cracked in a matter of hours, and then steals passwords and other personal information.[184] Although most engineers abandoned the use of export-grade keys after export controls were liberalized, it appears that this functionality continued to exist, largely unnoticed, in certain devices and servers for decades.[185] In May 2015, researchers uncovered a similar type of attack called Logjam which exploits a weakness in TLS to downgrade encryption keys to weaker export-grade key lengths.[186] In both the FREAK and Logjam cases, the vulnerabilities were a direct result of the decision to split functionality into domestic grade and export-grade encryption. The attacks serve as a powerful reminder about the vulnerabilities that may be created by policies that restrict the export of strong encryption.

STRONG ENCRYPTION HAS BECOME AN INTEGRAL TOOL IN THE PROTECTION OF PRIVACY AND THE PROMOTION OF FREE EXPRESSION ONLINE

The end of the Crypto Wars ushered in an age where the security and privacy protections afforded by the use of strong encryption also help promote free expression. As the American Civil Liberties Union recently explained in a submission to the UN Human Rights Council, "encryption and anonymity are the modern safeguards for free expression. Without them, online communications are

effectively unprotected as they traverse the Internet, vulnerable to interception and review in bulk.
Encryption makes mass surveillance significantly more costly."[187]

The human rights benefits of strong encryption have undoubtedly become more evident since the end of the Crypto Wars. Support for strong encryption has become an integral part of American foreign policy related to Internet freedom, and since 2010, the U.S. government has built up a successful policy and programming agenda based on promoting an open and free Internet.[188] These efforts include providing over $120 million in funding for "groups working to advance Internet freedom," much of which specifically funds circumvention tools that rely on strong encryption — which makes Internet censorship significantly harder — as part of the underlying technology.[189] Similarly, a June 2015 report by David Kaye, the UN Special Rapporteur for Freedom of Expression and Opinion found that, "Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks."[190] The report goes on to urge all states to protect and promote the use of strong encryption, and not to restrict it in any way.

Over the past fifteen years, a virtuous cycle between strong encryption, economic growth, and support for free expression online has evolved. Some experts have dubbed this phenomenon "collateral freedom," which refers to the fact that, "When crucial business activity is inseparable from Internet freedom, the prospects for Internet freedom improve."[191] Free expression and support for human rights have certainly benefited from the rapid expansion of encryption in the past two decades.

THE ORGANIZING EFFORTS CARRIED OUT IN SUPPORT OF INTERNET OPENNESS DURING THE CRYPTO WARS HAVE HELPED SHAPE MODERN INTERNET ADVOCACY CAMPAIGNS

It is important to remember that the successful resolution of the Crypto Wars was neither a foregone conclusion nor a happy accident of aligned interests. Advocates worked tirelessly to build a strong case in favor of the benefits of encryption, bringing together technical experts alongside a broad coalition of privacy advocates and companies to engage in a coordinated effort of public education and targeted lobbying. They also worked closely with members of Congress, building support across the political spectrum through organizations like the non-profit Internet Caucus Advisory Committee[192] and the Americans for Computer Privacy.[193]

The success of this campaign during the Crypto Wars has informed a number of subsequent advocacy campaigns, including the Internet blackout and coordinated protests that stopped the 2012 Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) as well as the months-long push to get the Federal Communications Commission to adopt strong net neutrality rules after the 2014 Verizon v. FCC court decision. Organizers of both the SOPA/PIPA and net neutrality campaigns employed a number of similar tactics to convince policymakers to heed their advice, bringing together broad coalitions of stakeholders from both the public interest and the private sector and emphasizing the technical, legal, and economic impacts of the decisions at hand.[194] Thus, history has not only validated the substance of the crypto warriors' arguments, but also confirmed the wisdom of their strategy — one that may need to be implemented again as new threats to encryption are on the rise.

CONCLUSION: ENCRYPTION UNDER THREAT... AGAIN

Unfortunately, in the past few years the consensus that strong encryption is good for security, liberty, and economic growth has come under threat. The June 2013 revelations about the U.S. National Security Agency's pervasive surveillance programs — not to mention the NSA's direct attempts to thwart Internet security to facilitate its own spying — dramatically shifted the national conversation, highlighting the vulnerabilities in many of the tools and networks on which we now rely for both everyday and sensitive communications. While ordinary individuals, civil liberties advocates, and major technology companies have since embraced greater use of encryption as a necessary step to address a wide range of modern threats from both government and nongovernment actors, intelligence agencies and law enforcement officials have also become increasingly outspoken against measures to strengthen these systems through encryption. To make their case, they have revived many of the arguments they made about encryption in the 1990s, seeming to have forgotten the lessons of the past. In response, encryption proponents have countered with many of the same arguments that they made in the 1990s, along with a few new ones.[195]

It seems like we may once again be on the verge of another war: a Crypto War 2.0. But it would be far wiser to maintain the peace than to begin a new and unnecessary conflict. We already had a robust public debate that resolved this dispute, and nothing has changed since the 1990s that would cast doubt on the policy conclusions we reached then; indeed, the post-war period has only reinforced those conclusions. Although there are numerous individual lessons from the Crypto Wars, the overarching takeaway is that weakening or otherwise undermining encryption is bad for our economy, our economic security, and our civil liberties — and there is no reason to repeat our previous mistakes.

ENDNOTES

1. Craig Timberg, "Apple will no longer unlock most iPhones, iPads for police, even with search warrants," *The Washington Post*, September 18, 2014, http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html (accessed June 15, 2015); Craig Timberg, "Newst Androids will join iPhones in offering default encryption, blocking police," *The Washington Post*, September 18, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/ (accessed June 15, 2015).

2. Danielle Kehl et al., "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, and Cybersecurity," *New America's Open Technology Institute*, July 2014, https://static.newamerica.org/attachments/184-surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-and-cybersecurity/Surveilance_Costs_Final.pdf (accessed June 15, 2015).

3. End-to-end encryption is a system in which "messages are encrypted in a way that allows only the unique recipient of a message to decrypt it, and not anyone in between." With end-to-end encryption, you encrypt the contents of a message on your local machine or device. That data is then transmitted as ciphertext by the email provider to the intended recipient, who is the only person who can decrypt and read it. Danielle Kehl, "Encryption 101," *Slate*, February 24, 2015, http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html (accessed June 15, 2015).

4. Andy Greenberg, "Whatsapp Just Switched On End-to-End Encryption for Hundreds of Millions of Users," *Wired*, November 18, 2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/ (accessed June 15, 2015); Andrea Peterson, "Yahoo's plan to get Mail users to encrypt their e-mail: Make it simple," *The Washington Post*, March 15, 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/15/yahoos-plan-to-get-mail-users-to-encrypt-their-e-mail-make-it-simple/ (accessed June 15, 2015).

5. Craig Timberg and Greg Miller, "FBI blasts Apple, Google for locking police out of phones," *The Washington Post*, September 25, 2014, http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html (accessed June 15, 2015); "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *The Brookings Institution*, October 16, 2015, event recording available at http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi (accessed June 15, 2015); Cyrus Vance Jr., "Apple and Google threaten public safety with default smartphone encryption," *The Washington Post*, September 26, 2014, http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphoneencryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html (accessed June 15, 2015).

