Comments to the UN Special Rapporteur on Freedom of Expression and Opinion Regarding the Relationship Between Free Expression and the Use of Encryption

By Danielle Kehl, Kevin Bankston, and Andi Wilson
February 10, 2015

Introduction and Summary

New America's Open Technology Institute welcomes the opportunity to provide input to David Kaye, the United Nations Special Rapporteur on the protection and promotion of the right to freedom of expression and opinion, as he prepares his report "on the legal framework governing the relationship between freedom of expression and the use of encryption to secure transactions and communications, and other technologies to transact and communicate anonymously online," including his request for "information on national laws, regulations, policies or practices that permit or limit, directly or indirectly, the use of encryption technologies."[1]

New America is a nonprofit, nonpartisan public policy institute based in Washington DC that invests in new thinkers and new ideas to address the next generation of challenges facing the United States and the global community. The Open Technology Institute (OTI) is a program within New America which promotes affordable, universal access to open and unrestricted communications networks through technology development, applied learning, and policy reform. OTI offers in-depth, objective research, analysis, and findings for policy decision-makers and the general public, develops technologies and tools to support universal and secure communications, and works directly with communities to address communications and technological disparities. A significant portion of OTI's portfolio focuses on cybersecurity, surveillance reform, and research and analysis of public policies that impact individual privacy and free expression online.

These comments focus on the debate about encryption technology in the United States over the past few decades. Based on the arguments made during the Crypto Wars of the 1990s, we describe the establishment of legal and practical norms in the U.S. premised on the conclusion that strong encryption benefits Internet security, economic growth, individual privacy, and free expression. We discuss how innovations in applied cryptography after the end of the Crypto Wars laid the foundation for the unprecedented growth of the Internet economy, which in turn brought the human rights benefits of encryption to the forefront of U.S. foreign policy efforts related to Internet freedom. Finally, we explain how the post-Snowden debate about encryption has evolved, describing new threats to established norms regarding the value of encryption. These comments are divided into three main parts.

[1] "Call for Submission of Information: Special Rapporteur will study the use of encryption and anonymity in digital communications in his 2015 HRC report," *United Nations Human Rights Council*, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

I. The History of the Crypto Wars. The first section of these comments traces the history of the "Crypto Wars" in the 1990s, a period when policymakers and advocates debated the tradeoffs related to the proliferation of encryption technology both in the United States and overseas, and ultimately concluded that the positive benefits of encryption outweighed any potential negatives. In particular, we describe the specific arguments about why encryption is good for Internet security, individual privacy, free expression, and economic growth:

- ***Strong encryption is necessary for Internet security.*** Strong encryption both protects individuals' private communications and improves the overall security of the networks that store and transmit information. Attempts to address the spread of encryption by mandating that companies build surveillance backdoors into their products and imposing strict export controls on products containing cryptography ultimately weakens the security of those products and slows the overall growth of a more secure Internet.

- ***Strong encryption protects individual privacy, and surveillance backdoors threaten it.*** Cryptography tools allow individuals to protect the privacy and safety of their data online. During the Crypto Wars, a wide range of technical experts, grassroots organizations, and prominent politicians united behind the value of access to strong encryption free of surveillance backdoors for the government. They argued that the U.S. government should encourage rather than stifle the use of strong encryption to preserve civil liberties and the fundamental right to privacy in the face of rapid technological change.

- ***Strong encryption enables free expression.*** The security and privacy protections afforded by the use of strong encryption also help promote free expression. Surveillance has a chilling effect on free speech and the free flow of information online, whereas the expansion of a secure Internet contributes positively to free expression. Moreover, attempts to restrict the export of encryption code to foreign countries raise their own free expression concerns.

- ***Strong encryption is necessary for the growth of the Internet and the information economy.*** Strong encryption increases users' confidence in the security of their online communications and transactions, which is a critical step toward enabling the growth of the information economy and the migration of sensitive communications online. Conversely, undermining or deliberately weakening encryption can have a detrimental effect on economic growth and the global competitiveness of technology companies, adding both direct and indirect costs and hampering their ability to sell products overseas.

II. After the Crypto Wars: Encryption, the Internet Economy, and Human Rights. Encryption played a role in the unprecedented growth of the Internet economy in the early 21st century by ensuring that users could securely communicate and conduct transactions online. This growth also made it possible for the Internet to emerge as an important platform for the exercise of human rights, which is why support for technologies that rely on encryption have become a

key component of the U.S. foreign policy initiative to protect and promote online free expression and the free flow of information globally.

III. Encryption Under Threat. Finally, we describe how the long-established norms promoting the use and spread of encryption technology have recently come under threat, especially following the 2013 Snowden disclosures. We describe the strong negative reaction to the revelations that the National Security Agency has carried on its own secret war against encryption technology over the past two decades, which accelerated the adoption of encryption by default into popular technology products in 2014 — and the subsequent backlash against encryption from law enforcement and intelligence officials who have once again revived the arguments they made in the 1990s.

We conclude by respectfully recommending that the Special Rapporteur reiterate the important role that encryption plays in protecting fundamental values like free speech and privacy in the digital age. The arguments that won the original Crypto Wars still hold true today, while the intervening years have also demonstrated that encryption is a critical tool for the exercise of human rights online. We urge the Special Rapporteur to send a clear message to lawmakers both in the United States and around the world that the widespread availability and use of strong encryption without surveillance backdoors can and still should be the practical and legal norm in the modern era.

I. The History of the Crypto Wars

The "Crypto Wars" of the 1990s was a historic conflict between the proponents of strong encryption and U.S. government actors who sought to limit its proliferation. The conflict has its roots in 1976, when two researchers first published their work on split-key encryption, making it possible for both individuals and corporations to access strong encryption technology that had previously been the exclusive purview of military and government agencies.[2] Many military and law enforcement officials perceived this shift as a threat to the government's ability to conduct criminal investigations and gather intelligence. They argued that if individual and commercial use of encryption became widespread, they might need to take action to ensure that the government retained its ability to access communications. By the 1990s, the U.S. government had advanced a variety of proposals aimed at limiting the spread of strong encryption both at home and abroad — sparking a heated debate between policymakers, privacy advocates, and industry representatives about the tradeoffs related to the widespread adoption and use of encryption technology.[3]

