Statement of Kevin S. Bankston
Policy Director of New America's Open Technology Institute
& Co-Director of New America's Cybersecurity Initiative

Before the U.S. House of Representatives
Subcommittee on Information Technology
of the Committee on Oversight and Government Reform

Hearing on "Encryption Technology and Possible U.S. Policy Responses"

April 29, 2015

Chairman Hurd, Ranking Member Kelly and Members of the Subcommittee:

Thank you for giving me the opportunity to testify today on the importance of strong encryption technology to Americans' continued security and prosperity, and allowing me to articulate the arguments against recent suggestions that Congress should legislate to limit the availability of strongly encrypted products and services. I represent New America's Open Technology Institute (OTI), where I am Policy Director of the OTI program and also Co-Director of New America's cross-programmatic Cybersecurity Initiative. New America is a nonprofit civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences. OTI is New America's program dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open and secure communications networks.

In September, Apple and Google enhanced the security of all smartphone users by modifying the operating system software of iPhones and Android smartphones, respectively, to ensure that the contents of those phones are encrypted by default such that only the user can decrypt them.[1] However, instead of praising those companies for taking a step that would help prevent countless crimes and data breaches, a variety of high-level law enforcement and intelligence officials instead quickly raised concerns that such unbreakable encryption—whether in the context of smartphones or in the context of end-to-end encrypted Internet communications—may pose a challenge to law enforcement and intelligence investigations.[2] Several officials have even gone

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

[2] For a summary of the controversy as it stood in November 2014, along with a bibliography of relevant announcements, speeches, op-eds, analyses and other resources that had been published up to that point, see

so far as to urge Congress to pass legislation to address the issue,[3] presumably by requiring companies to build their systems such that even when their users' data is encrypted, the government can still obtain the plain text of that data when necessary to a lawful investigation. Put more colloquially, they seem to be suggesting that companies build "backdoors" into their encrypted products and services in order to allow surreptitious access by the government.

With all due respect for the many legitimate needs of our law enforcement and intelligence agencies, I am here today to give you ten reasons why Congress should reject any such proposal. First and most obviously…

1. It was already rejected as a policy approach two decades ago, including by Congress. American policymakers were faced with just this issue in the 90s as part of a policy debate often referred to as the "Crypto Wars," where the Clinton Administration battled against privacy advocates and the technology industry on a variety of fronts to limit the spread of strong encryption in order to address law enforcement and intelligence concerns.[4] One conflict was over the U.S. government's attempts to promote so-called "key escrow" technologies—such as the much-maligned "Clipper Chip"[5]—whereby the government or a trusted third party would hold master keys that could decode any encrypted communications. The other conflict was over the U.S. government's attempts to restrict the proliferation of strong encryption products overseas by treating them as munitions subject to export controls. Ultimately, after many years of debate and widespread opposition from the public as well as from Congress, the Administration withdrew its key escrow proposals and relaxed export restrictions on encryption. It did so in response to many of the same arguments that I will make today: that strong encryption is vital to our information security, to our economic security, and to our privacy and free speech, and that attempts to limit

---

Danielle Kehl & Kevin Bankston, "The #CryptoDebate is Coming: Are You Prepared?", *New America's Open Technology Institute,* November 14, 2014, *available at* https://www.newamerica.org/oti/the-cryptodebate-is-coming-are-you-prepared/. For a basic introduction to encryption technology and the role that it plays in our lives, see Danielle Kehl, "Encryption 101," *Slate*, February 24, 2015, *available at* http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html.

[3] Spencer Ackerman, "FBI director attacks tech companies for embracing new modes of encryption," *The Guardian*, October 16, 2014, *available at* http://www.theguardian.com/us-news/2014/oct/16/fbi-director-attacks-tech-companies-encryption; "FBI Director Continues Crusade Against Encryption, Calls on Congress to Act," *The District Sentinel*, March 25, 2015, *available at* https://www.districtsentinel.com/fbi-director-continues-crusade-against-encryption-calls-on-congress-to-act/; Andrew Weissmann, "Apple, Boyd, and Going Dark," *Just Security*, October 20, 2014, *available at* http://justsecurity.org/16592/apple-boyd-dark/; Cyrus Vance Jr., "Apple and Google threaten public safety with default smartphone encryption," *The Washington Post*, September 26, 2014, *available at* 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 ("Absent remedial action by the companies, Congress should act appropriately.").