6. David E. Sanger and Matt Apuzzo, "James Comey, FBI Director, Hints at Action as Cell Phone Data is Locked," *The New York Times*, October 16, 2014, http://www.nytimes.com/2014/10/17/us/politics/fbi-director-in-policy-speech-calls-dark-devices-hindrance-to-crime-solving.html?_r=1 (accessed June 15, 2015); "FBI Director Continues Crusade Against Encryption, Calls on Congress to Act," *The District Sentinel*, March 25, 2015, https://www.districtsentinel.com/fbi-director-continues-crusade-against-encryption-calls-on-congress-to-act/ (accessed June 15, 2015).

7. Craig Timberg, "Holder urges tech companies to leave device backdoors open for police," *The Washington Post*, September 30, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/30/holder-urges-tech-companies-to-leave-device-backdoors-open-for-police/ (accessed June 15, 2015).

8. Ellen Nakashima and Barton Gellman, "As encryption spreads, U.S. grapples with clash between privacy, security," *The Washington Post*, April 10, 2015, http://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html (accessed June 15, 2015); "VIDEO: ODNI General Counsel Robert Litt Speaks on Intelligence Surveillance Reform at the Brookings Institute," *Office of the Director of National Intelligence: IC on the Record*, February 4, 2015, http://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on (accessed June 15, 2015).

9. For a fairly comprehensive list of articles and new stories, see Andi Wilson, "Updated #Cryptodebate Bibliography," New America's Open Technology Institute, June 16, 2015, http://www.newamerica.org/oti/updated-cryptodebate-bibliography/. *For specific discussions of the technical feasibility see, e.g.*, Jeffrey Vagle and Matt Blaze, "Security 'Front Doors' vs. 'backdoors': A Distinction Without a Difference," *Just Security*, October 17, 2014, http://justsecurity.org/16503/security-front-doors-vs-back-doors-distinction-difference/ (accessed June 15, 2015); Bruce Schneier, "Stop the hysteria over Apple encryption," *CNN*, October 31, 2014, http://www.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/index.html (accessed June 15, 2015); Tim Greene, "RSA: Panel calls NSA access to encryption keys a bad idea," *Network World*, April 22, 2015, http://www.networkworld.com/article/2913280/securityo/rsa-panel-

calls-nsa-access-to-encryption-keys-a-bad-idea.html (accessed June 15, 2015); Joseph Lorenzo Hall, "The NSA's Split-Key Encryption Proposal is Not Serious," *Center for Democracy & Technology*, April 20, 2015, https://cdt.org/blog/the-nsas-split-key-encryption-proposal-is-not-serious/ (accessed June 15, 2015); Andrea Peterson, "Congressman with computer science degree: Encryption back-doors are 'technologically stupid,'" *The Washington Post*, April 30, 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2015/04/30/congressman-with-computer-science-degree-encryption-back-doors-are-technologically-stupid/ (accessed June 15, 2015).

10. Julian Sanchez, "Old Technopanic in New iBottles," *Cato at Liberty*, September 23, 2014, http://www.cato.org/blog/old-technopanic-new-ibottles (accessed June 15, 2015);

11. For a succinct look back on the debate, *see* Matt Blaze, "Key Escrow from a Safe Distance: Looking Back at the Clipper Chip," *University of Pennsylvania*, December 2011, http://www.crypto.com/papers/escrow-acsac11.pdf (accessed June 15, 2015).

12. A good source for historical information is David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (Scribner: 1996). *See also* "Statement of Cindy A. Cohn, Testimony on Encryption as Constitutionally Protected Speech," before the Senate Judiciary Committee's Subcommittee on Constitution, Federalism and Property Rights, Washington, D.C., March 17, 1998, available at http://gos.sbc.edu/c/cohn.html (accessed June 15, 2015).

13. Kahn, *The Codebreakers*.

14. "History of Encryption," *The SANS Institute*, 2001, available at http://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730 (accessed June 15, 2015).

15. "Encryption is an essential tool in providing security in the information age. Encryption is based on the use of mathematical procedures to scramble data so that it is extremely difficult — if not virtually impossible — for anyone other than authorized recipients to recover the original 'plaintext.' Properly implemented encryption allows sensitive information to be stored on insecure computers or transmitted across insecure networks." Hal Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 1997, available at https://www.schneier.com/paper-key-escrow.pdf (accessed June 15, 2015). For a simple explanation of how encryption works to protect online security today, *see* Kehl, "Encryption 101," *Slate*, February 24, 2015.

16. "History of Encryption."

17. Also sometimes called the Diffie-Hellman key exchange.

18. Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, Nov. 6, November 1976. http://www.cs.tau.ac.il/~bchor/diffie-hellman.pdf (accessed June 15, 2015). It was later called the Diffie-Hellman Key Exchange.

19. Keith Palmgren, "Diffie-Hellman Key Exchange: A Non-mathematician's explanation," *ISSA: The Global Voice of Information Security*, October 2006, available at http://academic.regis.edu/cias/ia/Palmgren_-_Diffie-Hellman_Key_Exchange.pdf (accessed June 15, 2015).

20. Steven Levy, *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age* (New York: Penguin Books, 2002), 71.

21. Peter Wayner, "A Patent Falls, and the Internet Dances," *New York Times*, September 6, 1997, https://www.ics.uci.edu/~ics54/doc/security/pkhistory.html (accessed June 15, 2015). ("Before public key cryptography, anyone who wanted to use a secret code needed to arrange for both sides to have a copy of the key used to scramble the data, a problem that requires either trusted couriers or advance meetings. PKC, as it is sometimes known, erased this problem by making it possible for two people, or more properly their computers, to agree upon a key by performing some complicated mathematics. There is no publicly known way for an eavesdropper to pick up the key by listening in.")

22. R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Crypto Systems," *Massachusetts Institute of Technology*, April 4, 1977, available at http://people.csail.mit.edu/rivest/Rsapaper.pdf (accessed June 15, 2015). ("The era of "electronic mail" may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are private, and (b) messages can be signed. We demonstrate in this paper how to build these capabilities into an electronic mail system.")

23. *Ibid*, 2

24. Jay Stowsky, "Secrets or Shields to Share? New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age," UCAIS Berkeley Roundtable on the International Economy, Working Paper Series, February 21, 2003, available at http://econpapers.repec.org/paper/cdlucbrie/qt89r4j908.htm (accessed June 15, 2015).

25. Levy, *Crypto*, 130.

26. Other factors included the increased use of portable and mobile devices (which meant that sensitive data was being sent or carried to a wide variety of locations, including on media that could be lost or stolen easily) and the increased use of public and wireless networks.

27. Lotus Corporation's groupware products required built-in

encryption systems to "ensure the confidentiality of the electronic messages that Lotus Notes' major corporate users would exchange by the thousands across computer networks." Stowsky, "Secrets or Shields to Share?"