In April 1993, the Clinton Administration announced a new initiative intended to provide the public with strong cryptographic tools to secure their communications but without sacrificing the ability of law enforcement and intelligence agencies to access those communications.[4] They proposed a technical solution commonly known as the "Clipper Chip," a computer chip that could be inserted into consumer hardware such as cell phones.[5] 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.[6] Under the right conditions (i.e. when a court-approved warrant or wiretap order had been obtained) the two federal agencies jointly responsible for holding the keys would release them to law enforcement, providing access to unencrypted copies of the encrypted conversations.[7] Although the standard was technically voluntary, the government committed to purchasing a massive number of devices containing the Clipper Chip, which

---

[2] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory,* Vol. IT-22, Nov. 6, November 1976. In this paper, Diffie and Hellman detailed how individuals could communicate securely with a new technology called "split-key encryption" (later called the Diffie-Hellman key exchange) which involved each participant creating related private and public keys that could be used to encrypt and decrypt plaintext conversations. Using split-key encryption, plaintext communications are converted into ciphertext before they are transmitted over the Internet, meaning that no one but the recipient (who holds the correct private key) can decrypt and read the communications.

[3] 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.

[4] "Statement by the Press Secretary," The White House, April 16, 1993, *available at* http://csrc.nist.gov/keyrecovery/clipper.txt.

[5] Steven Levy, *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age* (New York: Penguin Books, 2002), 226-230; "The chip is an important step in addressing the problem of encryption's dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists. 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" ("Statement by the Press Secretary," April 16, 1993).

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

[7] Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard," AT&T Bell Laboratories, 1994, http://www.crypto.com/papers/eesproto.pdf; Froomkin, "It Came From Planet Clipper: The Battle Over Cryptographic Key Escrow."

officials hoped would strongly influence the marketplace and result in its widespread adoption throughout the 1990s.[8] And some feared that the government might eventually make the standard mandatory by codifying the key-escrow requirement.[9]

In addition to debating the merits of implementing a domestic key-escrow system, the Crypto Wars had an international component that focused on whether American technologies containing strong encryption should be exported overseas.[10] Historically, products containing robust encryption had been categorized as a military export in the United States and subject to strict controls.[11] By limiting the ability of American companies to sell certain cryptographic products in foreign markets, the government sought to delay the spread and adoption of strong encryption technology, which they feared could reduce their ability to gather intelligence on foreign targets. Moreover, requiring U.S. companies to seek approval before exporting cryptographic technologies allowed the government to continue to monitor — and indirectly influence — the development of commercial cryptography.[12] The actual controls were based on the strength of the encryption (i.e. the cryptographic key length) and applied not only to hardware but also encryption software and source code.[13] Industry advocates and others in favor of relaxing the controls argued that they impeded technological development, threatening the long-term competitiveness of the U.S. technology industry and otherwise undermining national interests.[14]

Ultimately, the public battle over encryption technology in the 1990s concluded with a recognition that the positive benefits of encryption — protecting Internet security, fostering the growth of Internet economy, and promoting individual privacy and free expression — outweighed any potential negatives. Although the Clinton Administration officially endorsed the

---

[8] Levy, *Crypto*, 249.
[9] Levy, *Crypto*, 295.
[10] Froomkin, "It Came from Planet Clipper: The Battle Over Cryptographic Key Escrow."
[11] 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): "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." Products with strong encryption were categorized as "dual use" technologies, meaning that they had both civilian and military applications. Other dual-use export controls aim to prevent threats like the proliferation of nuclear technology, munitions, and weaponizable chemicals.
[12] "Cryptography's Role in Securing the Information Society," National Research Council Committee to Study National Cryptography Policy (1996). 114. *Available at* http://legalphysics.org/wp-content/uploads/2014/07/5131.pdf.
[13] In 1994, products with "strong encryption" were categorized as those with key lengths of more than 40 bits. 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. A 40-bit key can hold approximately 1.1 trillion values.
[14] 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. ("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; that export restrictions will hinder its long-term competitiveness, given the increasing availability of strong foreign cryptography and the projected increase in demand for such products due to the increasing popularity of electronic commerce; and that U.S. interests are harmed by making increasingly strong U.S. encryption unavailable to legitimate users worldwide.")

Clipper Chip as a Federal Information Processing Standard in February 1994,[15] it was not widely adopted the way officials had hoped. As privacy advocates, industry representatives, and a number of politicians became increasingly vocal in their opposition to the Clipper Chip, public opinion began to shift.[16] In May 1994, a computer scientist at AT&T's Bell Labs discovered a critical flaw in the technology that proved it could be tampered with by unauthorized individuals.[17] By 1996, it was clear that the Clipper Chip had become largely irrelevant.

Simultaneously, the arguments in favor of maintaining strict controls on the export of cryptography products were also losing ground. The Clinton Administration took its first step toward relaxing export controls for certain commercial encryption products in the fall of 1996.[18] As Vice President Al Gore explained, "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 US encryption product manufacturers during the transition to a key management infrastructure."[19] This marked the start of a broader trend of liberalizing export controls related to encryption which continued throughout the 1990s and 2000s.[20] One of the most important steps in this liberalization process was the creation of an exemption for the export of free and open source cryptography, which paved the way for the development of tools that specifically relied on encryption to promote free speech and anonymous communications.[21]

---

[15] Officially known as the Escrowed Encryption Standard (EES), the Clipper Chip endorsement was published in the Federal Register on February 9, 1994. Department of Commerce's National Institute of Standards and Technology, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)," *The Federal Register* Vol. 59, No. 27, February 9, 1994, *available at* https://epic.org/crypto/clipper/fips_185_clipper_feb_94.html.

[16] According to a CNN/Time poll taken in March 1994, eighty percent of Americans opposed the Clipper Chip. Philip Elmer-Dewitt, "Who Should Keep the Keys?" *TIME Magazine*, March 14, 1994. http://content.time.com/time/magazine/article/0,9171,980329,00.html.

[17] 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. *For a full explanation of these concerns, see* Blaze, "Protocol Failure in the Escrowed Encryption Standard."

[18] Executive Order 13026, issued on November 15, 1996, 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 on the Commerce Control List (CCL). *Full text of Executive Order 13026 is available at*: http://www.gpo.gov/fdsys/pkg/FR-1996-11-19/pdf/96-29692.pdf.

[19] "Statement of Vice President Al Gore," October 1, 1996, *available at* https://epic.org/crypto/key_escrow/clipper4_statement.html.

[20] *See, e.g.*, President's Export Council Subcommittee on Encryption, "Liberalization 2000: Recommendations for Revising the Encryption Export Regulations, August 25 1999, *available at*: http://cryptome.org/LIB42.htm; "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; "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.