[4] For a brief but well-documented summary of the Crypto Wars and their lessons for today's policymakers, see Danielle Kehl, Kevin Bankston & Andi Wilson, "Comments to the UN Special Rapporteur on Freedom of Expression and Opinion Regarding the Relationship Between Free Expression and the Use of Encryption," *New America's Open Technology Institute*, February 10, 2015, *available at* https://static.newamerica.org/attachments/1866-oti-urges-un-human-rights-council-to-promote-the-benefits-of-strong-encryption/OTI_Crypto_Comments_UN.pdf. For a more detailed history, see Steven Levy, *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age* (New York: Viking, 2001).

[5] See Steven Levy, "Battle of the Clipper Chip," *The New York Times*, June 12, 1994, *available at* http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.

the distribution or use of strong encryption that is free of government backdoors will not only undermine those priorities but will be ineffective and ultimately unnecessary.

The eventual consensus on these points was summed up at the time by Representative Bob Goodlatte, who concluded that "[o]nly 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."[6] That consensus was reflected by Congressman Goodlatte's Security and Freedom Through Encryption or "SAFE" Act, a bill that sought to reaffirm Americans' right to distribute and use strong encryption, bar the government from mandating the use of key escrow technologies, and allow for the export of strong encryption.[7] By 1999, that bill was cosponsored by a majority of House members—258 of them, including current members of this oversight committee, Ranking Member Elijah Cummings (D-MD), Rep. John "Jimmy" Duncan Jr. (R-TN), Rep. John Mica (R-FL), and Del. Eleanor Norton (D-DC).[8]

That bill was also in line with the recommendations of the National Academies, which after extensive study issued a 700-plus page report on the policy challenges posed by encryption. Its primary recommendation was:

> **Recommendation 1**—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.[9]

As Professor Peter Swire, the White House's privacy czar at the time that it announced its newly liberalized encryption export policies, recently summed up the conclusion of the Crypto Wars: "If there is modest harm and enormous gain to be derived from using certain technology, societies should logically adopt that technology. In 1999, the U.S. government concluded that strong encryption was precisely that type of valuable technology—it was worth going at least slightly "dark" in order to reap the many benefits of effective encryption."[10] One of the most obvious benefits of encryption—then as now—is that it ensures the security of the private communications and data of Americans and American companies against all attackers. And if the government were to mandate backdoors into encrypted products and services…

2. It would seriously undermine our nation's cybersecurity, at a time when that security is already in crisis as demonstrated by the endless string of high profile data breaches in the past

---

[6] "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.
[7] *See* H.R. 850, 106th Cong. (1999).
[8] *See id*.
[9] Kenneth W. Dam and Herbert S. Lin, Editors, Committee to Study National Cryptography Policy, National Research Council, "Cryptography's Role in Securing the Information Society," *National Academies Press* (1996), *available at* http://www.nap.edu/catalog/5131/cryptographys-role-in-securing-the-information-society.
[10] Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 8 Colum. Sci & Tech. L. Rev. 437 (2013), *available at* http://ssrn.com/abstract=1960602.

year.[11] Every technical expert that has spoken publicly on this controversy since it began last September—both experts from the generation that fought in the original Crypto Wars,[12] as well as experts from the next generation[13]—has concluded that it is impossible to devise a system that provides government access to data on encrypted devices, or to end-to-end encrypted communications, while also ensuring that it remains secure against other attackers, be they computer criminals, industrial spies, Chinese intelligence, or anyone else.[14] Whether you want to call it a front door or a back door, mandating guaranteed government access to encrypted data would open us up to a variety of new cyber-threats. In fact, it would be an open invitation for attackers to focus on hacking into U.S. products and services because they would be easier targets than products and services that are not subject to such mandated vulnerabilities.