28. Levy, *Crypto*, 149-125; Stowsky, "Secrets or Shields to Share?"

29. Stowsky, "Secrets or Shields to Share?"

30. Zimmermann, "Why I Wrote PGP."

31. Ibid.

32. Levy, *Crypto*, 106-107.

33. Henry Corrigan-Gibbs, "Keeping Secrets," *Stanford Magazine*, November/December 2014, available at http://www.henrycg.com/files/academic/papers/stanfordmag14keeping.pdf (accessed June 15, 2015).

34. Stowsky, "Secrets or Shields to Share?"

35. One of the primary ways that the U.S. government could exert control over the development of cryptographic standards was through limits on funding for academics working in cryptography. Many academics received funding from organizations like the National Science Foundation (NSF), which would send research proposals about encryption technology to the NSA.

36. John Markoff, "Paper on Codes Is Sent Despite U.S. Objections," *The New York Times*, August 9, 1989, http://www.nytimes.com/1989/08/09/us/paper-on-codes-is-sent-despite-us-objections.html (accessed June 15, 2015). ("Over the past 12 years the National Security Agency has consistently opposed the publication or transmission of research on encryption technology. The agency is concerned that advances in cryptography will make it harder to break coded transmissions sent by foreign intelligence agents in the United States to their governments.")

37. Section 2201 of S. 266, The Comprehensive Counter-Terrorism Act of 1991, available at https://w2.eff.org/Privacy/Surveillance/?f=s266_91.comments.txt (accessed June 15, 2015). A few months later, after an outpouring of backlash from civil liberties groups, Biden quietly withdrew the bill. Levy, *Crypto*, 198.

38. Levy, *Crypto*, 228.

39. "Statement by the Press Secretary," *The White House*, April 16, 1993, available at https://www.epic.org/crypto/clipper/white_house_statement_4_93.html ("1993 WH Clipper Chip Announcement") (accessed June 15, 2015).

40. A. Michael Froomkin, "It Came From Planet Clipper: The Battle Over Cryptographic Key Escrow," *Chicago Legal Forum Law of Cyberspace* (1996), available at http://osaka.law.miami.edu/~froomkin/articles/planet_clipper.htm (accessed June 15, 2015).

41. 1993 WH Clipper Chip Announcement.

42. Ibid.

43. Levy, *Crypto*, 249.

44. Froomkin, "It Came From Planet Clipper: The Battle Over Cryptographic Key Escrow."

45. Skipjack was viewed as stronger than the most popular alternative, the Data Encryption Standard (DES). DES is a symmetric key encryption algorithm that was designed by IBM researchers in the early 1970s. When the U.S. government made it a Federal Information Processing Standard in 1977, DES became the algorithm of choice for the encryption of commercial and sensitive yet unclassified government computer data. Many industries, like financial services and banking, quickly adopted DES to protect their sensitive data. The design of DES keys limits their length to an effective 56-bits, which some researchers felt wasn't adequately secure. Some are suspicious that the National Security Agency weakened IBM's original algorithm, reducing it from 112-bits to 56. Even so, DES was revised and adopted as federal standard again three more times (in 1983, 1988, and 1993) before it was withdrawn as a standard. Skipjack, the algorithm selected for use in the Clipper Chip, was also symmetric but it had an 80-bit key which made it significantly more secure than the DES algorithm. As a result of this increased key length, Skipjack encryption has 2^{80} possible keys, compared to DES's 2^{56} possible keys. This made it much less feasible to perform an exhaustive (brute-force) search for the key used to secure a particular communication.

46. Ernest F. Brickell, Dorothy E. Denning, Stephen T. Kent, David P. Maher, and Walter Tuchman, "Skipjack Review Interim Report," July 28, 1993, available at http://faculty.nps.edu/dedennin/publications/SkipjackReview.txt (accessed June 15, 2015).

47. The Law Enforcement Access Field (LEAF) was the core component of a novel specification for allowing easy — though theoretically restricted — third-party access to communication systems that were otherwise secured with strong crypto. Every device that made up a LEAF-equipped "secure" communications system had the digital equivalent of a skeleton key, which could be used to access anything that particular device ever sent. Specifically, this meant that every communication was required to begin with the transmission of a LEAF message, which would contain the ID number of the originating device, along with an encrypted copy of the "session key" used to encipher the rest of the communication. The skeleton key for any given device (literally just another cryptographic key) would grant access to any session key that the device had ever generated.

48. Levy, *Crypto*, 249-253.

49. Brickell et al., "Skipjack Review Interim Report."

50. *See, e.g.*, Dorothy E. Denning, "Concerning Hackers Who Break Into Computer Systems," presented at the 13th National Security Conference in Washington DC, October 1-4, 1990, available at http://cpsr.org/prevsite/cpsr/privacy/crime/denning.hackers.html/ (accessed June 15, 2015).

51. Steven Levy, "Clipper Chick," *Wired*, September 1996, http://archive.wired.com/wired/archive/4.09/denning_pr.html; Dorothy E. Denning, "The Case for Clipper (Clipper Chip offers escrowed encryption)," *MIT's Technology Review*, July 1995, available at http://encryption_policies.tripod.com/us/denning_0795_clipper.htm (accessed June 15, 2015).

52. Denning, "The Case for Clipper."

53. Brickell et al., "Skipjack Review Interim Report."

54. Whitfield Diffie and Susan Eva Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, *Updated and Expanded Edition* (Cambridge, MA: MIT Press, 2010), 236.

55. Steven Levy, "Battle of the Clipper Chip," *The New York Times*, June 11, 1994, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-Chip.html?pagewanted=all (accessed June 15, 2015).

56. *Ibid*.

57. Department of Commerce's National Institute of Standards and Technology, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)," Federal Register Vol. 59, No. 27, February 9, 1994, available at https://epic.org/crypto/clipper/fips_185_clipper_feb_94.html (accessed June 15, 2015).

58. Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip* (New Haven, CT: Yale University Press, 1997), 40.

59. Diffie and Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, 237.

60. Froomkin, "It Came from Planet Clipper: The Battle Over Cryptographic Key Escrow." ("If the government could not prevent the public from using nonconforming products, perhaps it could set the standard by purchasing and deploying large numbers of escrowed products. People who wanted to interoperate with the government's machines would naturally buy the same equipment. The existence of a large functioning user base would create further incentives for others to buy the same equipment.")

61. Levy, "Battle of the Clipper Chip."

62. NIST, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)."

63. Shari Steele and Daniel J. Weitzner, "Chipping Away at Privacy," *BBS Magazine*, September 1993, available at https://w2.eff.org/Privacy/Key_escrow/Clipper/clipper.summary (accessed June 15, 2015).

64. Diffie and Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, 236.

65. "Testimony of Whitfield Diffie, The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology," May 11, 1993, available at http://cpsr.org/prevsite/program/clipper/diffie-testimony.html/ (accessed June 15, 2015).

66. The Computer System Security and Privacy Advisory Board (now known as the Information Security and Privacy Advisory Board) is a government review panel that identifies emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy, advises the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, and reports its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency and the appropriate committees of the Congress. For more information about ISPAB, see http://csrc.nist.gov/groups/SMA/ispab/index.html (accessed June 15, 2015).