[21] Before this change, computer scientist Phillip Zimmerman was investigated by the United States Justice Department for possible export violations because his cryptographic software program, Pretty Good Privacy (PGP), was distributed over the Internet. Liberalizing export controls made the distribution of PGP legal, because it met the criteria included in the free and open source exemption. 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

The growing consensus on the benefits of encryption and the detriments of surveillance backdoors that would undermine its effectiveness was even codified into law by the U.S. Congress. The 1994 Communications Assistance for Law Enforcement Act (CALEA), which required telecommunications carriers to have the technical capacity to comply with lawful wiretap demands, made clear that the law's mandate did not prevent telecommunications users from employing encryption nor require service providers to block or break such user-generated encryption.[22]

In the end, advocates of strong encryption won the debate by weaving together a number of important, interrelated arguments that articulated why encryption is good for Internet security, individual privacy, free expression, and the information economy. We explain these arguments in further detail below. While we describe them in the specific context of the U.S. Crypto Wars, it is important to note that they reflect generally applicable principles that are relevant to countries all over the world.

Strong Encryption is Necessary for Internet Security

Strong encryption improves the overall security of networks by protecting the data that is stored on or transmitted through those networks and is an essential ingredient to the overall security of the modern network.[23] By contrast, any attempt to address the spread of encryption technology by requiring tech companies to intentionally create a "backdoor"[24] comes with significant security concerns. Indeed, after the Clipper Chip was proposed, the Commerce Department's National Institute of Standards and Technology (NIST) implemented a public comment process on key escrow.[25] NIST received 320 comments in response, of which only two

[22] "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." Communications Assistance for Law Enforcement Act, 47 U.S.C. §§1001 et. seq. (1994), *available at* https://www.congress.gov/bill/103rd-congress/house-bill/4922?q=%7B%22search%22%3A%5B%22Communications+Assistance+for+Law+Enforcement+Act%22%5D%7D. 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." Telecommunications Carrier Assistance to the Government. *103rd Congress.* October 4, 1994. *Available at* https://epic.org/privacy/wiretap/calea/H_Rpt_103_827.txt

[23] "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." (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) For more information on why encryption is good for security, see "What is Encryption?" *Surveillance Self Defense: A Project of the Electronic Frontier Foundation*, last updated November 3, 2014, *available at* https://ssd.eff.org/en/module/what-encryption.

[24] A backdoor refers to a mechanism by which a third party (like the government) has the technical means to access private communications, such as by inserting a vulnerability into cryptographic algorithms, which could then be exploited, or by maintaining a copies of private keys, as the Clipper Chip would have done.

[25] Computer Security Resource Center. "Fact Sheet: Public Encryption Management." National Institute of Standards and Technology. April 16, 1993, http://csrc.nist.gov/keyrecovery/clipfact.txt

were positive.[26] Experts voiced broad concerns about the trustworthiness of the key-escrow system and the specific challenge of relying on the U.S. government as the keyholder, which would give federal agencies and law enforcement officials unprecedented access to and power over the private information of their citizens. The Clipper Chip technology itself also contained additional vulnerabilities, as technical analysis revealed that the encryption could be bypassed or exploited without the chip-unique key.[27]

Just as backdoor mandates threatened information security, so did export controls. Because export controls originally restricted the spread of encryption based on its strength, the practical result was that only American products containing weak encryption — or with its encryption technology removed entirely — were exported abroad. Because of the size of the American technology market, these limitations could have slowed the overall development and adoption of encryption technology worldwide. As Representative Bob Goodlatte explained when he introduced the Security and Freedom Through Encryption (SAFE) Act in February 1999,[28] governments should be encouraging the private sector to adopt robust security standards in their products, not making it more difficult. "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," he said.[29] The SAFE Act aimed to prevent the government from creating a mandatory key-escrow system and relax U.S. export controls around encryption. Although the bill was never voted on, it enjoyed widespread support including sponsorship from a majority of the members of the House of Representatives, reflecting a broad and bipartisan consensus on the importance of promoting and protecting access to strong encryption tools.[30]

---

[26] "The private sector and the public have expressed nearly unanimous opposition to Clipper. In the formal request for comments conducted by the Department of Commerce last year, less than a handful of respondents supported the plan. Several hundred opposed it." ("Letter from Computer Professionals for Social Responsibility," January 24, 1994, *available at* http://cpsr.org/prevsite/program/clipper/cpsr-clipper-letter.html/.)

[27] 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; Matt Blaze, 1994.

[28] The Security and Freedom Through Encryption Act (H.R. 850) originated in 1996 and was re-introduced to the 106th Congress in February 1999. The bill sought to ensure not only that individuals within the United States should be able to use strong encryption, but also that many of the more onerous restrictions on the export of encryption overseas would be lifted. Despite substantial support in Congress — including a majority of the members of the House as co-sponsors — the SAFE Act faced significant pushback from the Clinton Administration. Although an amended version that limited the scope of the bill was approved by various Congressional committees, no further action was taken. The Clinton Administration did separately take a number of steps later that year to liberalize encryption export controls. H.R. 850, Security and Freedom Through Encryption (SAFE) Act, 106th Cong. (1999), *available at* https://www.congress.gov/bill/106th-congress/house-bill/850?q=%7B%22search%22%3A%5B%22%5C%22Security+and+Freedom+Through+Encryption%5C%22+Act%22%5D%7. *For additional background and amendments to the SAFE Act, see* "Summary of Encryption Bills in the 106th Congress," Tech Law Journal, 1999, *available at* http://www.techlawjournal.com/cong106/encrypt/Default.htm.

[29] "Statement of Rep. Bob Goodlatte (R-VA) on 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.

[30] Levy, *Crypto*, 295, 305.