As the Chief Information Security Officer of Yahoo put it when debating the issue with the Director of the NSA at New America's cybersecurity conference in February, "all of the best public cryptographers in the world would agree that you can't really build [secure] backdoors in

---

[11] A wide variety of commentators have labeled 2014 "the year of the hack" after an unprecedented string of major security breaches. Arjun Kharpal, "Year of the Hack? A Billion Records Compromised in 2014," *NBC News*, February 12, 2015, *available at* http://www.nbcnews.com/tech/security/year-hack-billion-records-compromised-2014-n305001; Bridget Carey, "2014: Year of the Hack," *CNET Magazine*, December 18, 2014, *available at* http://www.cnet.com/news/2014-the-year-of-the-hack/; Andrew Lumby, "2014: The Year of the Hack," *Fiscal Times*, December 30, 2014, *available at* http://www.thefiscaltimes.com/2014/12/30/2014-Year-Hack; Jennifer LeClaire, "2014: The Year of the Hacker, More to Come in 2015," *CIO Today*, December 31, 2014, *available at* http://www.cio-today.com/article/index.php?story_id=00100015QE3O.

[12] *See, e.g.,* Jeffrey Vagle and Matt Blaze, "Security 'Front Doors' vs. 'Back Doors': A Distinction Without a Difference," *Just Security*, October 17, 2014, *available at* http://justsecurity.org/16503/security-front-doors-vs-back-doors-distinction-difference/ ("Security engineers, cryptographers, and computer scientists are in almost universal agreement that any technology that provides a government backdoor also carries a significant risk of weakening security in unexpected ways."); Bruce Schneier, "Stop the hysteria over Apple encryption," *CNN.com*, October 31, 2014, *available at* http://www.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/index.html ("You can't build a backdoor that only the good guys can walk through. Encryption protects against cybercriminals, industrial competitors, the Chinese secret police and the FBI. You're either vulnerable to eavesdropping by any of them, or you're secure from eavesdropping from all of them."); Steven M. Bellovin, "Apple's 'Warrant-Proof' Encryption," *SMBlog*, September 23, 2014, *available at* https://www.cs.columbia.edu/~smb/blog/control/ ("[T]he existence of the code to implement [a] back door is itself a danger. Code is often buggy and insecure; the more code a system has, the less likely it is to be secure. This is an argument that has been made many times in this very context, [including in] debates over the Clipper Chip and key escrow in the 1990s…."); Tim Greene, "RSA: Panel calls NSA access to encryption keys a bad idea," *Network World*, April 22, 2015, *available at* http://www.networkworld.com/article/2913280/security0/rsa-panel-calls-nsa-access-to-encryption-keys-a-bad-idea.html (Quoting esteemed cryptologists and Crypto War veterans Ron Rivest, co-founder of RSA, and Whitfield Diffie, one of the inventors of public key cryptography, raising doubts about any new key escrow scheme. "'This is going to be a house of many doors and many parties and it's just not going to work,' Rivest says.").

[13] *See, e.g.,* Matthew Green, "How do we build encryption backdoors?", *A Few Thoughts on Cryptographic Engineering*, April 16, 2015, *available at* http://blog.cryptographyengineering.com/2015/04/how-do-we-build-encryption-backdors.html; Joseph Lorenzo Hall, "The NSA's Split-Key Encryption Proposal is Not Serious," *Center for Democracy & Technology*, April 20, 2015, *available at* https://cdt.org/blog/the-nsas-split-key-encryption-proposal-is-not-serious/.