67. John Markoff, "Computer Code Plan Challenged," *The New York Times*, May 29, 1993, http://www.nytimes.com/1993/05/29/business/company-news-computer-code-plan-challenged.html (accessed June 15, 2015).

68. "The most important means to the defense of privacy is encryption. To encrypt is to indicate the desire for privacy. But to encrypt with weak cryptography is to indicate not too much desire for privacy. Cypherpunks hope that all people desiring privacy will learn how best to defend it. Cypherpunks are therefore devoted to cryptography. Cypherpunks wish to learn about it, to teach it, to implement it, and to make more of it. Cypherpunks know that cryptographic protocols make social structures. Cypherpunk know how to attack a system and how to defend it. Cypherpunks know just how hard it is to make good cryptosystems." Eric Hughes, "Welcome to the Cypherpunks Email," *Cyphernomicon*, September 10, 1994, available at http://www.cypherpunks.to/faq/cyphernomicron/chapter4.html (accessed June 15, 2015).

69. John Markoff, "Big Brother and the Computer Age," *The New York Times*, May 6, 1993, http://www.nytimes.com/1993/05/06/business/big-brother-and-the-computer-age.html (accessed June 15, 2015).

70. Andy Greenberg, *This Machine Kills Secrets* (New York: Penguin Group, 2012), 85.

71. *Ibid*, 85.

72. *Ibid*, 81-85.

73. In its initial analysis of the Clipper Proposal, for example, EFF laid out three serious concerns, largely related to how quickly the government was moving forward with an untested proposal that might have serious security vulnerabilities. "Initial EFF Analysis of Clinton Privacy and Security Proposal," *Electronic Frontier Foundation*, April 16, 1993, https://w2.eff.org/Privacy/Newin/Cypherpunks/930416.eff.initial.analysis (accessed June 15, 2015).

74. "Electronic Petition to Oppose Clipper," *Computer Professionals for Social Responsibility*, January 24, 1994, available at https://www.epic.org/crypto/clipper/cpsr_electronic_petition.html (accessed June 15, 2015).

75. For an in-depth discussion of the online organizing efforts and coordinated protest efforts that stopped the Stop Online Piracy Act (SOPA) and PROTECT IP Act (PIPA) in 2012, *see* Marvin Ammori, *On Internet Freedom* (Elkat Books: January 15, 2013).

76. Gurak, *Persuasion and Privacy in Cyberspace*, 34.

77. About CPSR," *Computer Professionals for Social Responsibility*, http://cpsr.org/about/ (accessed June 15, 2015).

78. "Letter to the President," *Computer Professionals for Social Responsibility*, January 24, 1994, available at http://cpsr.org/prevsite/program/clipper/cpsr-clipper-letter.html/ (accessed June 15, 2015).

79. Ibid.

80. "A Letter from the Digital Privacy and Security Working Group to President Clinton," May 7, 1993, available at https://www.eff.org/effector/5/8 (accessed June 15, 2015).

81. Levy, *Crypto*, 254, 264-268, 304; Markoff, "Big Brother and the Computer Age" (quoting Ed Markey, "There are many ways the N.S.A. is trying to put the cryptography genie back in the bottle, but it's already available for everyone openly.").

82. "Statement Of Senator Patrick J. Leahy, Chairman, Technology And The Law Subcommittee Hearing On The Administration's Clipper Chip Key Escrow Encryption Program," May 3, 1994, available at https://w2.eff.org/Privacy/Key_escrow/Clipper/leahy_clipper_050394.testimony (accessed June 15, 2015).

83. "Telecommunications Carrier Assistance to the Government," 103rd Congress 2nd Session, Report 103-827, October 4, 1994, available at https://epic.org/privacy/wiretap/calea/H_Rpt_103_827.txt (accessed June 15, 2015). *Also see* Christopher Soghoian, "CALEA and encryption," *Slight Paranoia*, September 28, 2010, http://paranoia.dubfire.net/2010/09/calea-and-encryption.html (accessed June 15, 2015).

84. NIST, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)."

85. Philip Elmer-Dewitt, "Who Should Keep the Keys?" *TIME Magazine*, March 14, 1994, http://content.time.com/time/magazine/article/0,9171,164002,00.html (accessed June 15, 2015). ("In a Time/CNN poll of 1,000 Americans conducted last week by Yankelovich Partners, two-thirds said it was more important to protect the privacy of phone calls than to preserve the ability of police to conduct wiretaps. When informed about the Clipper Chip, 80% said they opposed it.")

86. Stewart A. Baker, "Don't Worry Be Happy: Why Clipper Is Good For You," *Wired*, May 1994, available at http://groups.csail.mit.edu/mac/classes/6.805/articles/baker-clipper.txt (accessed June 15, 2015).

87. Dorothy Denning debated John Perry Barlow, a cofounder of the EFF, on America Online. Levy, "Clipper Chick."

88. Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard," *AT&T Bell Laboratories*, 1994, http://www.crypto.com/papers/eesproto.pdf (accessed June 15, 2015).

89. John Markoff, "Flaw Discovered in Federal Plan for Wiretapping," *The New York Times*, June 2, 1994, http://www.nytimes.com/1994/06/02/us/flaw-discovered-in-federal-plan-for-wiretapping.html (accessed June 15, 2015).

90. Sharon Begley, "Foiling the Clipper Chip," *Newsweek*, June 12, 1994, http://www.newsweek.com/foiling-clipper-Chip-188912 (accessed June 15, 2015).

91. Markoff, "Flaw Discovered in Federal Plan for Wiretapping."

92. Ibid.

93. Jared Sandberg and Don Clark, "AT&T, VLSI Technology to Develop Microchips That Offer Data Security," *The Wall Street Journal*, January 31, 1995.

94. "Testimony of Philip R. Zimmermann," before the Subcommittee on Science, Technology, and Space of the U.S. Senate Committee on Commerce, Science, and Transportation, June 29, 1996, available at https://www.philzimmermann.com/EN/testimony/index.html (accessed June 15, 2015).

95. In a letter to Representative Maria Cantwell in July 1994, Vice President Al Gore referred repeatedly to "future escrow systems"

and efforts with industry and academia to design and create such systems. "Letter from Vice President Al Gore to the Honorable Maria Cantwell," July 20, 1994, available at https://epic.org/crypto/key_escrow/Gore_letter_1994.html (accessed June 15, 2015).

96. Froomkin, "It Came from Planet Clipper: The Battle Over Cryptographic Key Escrow."

97. "By the summer of 1996, 'key escrow' had amassed so much criticism that proponents of the idea started using the term "key recovery" to mean essentially the same thing. There have been several attempts to explain the difference, usually by companies that have developed key escrow schemes. The explanation usually boils down to 'Key escrow was that old unacceptable idea, but this particular feature of our product includes makes it recovery rather than escrow.'" Notes from Ethics and the Law on the Electronic Frontier (2005), "1995-1997: From Clipper to Key Recovery," *MIT Open Courseware*, http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-805-ethics-and-the-law-on-the-electronic-frontier-fall-2005/readings/encrypt_4/ (accessed June 15, 2015).