Strong Encryption Protects Individual Privacy, and Surveillance Backdoors Threaten It

In addition to protecting the overall security of the Internet, many of the early pioneers of open source and commercial cryptography recognized that encryption would be a vital tool to protect personal privacy online. They understood one of the great challenges of the information age: as more and more personal and sensitive information gets transmitted quickly and efficiently over our communications infrastructure, it becomes increasingly difficult to protect the security of that information on a large scale.[31] Cryptography represented one of the best ways for governments and commercial entities as well as individuals to protect the privacy and safety of their data.[32] When the ability to securely encrypt was threatened during the Clipper Chip debate, nascent organizations like the Electronic Frontier Foundation, the Electronic Privacy Information Center, and Center for Democracy and Technology rallied against the proposal, which they understood as a clear threat to the right to privacy online.[33] A group called the Computer Professionals for Social Responsibility[34] wrote letters to the Clinton Administration signed by prominent cryptography and computer security experts and gathered over 50,000 signatures by email in opposition to the Clipper Chip — one of the first online advocacy campaigns of its kind.[35]

Protecting privacy was not just a concern of grassroots organizations and technical experts, either. A number of prominent politicians came out against mandated backdoors like the Clipper Chip, which had a powerful impact on the public debate. Opponents of the Clipper Chip included Senators John Kerry, Patrick Leahy, and John Ashcroft, who later became Attorney General, and Representatives Maria Cantwell, and Sam Gejdenson.[36] In 1997, 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

[31] See, e.g., Levy, *Crypto*, 33. ("Both Diffie and Hellman firmly believed that the advent of digital communications made commercial cryptography absolutely essential. All of these huge computer and telephone networks made life incredibly easy for eavesdroppers--it was going to be possible to fully automate spying.")
[32] Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 5.
[33] Brian McCullough, "The NSA Tried This Before - What the 90s Debate Over the Clipper Chip Can Teach Us About Digital Privacy," *Internet History Podcast*, August 11, 2014, http://www.Internethistorypodcast.com/2014/08/the-nsa-tried-this-before-what-the-90s-debate-over-the-clipper-chip-can-teach-us-about-digital-privacy-debates/. Some have argued was a key turning point in the evolution of the digital rights movement in the United States; "Crypto Experts' Letter on Clipper," Electronic Privacy Information Center, January 27, 1994, *available at* https://epic.org/crypto/clipper/crypto_experts_letter_1_94.html.
[34] CPSR was founded in 1981 to "promote the responsible use of computer technology." See "About CPSR," Computer Professionals for Social Responsibility, http://cpsr.org/about/.
[35] They wrote: "The Clipper proposal should not be adopted. We believe that if this proposal and the associated standards go forward, even on a voluntary basis, privacy protection will be diminished, innovation will be slowed, government accountability will be lessened, and the openness necessary to ensure the successful development of the nation's communications infrastructure will be threatened" ("CPSR's Electronic Clipper Petition," Computer Professionals for Social Responsibility, August 1995, http://cpsr.org/prevsite/program/clipper/cpsr-electronic-petition.html/).
[36] Levy, *Crypto*, 254, 264-268, 304.

to our communications across the Web?"[37] These remarks reflected a desire to preserve civil liberties and the fundamental right to privacy in the face of rapid technological change.

Strong Encryption Enables Free Expression

The security and privacy protections afforded by the use of strong encryption help promote free expression online as well. It has been well-established, including by the previous UN Special Rapporteur on Freedom of Expression and Opinion, that the right to privacy and free expression often go hand-in-hand in the digital age.[38] When individuals know or believe that they may be under surveillance, it has a demonstrable chilling effect on free speech and the free flow of information online.[39] Moreover, because it is widely acknowledged that the growth of a secure Internet has contributed positively to free expression,[40] actions that impede or slow the proliferation of secure, Internet-based communications indirectly impede that same freedom.

Attempting to restrict the export of encryption technology to foreign countries — particularly source code[41] — also raises additional free expression concerns, as demonstrated by First Amendment challenges to the United States' limits on encryption exports. In the 1990s multiple legal cases, including *Bernstein v. U.S. Department of Justice*[42] and *Karn v. U.S. Department of State*,[43] focused on the question of whether encryption source code should be recognized as "speech" subject to the protections of the First Amendment. Although the outcomes of these cases were mixed, in *Bernstein* the court ruled that the software code at issue

[37] "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.

[38] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, Frank LaRue," United Nations General Assembly Human Rights Council, A/HRC/23/40, April 17, 2013, ¶24-27, *available at* http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf. ("The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression.")

[39] A. Michael Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution," University of Pennsylvania Law Review (1995) (particularly the discussions of "Chilling Effect on Speech" and "Anonymity and Freedom of Association" in Part III.A "First Amendment Issues"). *More recently, see* "With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy," *Human Rights Watch & The American Civil Liberties Union*, July 2014, *available at* https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf.

[40] *See* "Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, Frank LaRue," United Nations General Assembly Human Rights Council, A/HRC/17/27, May 16, 2011, ¶19-27, *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf?utm_source=twitterfeed&utm_medium=twitter. *See also* "'Regardless of Frontiers': The International Right to Freedom of Expression in the Digital Age," *Center for Democracy & Technology*, April 2011, *available at* https://cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf; "Freedom of Expression and ICTs: Overview of international standards," *Article 19*, 2013, *available at* http://www.article19.org/data/files/medialibrary/37380/FoE-and-ICTs.pdf ("Access to the internet is crucial for the enjoyment of the right to freedom of expression and other rights in the digital age. It has been observed that without the means to connect or without an affordable connection, the right to freedom of expression and the freedom of the media become meaningless in the online world.").

[41] Posting software to the Internet or otherwise publishing source code is considered an export if it can be accessed by non-U.S. citizens.

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

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

was indeed speech, and that attempting to require Bernstein to register and obtain a license to publish his code outside of the United States was an unconstitutional prior restraint on that speech.[44] The creation of an exemption that covered the export of free and open source software helped to resolve this issue.

Strong Encryption is Necessary for the Growth of the Information Economy

Strong encryption increases users' confidence in the security of their online communications and transactions, which is a critical step toward enabling the growth of the information economy and the migration of sensitive communications online. In 1996, the National Research Council's Committee to Study National Cryptography Policy[45] 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."[46] This prediction was borne out in the decade that followed. The growing uses for encryption to secure everyday transactions made electronic commerce and other types of transactions more appealing option to individuals and businesses alike. And as the Internet grows as a platform for commerce, it also grows as a platform for free expression.