98. Froomkin, "It Came from Planet Clipper: The Battle Over Cryptographic Key Escrow." For comparison, it's worth noting that Skipjack had an 80-bit key length. See notes 45 and 184 for an explanation of the significance of key length.

99. Froomkin, *Ibid.*

100. Giampiero Giacomello, *National Governments and Control of the Internet: A Digital Challenge* (New York: Routledge, 2005), 44.

101. For a good description of the opposition to the Clipper II and Clipper III proposals, see Notes from Ethics and the Law on the Electronic Frontier, "1995-1997: From Clipper to Key Recovery."

102. Giacomello, *National Governments and Control of the Internet,* 44.

103. Diffie and Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, 246-247.

104. "Open Letter to the Internet Community from Senator Conrad Burns," May 2, 1996, available at https://www.epic.org/crypto/legislation/burns_letter.html (accessed June 15, 2015).

105. "Pro-CODE Encryption Legislation," *The Electronic Privacy Information Center*, n.d., https://epic.org/crypto/legislation/pro_code.html (accessed June 15, 2015).

106. Original text of S.1726, "Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996," introduced July 27, 1996, available at https://www.congress.gov/bill/104th-congress/senate-bill/1726 (accessed June 15, 2015).

107. "Keep Big Brother's Hands off the Internet," Remarks of Senator John Ashcroft as Chairman of the Senate Commerce Subcommittee on Consumer Affairs, Foreign Commerce and Tourism, 1997, available at http://rense.com/general31/keepbigbrothershands.htm (accessed June 15, 2015).

108. Kenneth W. Dam and Herbert S. Lin, eds., "Cryptography's Role in Securing the Information Society," National Research Council's Committee to Study National Cryptography Policy, May 30, 1996, at 7, available at http://www.nap.edu/catalog/5131.html (accessed June 15,

2015). The National Research Council members were drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

109. *Ibid*, 4.

110. The final recommendation said that "governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade," and warned against governments initiating "legislation which limits user choice." "Recommendation of the Council Concerning Guidelines for Cryptography Policy," (*Organisation for Economic Co-operation and Development*), C(97)62/FINAL, March 27, 1997, available at http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=115&InstrumentPID=111&Lang=en&Book= (accessed June 15, 2015).

111. "Towards a European Framework for Digital Signatures and Encryption," *European Commission*, October 8, 1997, available at http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/eu-october-8-97.html (accessed June 15, 2015).

112. Edmund Andrews, "Europeans Reject U.S. Plan on Electronic Cryptography," *The New York Times*, October 9, 1997, http://partners.nytimes.com/library/cyber/week/100997encrypt-side.html (accessed June 15, 2015).

113. Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption."

114. *Ibid*.

115. *Ibid*.

116. The book "details how programmers and electronic communications professionals can use cryptography — the technique of enciphering and deciphering messages — to maintain the privacy of computer data. It describes dozens of cryptography algorithms, gives practical advice on how to implement them in cryptographic software, and shows how they can be used to solve security problems." Among other things, it includes actual source code for a number of encryption algorithms. "Applied Cryptography," *Schneier*

on Security, available at https://www.schneier.com/books/applied_cryptography/ (accessed June 15, 2015).

117. Karn's action was likely motivated by a desire to challenge the export controls on encryption software. Other early acts of resistance included a decision in 1994 by MIT to publish PGP source code and run a key server on the Internet, which could well have been interpreted as a violation of export controls because the software was made available to anyone in the world. See "MIT PGP Announcement," available at http://town.hall.org/cyber94/pgp.html (accessed June 15, 2015).

118. Keith Aoki, "Privacy and Encryption Export Controls: A Crypto Trilogy (Bernstein, Junger & Karn)," *University of Oregon School of Law*, August 24, 2000, available at http://www.cyberspacelaw.org/aoki/ (accessed June 15, 2015).

119. *Ibid*.

120. Levy, *Crypto*, 197-8, 287-8. Zimmermann was investigated by the Justice Department for three years relating to possible export control violations because PGP had been posted online. In 1996, the Justice Department announced it would not seek an indictment due to insufficient evidence. Ira S. Rubenstein and Michael Hintze, "Export Controls on Encryption Software," *Coping with U.S. Export Controls 2000*, Practising Law Institute, Commercial Law and Practice Course Handbook Series (December 2000) available at http://encryption_policies.tripod.com/us/rubinstein_1200_software.htm (accessed June 15, 2015), § 2(e) PGP. *Also see* Ronald J. Stay, "Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann," *Georgia State University Law Review*, Vol. 13: Issue 2, Article 14, available at http://readingroom.law.gsu.edu/gsulr/vol13/iss2/14/ (accessed June 15, 2015).

121. Category XIII, Auxiliary Military Equipment, for example, includes "Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems." 22 CFR Section 121 XIII(b)(1).

122. The length of the key is central to determining its level of security. Adding one "bit," or digit, to the key doubles the number of distinct values the key could potentially hold, and thereby also doubles the amount of time a hypothetical attacker would need to guess the actual value of the key. A two-bit key can hold four possible values, a three-bit key can hold eight, and so on.

123. A 40-bit symmetric encryption key can hold approximately 1.1 trillion values. Although the exact time required to guess a key depends on how much computing power is available, in the mid-1990s, a 40-bit key could be guessed in eight to ten days, according to experiments performed by graduate students at MIT and UC Berkeley. Today, a 40-bit key could be cracked in a matter of hours (or even minutes).

124. "Under the current ITAR regime, applications to export cryptographic software designed to encrypt messages with keys stronger than forty bits are generally denied, although authentication products that cannot be adapted for encryption, or which are designed for specific favored applications such as banking, tend to receive official export clearance. Applications to export DES, which uses fifty-six-bit encryption, are also often denied. Applications for stronger products are considered to have little chance of approval." Froomkin, "It Came From Planet Clipper: The Battle Over Cryptographic Key Escrow."

125. As Vice Admiral Bobby Ray Inman, who served as director of the NSA from 1977 to 1981, explained, "We were worried that foreign countries would pick up and use cryptography that would make it exceedingly hard to decrypt and read their traffic." Quoted in Corrigan-Gibbs, "Keeping Secrets."

126. Levy, "Battle of the Clipper Chip."

127. "Decoding the Encryption Debate," *Electronic Frontier Foundation*, 1997, https://www.eff.org/effector/10/10 (accessed June 15, 2015).

128. "Cryptography and Liberty 1999: An International Survey of Encryption Policy," *Electronic Privacy Information Center*, 1999, available at http://gilc.org/crypto/crypto-survey-99.html (accessed June 15, 2015). ("Internationally, export controls are the strongest tool used by governments to limit development of encryption products. Export controls reduce the availability of encryption in common programs such as operating systems, electronic mail and word processors, especially from American companies. The restrictions make it difficult to develop international standards for encryption and interoperability of different programs. Countries must develop their own local programs, which do not inter-operate well (if at all) with other programs developed independently in other countries. They may not be as secure because of a lack of peer-review. Because markets are smaller, companies and individuals are not as interested in developing programs because of smaller potential profits.")

129. Froomkin, "It Came from Planet Clipper: The Battle Over Cryptographic Key Escrow." Recent incidents have demonstrated the dangerous vulnerabilities that can be created as a result, which we will discuss in greater depth in the final section of this report.

130. Jeanne J. Grimmett, "Encryption Export Controls," *Congressional Research Services*, updated January 11, 2001, at CRS-3, available at http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30273_01112001.pdf (accessed June 15, 2015). ("With the growth of the global economy, the business community has

continued to express a need for strong encryption for domestic use and cross-border communications and transactions. While there are no statutory restrictions on the domestic use of encryption, the computer industry argues that restrictive export controls have hampered U.S. technological development since it is impracticable to develop separate products for the domestic and foreign market.")

131. U.S. Department of Commerce & National Security Agency, "A Study of the International Market for Computer Software With Encryption" at V-5 (1996), available at https://www.bis.doc.gov/index.php/formsdocuments/doc_view/24-a-study-of-the-international-market-for-computer-software-with-encryption-nsa-1995 (accessed June 15, 2015).

132. Erik R. Olbeter and Christopher Hamilton, "Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy," *Economic Strategy Institute*, April 1998, available at http://members.tripod.com/encryption_policies/us/olbeter_0498_key.htm (accessed June 15, 2015).

133. Jeri Clausing, "Study Puts Price on Encryption Controls," *The New York Times*, April 1, 1998, http://partners.nytimes.com/library/tech/98/04/cyber/articles/01encrypt.html (accessed June 15, 2015). The full study, "Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy," detailed four primary types of impact on the U.S. economy as a result of the restrictions: lost encryption product sales, slower growth in encryption-dependent industries, foregone cost savings and efficiency gains from the use of the Internet and networked technologies, and indirect spillover effects into broader American industries. Erik R. Olbeter and Christopher Hamilton, "Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy," *Economic Strategy Institute*, April 1998, available at http://members.tripod.com/encryption_policies/us/olbeter_0498_key.htm (accessed June 15, 2015).

134. Shari Steele and Daniel J. Weitzner, "A Government Computer Encryption System Would Threaten Civil Liberties," in *The Information Highway*, Ed. Charles P. Cozic (San Diego: Greenhaven Press, 1996) at 191-194, available at http://www.dikseo.teimes.gr/spoudastirio/E-NOTES/I/Information_Highway_The_Viewpoints.pdf (accessed June 15, 2015).

135. Bernstein v. United States Dept. of Justice, 176 F.3d 1132 (9th Cir. 1999).

136. Karn v. U.S. Dept. of State, 925 F.Supp 1 (D.D.C. 1996).

137. In *Junger v. Daley*, Case Western Law Professor Peter Junger found himself at odds with the Commerce over whether he was allowed to post some of his work related to computers and regulation to the World Wide Web. Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

138. There are numerous academic articles about the free speech implications of these three cases, but for a concise summary of how they were resolved, see Grimmett, "Encryption Export Controls," CRS-3. ("Federal district courts addressing this issue over the last three years have both upheld and dismissed First Amendment challenges to export licensing schemes for encryption.")

139. Quoted in Rubinstein and Hintze, "Export Controls on Encryption Software," § 4(a) The Karn and Bernstein Cases.

140. "Testimony of Alan B. Davidson, Staff Counsel, Center for Democracy and Technology," before the House Commitee on International Relations Subcommittee on International Economic Policy and Trade, May 18, 1999, available at https://www.cdt.org/files/testimony/990518davidson.shtml?page=15&issue=75 (accessed June 15, 2015) ("Davidson Encryption Testimony"). ("By limiting the spread of U.S. encryption outside the U.S., they make it harder for people in the U.S. to communicate securely with colleagues, business partners, family members, and others abroad. By "dumbing down" the security standards being built into the common products, they slow the use of encryption by law-abiding citizens in the U.S. By limiting the technical means of protecting information online, they leave our privacy unprotected in a world where Fourth Amendment protections stop at the border and information is not legally protected worldwide.")

141. In August 1995, several European researchers demonstrated that they could break the 40-bit encryption algorithm used in Netscape's SSL ("the only encryption algorithm generally approved for export from the U.S., and claimed by the Administration to be adequate for commercial applications") in eight days. In 1997, a grad student at UC Berkeley used a network of computers to crack a 40-bit key in under four hours. Notes from Ethics and the Law on the Electronic Frontier, "1995-1997: From Clipper to Key Recovery"; "Exportable Cryptography Totally Insecure: Challenge Cipher Broken Immediately," UC Berkeley, January 28, 1997, available at http://www.isaac.cs.berkeley.edu/isaac/press-release (accessed June 15, 2015).

142. Ronald L. Rivest, "The Case Against Regulating Encryption Technology," *Scientific American*, October 1998, available at http://people.csail.mit.edu/rivest/pubs/Riv98e.pdf (accessed June 15, 2015).

143. Lance J. Hoffman et al., "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations," *Cyberspace Policy Institute at the George Washington School of Engineering and Applied Science*, June 10, 1999, available at http://cryptome.org/cpi-survey.htm (accessed June 15, 2015). *See also* "Statement of Lance J. Hoffman, Professor, The George Washington University," before the U.S. Senate Committee on Commerce, Science, and Transportation, June 10, 1999, available at http://www.seas.gwu.edu/~lanceh/senate_testimony_pdf.pdf.

144. Hoffman et al., "Growing Development of Foreign

Encryption Products in the Face of U.S. Export Regulations." ("On average, the quality of foreign and U.S. products is comparable. There are a number of very good foreign encryption products that are quite competitive in strength, standards compliance, and functionality.")

145. Davidson Encryption Testimony.

146. Zimmermann, "Why I wrote PGP."

147. "Statement of Vice President Al Gore," *The White House*, October 1, 1996, available at https://epic.org/crypto/key_escrow/clipper4_statement.html (accessed June 15, 2015).

148. For an explanation of the National Research Council's findings, see footnote 108 above.

149. Full text of Executive Order 13026, "Administration of Export Controls on Encryption Products" (November 15, 1996), is available at http://www.gpo.gov/fdsys/pkg/FR-1996-11-19/pdf/96-29692.pdf (accessed June 15, 2015).

150. L. Jean Camp and Ken Lewis, "Code as Speech: a Discussion of Bernstein vs. USDOJ, Karn v. USDOS, and Junger v. Daley in light of the U.S. Supreme Court's recent shift to Federalism," *Ethics and Information Technology*, March 2001, Vol. 1, No. 2. *Also see* Rubenstein and Hintze, "Export Controls on Encryption Software."

151. "Statement of Rep. Bob Goodlatte (R-VA) on re-introduction of the Security and Freedom Through Encryption (SAFE) Act," *The Library of Congress*, February 25, 1999, available at http://www.techlawjournal.com/cong106/encrypt/19990225bg.htm (accessed June 15, 2015).