Conversely, undermining or deliberately weakening encryption can have a detrimental effect on the growth of the information economy and the global competitiveness of the technology companies that drive it. Requiring companies to have surveillance backdoors often comes with direct costs because of the additional complexity that hardware manufacturers and software developers have to build into their products, which could be enormous when scaled nationally or globally.[47] Mandating backdoors also carries indirect — but often significant — costs through its impact on consumer confidence and the potential chilling effect this can have on new technology adoption. Simply put, when customers know that a government has access to all of their encrypted communications, it diminishes trust in that country's technology products, which can lead to a decline in overall use. During the Clipper Chip debate, experts predicted that if the chip became standard, U.S. companies might even find it more difficult to sell products that did not include the Clipper Chip because of the decline in overall confidence in the security of American-made products.[48]

In addition to impacting local consumer trust, concerns about weak encryption and backdoors can undermine the U.S. tech sector abroad. There is a powerful disincentive for foreign customers to choose American products if the practical result is that their sensitive communications can be accessed by the U.S. government — let alone criminals and hackers who may be able to exploit flaws in the technology.[49] And in a rapidly growing market, if export

[44] Camp, L Jean and Lewis, Ken. "Code as Speech" *Ethics and Information Technology*, March 2001. *Available at* http://www.ljean.com/files/CODE_FEDERALISM.pdf; Bernstein v. U.S. Dept. of Justice, et. al, 176 F.3d 1132 (9th Cir. 1999), *available at* https://epic.org/crypto/export_controls/bernstein_decision_9_cir.html.

[45] 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.

[46] "Cryptography's Role in Securing the Information Society," (1996).

[47] Abelson et al. describe potentially billions of dollars of direct and indirect costs to "deploy a global key recovery infrastructure." *See* Section 3.2.1 ("Scale"), Section 3.2.2 ("Operational Complexity"), and Section 3.3 ("New Costs").

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

[49] *Ibid*.

controls make it difficult or impossible for American companies to sell products containing strong encryption outside of the United States, then foreign companies will likely step in to fill that gap. In the 1990s, U.S. companies worried that they faced potentially significant business losses because of the impact on their expansion into overseas markets.[50] Similar arguments would apply to any country that wants to be competitive internationally but is considering backdoor mandates.

Ultimately, the resolution of the Crypto Wars came down to a calculation of the costs versus benefits. Making it more complicated or impossible to produce and distribute tools that use encryption would almost certainly undermine the U.S. technology industry and the growth of the Internet economy generally. Yet, it was unlikely that export controls and other restrictions would actually stop the spread of strong cryptography around the world.[51] When weighed against the additional benefits that strong encryption provides for the security of the Internet, individual privacy, and free expression, the choice was clear. Since defeat of the Clipper Chip proposal and the relaxation of export controls on encryption technology — which are widely characterized as the end of the Crypto Wars — strong encryption has become a bedrock technology when it comes to the security of the Internet.

II. After the Crypto Wars: Encryption, the Internet Economy, and Human Rights

Developments since the 1990s have demonstrated that, in addition to its positive impact on security, liberty, and economic growth, encryption is increasingly critical to the protection of human rights online. The growth of an Internet economy based on the ability to conduct secure transactions has fueled a virtuous cycle that also enables safer and more secure communications channels for dissidents, human rights activists, and other marginalized groups, which has become a key component of U.S. foreign policy efforts related to Internet freedom in the 21st century.

Economic Growth After the Crypto Wars

The resolution of Clipper Chip debate in favor of robust encryption for everyone played a significant role in jumpstarting the nascent Internet economy in the early 21st century. Innovations in applied cryptography laid the foundation for the emergence of a vibrant

---

[50] 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/forms-documents/doc_view/24-a-study-of-the-international-market-for-computer-software-with-encryption-nsa-1995. ("Some firms acknowledge that the current foreign market for products like theirs is probably small, but is expected to grow substantially. They believe that not being able to participate at the early stage of market development will be a tremendous obstacle to their future international competitiveness. Most believe the potential foreign market is substantial, and predict that their export sales could increase significantly if allowed to export stronger algorithms — some by orders of magnitude.")

[51] A June 1999 report notes that "a total of 512 foreign companies that either manufacture or distribute foreign cryptographic products in at least 67 countries outside the United States," and "On average, the quality of foreign and U.S. products is comparable." For more on the foreign availability of encryption and encrypted products, see 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. *See also* "Statement of Lance J. Hoffman, Professor, The George Washington University, before the U.S. Senate Committee on Commerce, Science, and Transporation," June 10, 1999, *available at* http://www.seas.gwu.edu/~lanceh/senate_testimony_pdf.pdf.

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 people being able to conduct secure transactions online and to trust that connections advertised as secure actually are.[52] Since the Crypto Wars ended, electronic commerce in the United States has risen steadily.[53]

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."[54] The Secure Shell Protocol (SSH), though lesser known, quickly became an equally indispensable tool for administering large numbers of servers remotely — an essential prerequisite for the rise of the modern data-center.[55] In the early 21st century, 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 Virtual Private Networks (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.

Encryption and U.S. Human Rights Policies

While the human rights benefits of strong encryption did not play a central role in the 1990s debate, its value became more evident after the Crypto Wars ended. Support for strong encryption became an integral part of U.S. foreign policy related to Internet freedom in the 21st century. Since 2010, the American government has built up a successful policy and programming agenda based on promoting an open and free Internet.[56] These efforts include

---

[52] 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.")

[53] 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/. 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.

[54] Holly Lynne McKinley, "SSL and TLS: A Beginners Guide," *SANS Institute*, 2003, *available at* https://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029.

[55] "History of SSH (SSH, The Secure Shell: The Definitive Guide)." University of Arkansas, College of Engineering. *Available at* http://csce.uark.edu/~kal/info/private/ssh/ch01. At the same time as these new 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 and Comodo were formed to manage the so-called "Web of Trust," charged with arbitrating the authenticity of the digital certificates used in encryption and providing independent verification to consumers that the secure sites they were visiting were actually implementing encryption properly, and were not being impersonated by a malicious actor.

[56] 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.*

providing over $120 million in funding for "groups working to advance Internet freedom – supporting counter-censorship and secure communications technology, digital safety training, and policy and research programs for people facing Internet repression."[57] The American government provides a great deal of specific funding for circumvention tools and other programming that supports free expression, much of which relies on strong encryption as part of the underlying technology. For example, the Open Technology Fund, a division of Radio Free Asia,[58] is specifically mandated to "support programs focused on... privacy enhancement, including the ability to be free from repressive observation and the option to be anonymous when accessing the Internet; and security from danger or threat when accessing the Internet, including [by use of] encryption tools."[59] The U.S. government has also funded the development of The Onion Router (Tor), a free and open source tool used primarily to anonymize web traffic—further demonstrating how support for tools that rely on strong encryption can further U.S. government interests.[60]

Over the past fifteen years, a virtuous cycle between strong encryption, economic growth, and support for free expression online has evolved. Not only does the proliferation of strong encryption bring clear economic benefits, it oftens serves to increase the free flow of information online as well. Some experts have dubbed this phenomenon "collateral freedom," which refers to the fact that "[w]hen crucial business activity is inseparable from Internet freedom, the prospects for Internet freedom improve."[61] Thus, while free expression and support for human rights may not have been the primary impetus behind the growth of the encrypted web since the end of the Crypto Wars, they have certainly benefited from its rapid expansion in the past two decades.

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). *Also see* the U.S. State Department's Internet Freedom page: http://www.humanrights.gov/issues/Internet-freedom/.

[57] 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

[58] Radio Free Asia is a private non-profit funded by the Broadcasting Board of Governors.

[59] "About the Program," *Open Technology Fund*, n.d., https://www.opentechfund.org/about (accessed February 8, 2015).

[60] Originally a project of the U.S. Naval Research Laboratory, Tor is a service that attempts to protect user identities by routing traffic through a network of virtual tunnels. According to the project website, "Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination." ("Tor: Overview," The Tor Project, n.d., https://www.torproject.org/about/overview.html.en). Tor is still largely funded by other parts of the U.S. government, including the State Department's Internet Freedom program, the National Science Foundation, and Radio Free Asia.

[61] 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.)

III. Encryption Under Threat

In recent 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 modern threats from both government and non-government 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. Fortunately, this amnesia is one-sided. The counter-arguments that won the Crypto Wars in the 1990s still hold true, and are again being made by advocates for privacy, security, and human rights.

The Snowden leaks demonstrated that, in many ways, the NSA continued the Crypto Wars in secret after it lost the public battle against encryption in the 1990s. As a September 2013 *New York Times* story revealed, the NSA has been clandestinely inserting backdoors into secure products and working to weaken key encryption standards over the past two decades.[62] Reports also suggest that the NSA has tapped fiber optic links connecting Google and Yahoo data centers located outside of the United States[63] and tried to crack anonymity tools like Tor.[64] According to the "black budget" published by *The Washington Post* in August 2013, 21 percent of the intelligence budget (roughly $11 billion) goes toward the Consolidated Cryptologic Program, which has 35,000 staff in the NSA and armed forces' surveillance and code breaking units.[65] The

[62] Nicole Perlroth, Jeff Larson & Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *The New York Times*, September 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-Internet-encryption.html?pagewanted=all&_r=0. According to a GCHQ memo from 2010: "For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies." For a full discussion of how the NSA worked to undermine Internet security, see "Part V: Costs to Cybersecurity" in Danielle Kehl et al., "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity," *New America's Open Technology Institute*, July 2014, http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf).

[63] Barton Gellman & Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post*, October 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[64] James Ball, Bruce Schneier & Glenn Greenwald, "NSA and GCHQ target Tor network that protects anonymity of web users," *The Guardian*, October 4, 2013, http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

[65] Kevin Poulsen, "New Snowden Leak Reports 'Groundbreaking' NSA Crypto Cracking," *Wired*, August 29, 2013, http://www.wired.com/2013/08/black-budget/; Barton Gellman and Greg Miller, "U.S. spy network's successes, failures and objectives detailed in 'black budget' summary," *The Washington Post*, August 29, 2013, http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html?tid=pm_world_pop.

NSA's strategy also includes developing private partnerships with the tech industry to shape the development of the worldwide telecommunications and cryptography market.[66]

These revelations were met with broad public outcry from industry representatives, privacy advocates, and technologists who warned against the dangers of the NSA's actions to the overall security of the Internet.[67] In the summer of 2014, the U.S. House of Representatives approved with overwhelming bipartisan support an appropriations amendment to ban spending on government-mandated backdoors, although procedural maneuvers prevented it from being adopted into the final bill.[68] The strong negative public reaction to the Snowden leaks also accelerated faster and wider adoption of encryption in a number of commercial services, from email and mobile messaging to the transmission of Internet traffic[69] more broadly. Policymakers and industry have responded swiftly to increased pressure from advocacy groups as well as individual and enterprise customers who have expressed concerns about the security of their data.[70] A range of different encryption proposals have been proposed by politicians in Europe since June 2013.[71] Meanwhile, American technology companies have begun adding more

---

[66] "SIGINT Enabling Project," *ProPublica*, available at https://www.propublica.org/documents/item/784285-sigint-enabling-project.html.

[67] See, e.g., Aleksei Oreskovic, "Facebook CEO Zuckerberg phoned Obama to complain about spying," *Reuters*, March 13, 2014, http://www.reuters.com/article/2014/03/13/us-facebook-obama-idUSBREA2C27920140313; Arik Hesseldahl, "In Letter to Obama, Cisco CEO Complains About NSA Allegations," *re/code*, May 18, 2014, http://recode.net/2014/05/18/in-letter-toobama-cisco-ceo-complains-about-nsa-allegations/; Bruce Schneier, "The U.S. Government Has Betrayed the Internet. We Need to Take It Back." *The Guardian*, September 5, 2013, http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying; Dan Auerbach and Eva Galperin, "Leaks Show NSA is Working to Undermine Encrypted Communications, Here's How You Can Fight Back," *Electronic Frontier Foundation*, September 5, 2013, https://www.eff.org/deeplinks/2013/09/leaks-show-nsa-working-undermine-encrypted-communications-heres-how-you-can-fight

[68] See Amendment to H.R. 4870, the Department of Defense Appropriations Act, offered by Representative Massie of Connecticut. The Amendment "prohibits funds for the government to request that products or services support lawful electronic surveillance" ("H.R. 5870 - The FY 2015 Department of Defense Appropriations Bill: House Adopted Amendments," *available at* http://appropriations.house.gov/uploadedfiles/06.20.14_fy_2015_defense_bill_-_floor_adopted_amendments.pdf). *The full text of the amendment is available at* https://www.eff.org/document/sensenbrenner-massie-lofgren-amendment-2014. For analysis of the amendment, see "House Passes Amendment to Rein in NSA's Warrantless Searches," *Center for Democracy & Technology*, June 20, 2014, https://cdt.org/press/house-passes-amendment-to-reign-in-nsas-warrantless-searches/; Nadia Kayyali, "Security Backdoors Are Bad News — But Some Lawmakers Are Taking Action to Close Them," *Electronic Frontier Foundation*, December 9, 2014, https://www.eff.org/deeplinks/2014/12/security-backdoors-are-bad-news-some-lawmakers-are-taking-action-close-them.