152. Original text of H.R. 3011, the Security and Freedom Through Encryption (SAFE) Act in the 104th Congress, introduced March 5, 1996, available at https://www.congress.gov/bill/104th-congress/house-bill/3011text?q=%7B%22search%22%3A%5B%22Security+and+Freedom+through+Encryption+Act%22%5D%7D. (accessed June 15, 2015)

153. Specifically, the bill stated that "No person in lawful possession of a key to encrypted information may be required by Federal or State law to relinquish to another person control of that key." There was an exception, however, which stipulated that the key-escrow prohibition "shall not affect the authority of any investigative or law enforcement officer, acting under any law in effect on the effective date of this chapter, to gain access to encrypted information." H.R. 3011.

154. The SAFE Act amended the Export Administration Regulations to allow the export without a license of most generally available software and hardware containing encryption unless there was substantial evidence that it would be used for military purposes.

155. "Press Briefing by the Vice President, Deputy Chief of Staff John Podesta, Principal Associate Deputy Attorney General Robert Litt, Assistant Director of the FBI Carolyn Morris, Undersecretary of Commerce William Reinsch," *The White House*, September 16, 1998, available at http://fas.org/irp/offdocs/EncryptionWH.htm (accessed June 15, 2015).

156. By the late 1990s, even 56-bit encryption keys were demonstrated to be insecure. On the heels of the cracks of export-grade encryption, in 1998 the Electronic Frontier Foundation demonstrated that the supposed "gold standard" of domestic encryption algorithms was vulnerable to attack. For less than $250,000, EFF built the first unclassified hardware for cracking the DES algorithm. It took under three days to decode a message, which the government had previously claimed would take months and require multimillion-dollar networks of computers. "'EFF has proved what has been argued by scientists for twenty years, that DES can be cracked quickly and inexpensively,' said John Gilmore, EFF co-founder and project leader. 'Now that the public knows, it will not be fooled into buying products that promise real privacy but only deliver DES. This will prevent manufacturers from buckling under government pressure to 'dumb down' their products, since such products will no longer sell.' EFF Executive Director Barry Steinhardt added, 'If a small nonprofit can crack DES, your competitors can too. Five years from now some teenager may well build a DES Cracker as her high school science fair project.'" For more on how DES works, see note 45. "EFF DES Cracker Machine Brings Honesty To Crypto Debate," *Electronic Frontier Foundation*, July 17, 1998, https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html.

157. Courtney Macavinta, "White House eases crypto limits," *CNET News*, September 16, 1998, http://news.cnet.com/2100-1023-215577.html (accessed June 15, 2015).

158. The President's Export Council was first created in 1973 to advise the President on export enhancement and work with industry to encourage U.S. companies to increase exports and enter new markets.The Subcommittee on Encryption, established in 1979, was created to advise on future key recovery issues, including evaluating the developing global key architecture, assessing lessons learned from key recovery implementation, advising on technical confidence issues, addressing interoperability and standards issues, and identifying other technical, policy, and program issues for government action. U.S. Department of Commerce: International Trade Administration. "President's Export Council History," *U.S. Commerce Department's International Trade Division*, available at http://trade.gov/pec/history.asp.

159. "Liberalization 2000: Recommendations for Revising the Encryption Export Regulations," *President's Export Council Subcommittee on Encryption*, August 25 1999, available at http://cryptome.org/LIB42.htm (accessed June 15, 2015).

160. "Administration Announces New Approach to Encryption," *The White House*, September 16, 1999, available at https://epic.org/crypto/legislation/cesa/WH_release_9_16.html (accessed June 15, 2015).

161. "Update to Encryption Policy," *U.S. Commerce Department*, September 16, 1999, available at https://epic.org/crypto/export_controls/commerce_q&a_9_99.html (accessed June 15, 2015).

162. Jeri Clausing, "In a Reversal, White House Will End Data-Encryption Export Curbs," *The New York Times*, September 17, 1999, http://www.nytimes.com/1999/09/17/business/in-a-reversal-white-house-will-end-data-encryption-export-curbs.html (accessed June 15, 2015).

163. *Ibid*.

164. Levy, *Crypto*, 307.

165. "Revised U.S. Encryption Export Control Regulations," *U.S. Commerce Department*, January 2000, available at https://epic.org/crypto/export_controls/regs_1_00.html (accessed June 15, 2015).

166. 15 CFR § 740.13 "Technology and Software Unrestricted (TSU)" License Exception, which is described at https://www.bis.doc.gov/index.php/forms-documents/doc_view/986-740 (accessed June 15, 2015).

167. Clausing, "In a Reversal, White House Will End Data-Encryption Export Curbs." (Quoting Representative Goodlatte, "'I am surprised that they moved this much this quickly,' Mr. Goodlatte said. 'But we are very pleased that they have done so and that they have come this close. There is no doubt that this announcement is a direct result of the fact that we had 258 co-sponsors.'")

168. Rubinstein and Hintz, "Export Controls on Encryption Software."

169. Dam and Lin, eds., "Cryptography's Role in Securing the Information Society."

170. Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 4. ("Without a secure and trusted infrastructure, companies and individuals will become increasingly reluctant to move their private business or personal information online.")

171. For example, U.S. electronic commerce expanded from around $28 billion in the year 2000 to $143 billion in 2009. D. Steven White, "U.S. E-Commerce Growth 2000-2009," available at http://dstevenwhite.com/2010/08/20/u-s-e-commerce-growth-2000-2009/ (accessed June 15, 2015). These statistics were drawn from "E-Stats - Measuring the Electronic Economy," *United States Census Bureau*, May 22, 2014, http://www.census.gov/econ/estats/index.html (accessed June 15, 2015).

172. Holly Lynne McKinley, "SSL and TLS: A Beginners Guide," *The SANS Institute*, 2003, https://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029 (accessed June 15, 2015).

173. "What is SSL (Secure Sockets Layer) and What Are SSL Certificates?" *Digicert*, https://www.digicert.com/ssl.htm (accessed June 15, 2015).

174. "History of SSH (SSH, The Secure Shell: The Definitive Guide)," *University of Arkansas College of Engineering*, 2002, http://csce.uark.edu/~kal/info/private/ssh/ch01_05.htm (accessed June 15, 2015).

175. In 2010, Verisign sold its SSL certificate and related authentication businesses to Symantec.

176. For more information, *see* https://www.comodo.com/ (accessed June 15, 2015).

177. *See, e.g.*, EFF's "Encrypt the Web" Scorecard, which surveys the practices of 18 major Internet companies and providers, several categories related to support for and use of HTTPS. The latest version of the report is available at https://www.eff.org/encrypt-the-web-report (accessed June 15, 2015).

178. "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," *The White House*, December 12, 2013, at 216-217, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed June 15, 2015).

179. *Ibid*. 22.

180. Bob Goodlatte, "Let's Open Up Encryption," *The Washington Post*, June 12, 1997, http://www.washingtonpost.com/wp-srv/politics/special/encryption/stories/ocro61297.htm (accessed June 15, 2015). ("Just as dead-bolt locks and alarm systems help people protect their homes against intruders, thereby assisting law enforcement in preventing crime, strong encryption allows people to protect their digital communications and computer systems against criminal hackers and computer thieves.")