[69] One interesting data point is that in the year after the Snowden disclosures, encrypted web traffic doubled in North America and quadrupled in Europe and Latin America, according to data from Sandvine. Doug Drinkwater, "Encrypted Web Traffic Quadruples in Europe," *SC Magazine*, May 19, 2014, http://www.scmagazineuk.com/encrypted-web-traffic-quadruples-in-europe/article/347459/.

[70] See, e.g., the Electronic Frontier Foundation's "Encrypt the Web" report, *available at* https://www.eff.org/encrypt-the-web-report; Access's "Encrypt All the Things" campaign, which promotes its "Data Security Action Plan," *available at* https://encryptallthethings.net/; and Fight for the Future's "Reset the Net" campaign, *available at* https://www.resetthenet.org/.

[71] A study from New America's Open Technology Institute and the Global Public Policy Institute in Germany found that the majority of proposals from European political and business leaders to avoid foreign surveillance focused on largely ineffective measures like localized routing and data storage and the construction of new undersea cables. But some proposals, particularly those coming from the academic and technical communities, suggested that more (and more secure) encryption was the best way to secure communications from unwanted access. For a full discussion of the proposals for greater "technological sovereignty" that have emerged in Europe since the Snowden disclosures —

encryption to their products.[72] Major companies like Apple,[73] Google,[74] and Whatsapp,[75] for example, have all started building more encryption by default into their products. The consensus in the digital rights community — among policy groups, grassroots organizers, and their allies in industry and government — is that encryption is the best and most productive way to address concerns about government surveillance.

Building upon the broad bipartisan support for the amendment banning government-mandated backdoors that was offered in the summer of 2014, Senator Ron Wyden and Representative Zoe Lofgren introduced the Secure Data Act in December 2014, which would similarly prohibit the government from requiring that companies weaken the security of their products or insert backdoors to facilitate access.[76] The bill was prompted by the recognition that government technology mandates that weaken security are bad for national security, the U.S. economy, and individual privacy. "Strong encryption and sound computer security is the best

---

including those that would promote broader use of encryption — see Tim Maurer et al., "Technological Sovereignty: Missing the Point?" *New America's Open Technology Institute and The Global Public Policy Institute*, November 2014, http://www.newamerica.org/downloads/Technological_Sovereignty_Report.pdf.

[72] Andrea Peterson, "Privacy is tech's latest marketing strategy," *The Washington Post*, September 26, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/26/privacy-is-techs-latest-marketing-strategy/; Nuala O'Connor, "Encryption Makes Us All Safer," *Center for Democracy & Technology*, October 8, 2014, https://cdt.org/blog/encryption-makes-us-all-safer/; Seeta Peña Gangadharan, "Smartphone Encryption Restores Public Trust in Technology," *The New York Times*, September 30, 2014, http://www.nytimes.com/roomfordebate/2014/09/30/apple-vs-the-law/smartphone-encryption-restores-public-trust-in-technology.

[73] In September 2014, Apple announced that it was moving toward full smartphone encryption by default on its new iOS. David E. Sanger and Brian X. Chen, "Signaling Post-Snowden Era, New iPhone Locks Out NSA," *The New York Times*, September 26, 2014, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html?_r=0.

[74] In June 2013, Google released the source code for the Chrome browser's End-to-End extension, which would allow users to encrypt their data before it leaves the browser. The code can now be audited by security experts, and their ultimate goal is to develop an alternative to existing end-to-end encryption tools like PGP and GnuGP, which can be difficult and time-consuming to use. "Making end-to-end encryption easier to use," *Google Online Security Blog*, June 2014, http://googleonlinesecurity.blogspot.com/2014/06/making-end-to-end-encryption-easier-to.html. Google also followed Apple's smartphone encryption announcement in September by revealing that it intended to take similar steps on the Android platform. Craig Timberg, "Newest 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/?wpisrc=nl-swbd&wpmm=1.

[75] In November 2014, the popular mobile chat app WhatsApp began encrypting its message traffic end to end (Molly Wood, "Whatsapp Adds Android Encryption," *The New York Times*, November 18, 2014, http://bits.blogs.nytimes.com/2014/11/18/whatsapp-adds-encryption-on-android-phones/?_r=0). Whatsapp's decision represents "the world's largest-ever implementation of this standard of encryption in a messaging service" (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/).

[76] S.2981, Secure Data Act of 2014, 113th Cong. (2014), *available at* https://www.congress.gov/bill/113th-congress/senate-bill/2981?q=%7B%22search%22%3A%5B%22%5C%22secure+data+act%5C%22%22%5D%7D.

way to keep Americans' data safe from hackers and foreign threats," explained Senator Wyden.[77] The bill was reintroduced in the House in 2015, although no further action has been taken.[78]

Unfortunately, the trend toward greater use of encryption has pushed law enforcement advocates in the U.S. to return to past arguments that these technologies will exacerbate the "going dark" problem and prevent investigators from getting access to vital communications.[79] The current debate in the U.S. pits high-ranking officials like the FBI Director and the Attorney General[80] against major technology companies, privacy advocates, and lawmakers who believe that the benefits of strong encryption still far outweigh any negatives.[81] These concerns have been exacerbated in light of the January 2015 terrorist attacks in Paris, which prompted the Prime Minister of the UK to threaten to outlaw strong encryption absent backdoors for government surveillance.[82] While some have suggested that there must be a viable

---

[77] Press Release, "Wyden Introduces Bill To Ban Government-Mandated Backdoors Into Americans' Cell Phones and Computers," *The Office of Senator Ron Wyden*, December 4, 2014, http://www.wyden.senate.gov/news/press-releases/wyden-introduces-bill-to-ban-government-mandated-backdoors-into-americans-cellphones-and-computers.

[78] Cory Bennett, "House bill would ban mandated tech access," *The Hill*, February 4, 2015, http://thehill.com/policy/cybersecurity/231745-house-reintroduces-bill-to-ban-tech-backdoors.

[79] "[T]he Going Dark problem is about the government's practical difficulties in intercepting the communications and related data that courts have authorized it to collect," according to former FBI General Counsel Valerie Caproni (Valerie Caproni, "Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security," *Federal Bureau of Investigation*, February 17, 2011, *available at* http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies).The FBI has long argued that there is "a growing gap between the government's legal authority and its practical ability to capture communications" (Ellen Nakashima, "Proliferation of new online communications services poses hurdles for law enforcement," *The Washington Post*, July 26, 2014, http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html). However, some experts have disputed this assertion, explaining that despite the proliferation of encryption, we actually live in a "golden age for surveillance" where law enforcement officials have access to more data than ever about us, our communications, and our movements (Peter Swire & Kanesa Ahmad, "'Going Dark' Versus a 'Golden Age for Surveillance,'" *Center for Democracy & Technology*, November 28, 2011, http://www.futureofprivacy.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf; also see Peter Swire & Kanea Ahmad, "Encryption and Globalization," *The Columbia Science & Technology Review* Vol. XIII, Spring 2012, *available at* http://stlr.org/download/volumes/volume13/Swire.pdf.).

[80] After the Google and Apple announcements in September, FBI Director James Comey said that the companies' decisions would place smartphone users "beyond the law" and called for Congressional action in a speech at the Brookings Institution ("FBI Blasts Apple, Google for locking police out of phones," http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html; "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course). Manhattan District Attorney Cyrus Vance called device encryption a threat to public safety, while former Attorney General Eric Holder urged tech companies to leave backdoors open for police (http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html; http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/30/holder-urges-tech-companies-to-leave-device-backdoors-open-for-police/)

[81] For a full list of sources from the recent crypto debate, see the appendix attached to this filing.

[82] In an interview in January 2015, UK Prime Minister David Cameron said, "I think we cannot allow modern forms of communication to be exempt… from being listened to." (David Meyer, "UK's Cameron won't 'allow' strong encyption of communications," *GigaOm*, January 12, 2015, https://gigaom.com/2015/01/12/uks-cameron-wont-allow-strong-encryption-of-communications/). Boris Johnson, the Mayor of London, made similar assertions a few days before. (Steven Swinford, "Boris Johnson: I am not bothered with civil liberties stuff for terror suspects," *The*

compromise,[83] finding a technical solution that would enable robust encryption while ensuring that only the government can access the data with a warrant remains as impossible as it was during the Clipper Chip debate in the 1990s.[84]

Conclusion and Recommendations

Even after two decades of vast technological change and the rapid growth of the Internet into a global platform for commerce, speech, and the exchange of ideas, the arguments in favor of the benefits of encryption that won the Crypto Wars of the 1990s still hold true today. Therefore — and so that we might learn from history rather than be doomed to repeat it — we respectfully urge the Special Rapporteur to reiterate the importance of encryption to the protection of our fundamental rights online. A clear message must be sent to lawmakers both in the United States and around the world that promoting strong encryption without backdoors can and still should be the norm in the digital age. This recommendation is consistent with conclusions drawn by branches of and independent advisors to the U.S. government in the past few years. A recent report from *The Guardian*, for example, revealed leaked documents written by the U.S. National Intelligence Council in 2009 which highlighted both corporate and government vulnerabilities to hacking "due to the slower than expected adoption of... encryption and other technologies" and suggested that encryption technology is the "[b]est defense to protect data."[85]

More recently, in the wake of the NSA disclosures, the President's Review Group on Intelligence and Communications Technologies[86] issued a crucial recommendation on the

---

Telegraph, January 11, 2015, http://www.telegraph.co.uk/news/worldnews/europe/france/11338602/Boris-Johnson-I-am-not-bothered-with-civil-liberties-stuff-for-terror-suspects.html.)

[83] *The Washington Post* Editorial Board, for example, argues that to achieve the balance between privacy and security, the tech companies should create some kind of "secure golden key" that only the government has access to. "Compromise needed on smartphone encryption," *The Washingon Post*, October 3, 2014, http://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html.

[84] Jeremy Gillula, "Even a Golden Key Can Be Stolen By Thieves: The Simple Facts of Apple's Encryption Decision," *Electronic Frontier Foundation*, October 10, 2014, https://www.eff.org/deeplinks/2014/10/even-golden-key-can-be-stolen-thieves-simple-facts-apples-encryption-decision; 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. For a more in-depth discussion, see Ben Adida et al., "CALEA II: Risks of Wiretap Modifications to Endpoints," *Center for Democracy & Technology*, May 17, 2013, *available at* https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.

[85] Quoted in James Ball, "Secret US Cybersecurity Report: encryption vital to protect private data," *The Guardian*, January 15, 2015, http://www.theguardian.com/us-news/2015/jan/15/-sp-secret-us-cybersecurity-report-encryption-protect-data-cameron-paris-attacks.

[86] The Presidents' Expert Review Group was established in August 2013 in the wake of the Snowden disclosures. The group consisted of Richard Clarke, Michael Morell, Geoffrey Stone, Cass Sunstein and Peter Swire, who were tasked with reviewing "how in light of advancements in communications technologies, the United States can employ its technical collection capabilities in a manner that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure." "About the Review Group on Intelligence and Communications Technologies," Office of the Director of National Intelligence, http://www.dni.gov/index.php/intelligence-community/review-group.

importance of encryption in the wake of the Snowden disclosures. Arguing that "[e]ncryption is an essential basis for trust on the Internet,"[87] the report urged the U.S. government to:

> (1) fully support and not undermine efforts to create encryption standards;
> (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and
> (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.[88]

As various commentators have noted, this was one of the strongest recommendations made by the Review Group,[89] and we believe that both the language and the substance of this recommendation should inform your report and UN Member States' actions more broadly.

As we highlighted earlier in this submission, there are a number of existing examples in laws that the United States has either enacted or proposed that can further instruct Member States' approach to encryption technology. As a first step, States can codify that lawful intercept mandates do not require breaking or interfering with individuals' use of encryption, drawing upon the language in CALEA. States can further establish a legal norm that they will not require that companies weaken encryption or provide backdoor access to governments, following the example of the recently proposed Secure Data Act of 2014. Finally, States can affirm a positive right of the citizenry to possess, use, and distribute strong encryption, as proposed in the SAFE Act of the late 1990s.

Thank you for your consideration.

Respectfully submitted,

Danielle Kehl
Kevin Bankston
Andi Wilson

New America's Open Technology Institute
1899 L Street NW, Suite 400
Washington, DC 20036

[87] "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, 216. *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[88] "Liberty and Security in a Changing World," 36.
[89] Justin Elliott, "Presidential Panel to NSA: Stop Undermining Encryption," *ProPublica*, December 18, 2013, http://www.propublica.org/article/presidential-panel-to-nsa-stop-undermining-encryption.