181. There is a growing epidemic of smartphone theft, with 3.1 million stolen in the U.S. in 2013, nearly double the number of smartphones stolen in 2012. The vast amount of personal information on those devices makes them especially attractive targets for criminals aiming to commit identity theft or other crimes of fraud. "Smart phone thefts rose to 3.1 million last year, Consumer Reports finds," *Consumer Reports*, May 28, 2014, http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm (accessed June 15, 2015). Many now argued that

encryption actually makes us all safer. *See, e.g.,* Nuala O'Connor, "Encryption Makes Us All Safer," *Center for Democracy & Technology*, October 8, 2014, https://cdt.org/blog/encryption-makes-us-all-safer/ (accessed June 15, 2015).

182. Dan Goodlin, "'FREAK' flaw in Android and Apple devices cripples HTTPS crypto protection," *Ars Technica*, March 3, 2015, http://arstechnica.com/security/2015/03/freak-flaw-in-android-and-apple-devices-cripples-https-crypto-protection/ (accessed June 15, 2015). The full report by Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cedric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre Yves-Strub, Santiago Zanella-Beguelin, Jean-Karim Zinzindohoue, and Benjamin Beurdouche is available at https://www.smacktls.com/#freak (accessed June 15, 2015). The vulnerability is officially catalogued as CVE-2015-0204, available at https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204 (accessed June 15, 2015).

183. There are two types of key lengths: those of symmetric keys and those of asymmetric keys (for cryptosystems where separate keys are used to encrypt and decrypt), and direct comparison of their key lengths is meaningless. Prior to 2000 there were limits on the length of both types of keys, making the encryption weaker and easier to break. The 40-bit, 56-bit, and 128-bit keys discussed earlier in the paper were all used in symmetric encryption algorithms, like DES and AES. Government controls initially limited the export of keys above 40-bits, then above 56-bits, while keys used today for strong symmetric encryption are 128-bits, 192-bits, or 256-bits long. Asymmetric encryption requires much longer key lengths, such as the vulnerable 512-bit RSA keys threatened by the FREAK attack. As a comparison, strong RSA keys used today are either 2048 bits or 4096 bits long. Because the security of a key of either type increases exponentially as it get longer, the difference between the time necessary to brute force a 40-bit key and a 256-bit key, or between a 512-bit RSA key and a 4096-bit RSA key, is the difference between a few hours and many times the length of the history of the universe. Arjen K. Lenstra, "Key Lengths," in *Handbook of Information Security*, ed. Hossein Bidgoli (Hoboken, NJ: Wiley, 2006), available at http://infoscience.epfl.ch/record/164539/files/NPDF-32.pdf.

184. For a good technical explanation of how a FREAK Attack works, *see* Matthew Green, "Attack of the week: FREAK (or 'factoring the NSA for fun and profit')," *A Few Thoughts on Cryptographic Engineering*, March 3, 2015, http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html. (accessed June 15, 2015).

185. Craig Timberg, "'FREAK' flaw undermines security for Apple and Google users, researchers discover," *The Washington Post*, March 3, 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/03/freak-flaw-undermines-security-for-apple-and-google-users-researchers-discover/. (accessed June 15, 2015).

186. Dan Goodin, "HTTPS-crippling attack threatens tens of thousands of Web and mail servers," *Ars Technica*, May 20, 2015, http://arstechnica.com/security/2015/05/https-crippling-attack-threatens-tens-of-thousands-of-web-and-mail-servers/, (accessed June 15, 2015). *Also see* "The Logjam attack, available at https://weakdh.org/, (accessed June 15, 2015).

187. "ACLU Submission to the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression and Opinion," *American Civil Liberties Union*, February 10, 2015, https://www.aclu.org/sites/default/files/assets/aclu_submission_to_special_rapporteur_-_encryption_and_anonymity.pdf. (accessed June 15, 2015).

188. Hillary Clinton gave two major addresses on Internet Freedom during her tenure as Secretary of State, becoming the first global leader to emphasize Internet Freedom as a foreign policy priority and urging "countries everywhere… to join us in the bet we have made, a bet that an open Internet will lead to stronger, more prosperous countries." Hillary Clinton, "Internet Rights and Wrongs: Choices and Challenges in a Networked World," *U.S. Department of State*, February 15, 2011, *available at* http://blogs.state.gov/stories/2011/02/15/Internet-rights-and-wrongs-choices-and-challenges-networked-world. (accessed June 15, 2015). *Also see* the U.S. State Department's Internet Freedom page, available at http://www.humanrights.gov/issues/Internet-freedom/. (accessed June 15, 2015).

189. Scott Busby, "10 Things You Need to Know About U.S. Support for Internet Freedom," *IIP Digital*, May 29, 2014, http://iipdigital.usembassy.gov/st/english/article/2014/05/20140530300596.html#axzz32vEtH3C9. (accessed June 15, 2015).

190. "Report of the Special Rapporteur on promotion and protection of the right to freedom of expression and opinion, David Kaye," A/HRC/29/32, May 22, 2015, available at http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

191. A 2013 study of the experiences of 1,175 Chinese Internet users circumventing their country's Internet censorship found that the "circumvention tools that work best for these users are technologically diverse, but they are united by a shared political feature: the collateral cost of choosing to block them is prohibitive for China's censors. Our survey respondents are relying not on tools that the Great Firewall can't block, but rather on tools that the Chinese government does not want the Firewall to block. Internet freedom for these users is collateral freedom, built on technologies and platforms that the regime finds economically or politically indispensable." David Robinson et al., "Collateral Freedom: A Snapshot of Chinese Internet Users Circumventing Censorship," *Open Internet Tools Project*, April 2013, https://openitp.org/pdfs/CollateralFreedom.pdf (accessed June 15, 2015).

192. For more information, see "Advisory Committee to the

Congressional Internet Caucus," available at http://www.netcaucus.org/ (accessed June 15, 2015).

193. "Americans for Computer Privacy (ACP) is a broad-based coalition that brings together more than 100 companies and 40 associations representing financial services, manufacturing, telecommunications, high-tech and transportation, as well as law enforcement, civil-liberty, pro-family and taxpayer groups. ACP supports policies that advance the rights of American citizens to encode information without fear of government intrusion, and advocates the lifting of export restrictions on U.S.-made encryption products." "Who We Are," *Americans for Computer Privacy,* available at http://www.computerprivacy.org/who/index.html (accessed June 15, 2015).

194. *See, e.g.*, Craig Aaron, "How We Won Net Neutrality," *The Huffington Post*, February 26, 2015, http://www.huffingtonpost.com/craig-aaron/how-we-won-net-neutrality_b_6759132.html (accessed June 15, 2015).

195. *See, e.g.*, "Statement of Kevin S. Bankston, Policy Director of New America's Open Technology Institute and Co-Director of New America's Cybersecurity Initiative, at the Hearing on Encryption Technology and U.S. Policy Responses," before the U.S. House of Representatives Subcommittee on Information Technology of the Committee on Oversight and Government Reform, April 29, 2015, available at https://static.newamerica.org/attachments/2982-at-crypto-hearing-best-arguments-against-backdoor-mandates-come-from-members-of-congress-themselves/Bankston_Written_Testimony.5876d326c5fc4e0cbd17b59e8d53384f.pdf. (accessed June 15, 2015).