[14] *See* Schneier, *supra* note12, for a concise summary of known instances of surveillance backdoors being exploited for purposes other than lawful surveillance: "Back-door access built for the good guys is routinely used by the bad guys. In 2005, some unknown group surreptitiously used the lawful-intercept capabilities built into the Greek cell phone system. The same thing happened in Italy in 2006. In 2010, Chinese hackers subverted an intercept system Google had put into Gmail to comply with U.S. government surveillance requests. Back doors in our cell phone system are currently being exploited by the FBI and unknown others."

crypto… That it's like drilling a hole in the windshield."[15] Indeed, when the White House cybersecurity coordinator was asked last week if he could name a single respected technical expert who believed it was possible, he had no answer.[16] Even one of the government's own top experts, the chief cybersecurity adviser to the Commerce Department's National Institute of Standards and Technologies, has publicly concluded that when it comes to designing a secure 'key escrow' system where the government has access to a master decryption key that can't be subverted by other attackers, "[t]here's no way to do this where you don't have unintentional vulnerabilities."[17] Put another way, there is no way to build a "secure golden key" that can only be used by the government, like that which was suggested in a recent *Washington Post* editorial that was immediately and roundly criticized by the Internet community.[18] This fact was conclusively demonstrated in the 90s,[19] and it is equally true today.[20] However, even assuming such a "golden key" system were feasible…

---

[15] Andrea Peterson, "Here's how the clash between the NSA Director and a senior Yahoo executive went down," *The Washington Post*, February 23, 2015, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/23/heres-how-the-clash-between-the-nsa-director-and-a-senior-yahoo-executive-went-down/; *see also* John Reed, "Transcript: NSA Director Mike Rogers vs. Yahoo! on Encryption Back Doors," *Just Security*, February 23, 2014, *available at* http://justsecurity.org/20304/transcript-nsa-director-mike-rogers-vs-yahoo-encryption-doors/.

[16] Joseph Menn, "White House seeks Silicon Valley help on strong yet breakable encryption," *Reuters*, April 21, 2015, *available at* http://www.reuters.com/article/2015/04/21/us-cybersecurity-rsa-encryption-idUSKBN0NC2LT20150421?irpc=932.

[17] Ellen Nakashima and Barton Gellman, "As encryption spreads, U.S. grapples with clash between privacy, security," *The Washington Post*, April 10, 2015, *available at* 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.

[18] *See* Washington Post Editorial Board, "Compromise needed on smartphone encryption," *The Washington Post*, October 3, 2014, *available at* http://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html*, but see, e.g.,* Vagle and Blaze, *supra* note 12 ("The problem with the "golden key" approach is that it just doesn't work."); Jeremy Gillula, "Even a Golden Key Can Be Stolen By Thieves," *Electronic Frontier Foundation*, October 10, 2014, *available at* https://www.eff.org/deeplinks/2014/10/even-golden-key-can-be-stolen-thieves-simple-facts-apples-encryption-decision; Mike Masnick, "Washington Post's Clueless Editorial On Phone Encryption: No Backdoors, But How About A Magical 'Golden Key'?" *Techdirt*, October 6, 2014, *available at* https://www.techdirt.com/articles/20141006/01082128740/washington-posts-braindead-editorial-phone-encryption-no-backdoors-how-about-magical-golden-key.shtml; Julian Sanchez, "What NSA Director Mike Rogers Doesn't Get About Encryption," *Cato Institute*, February 24, 2015, *available at* http://www.cato.org/blog/what-nsa-director-mike-rogers-doesnt-get-about-encryption ("When [FBI Director James] Comey or [NSA Director Michael] Rogers get a ten minute briefing from their experts about the plausibility of designing 'golden' key backdoors, they are probably getting the technically accurate answer that yes, on paper, it is possible…. The trouble… is that real world systems are rarely as tidy as the theories, and the history of cryptography is littered with robust-looking cryptographic algorithms that proved vulnerable under extended scrutiny or were ultimately impossible to implement securely under real-world conditions."). *See also* Video: Surveillance in Cyberspace by Government Actors at the 2015 Idaho Law Review Symposium (Idaho Law Review), *available at* https://vimeo.com/album/3349185/video/124869982 (Professor Ed Felten explaining difficult questions and serious risks associated with key recovery proposals).

[19] The definitive work on this subject from the 90s is a technical report coordinated by the Center for Democracy & Technology and authored by nearly a dozen of the top cryptographers and computer scientists of the era. *See* Hal Abelson *et al*, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," May 27, 1997, *available at* https://www.cdt.org/files/pdfs/paper-key-escrow.pdf.

[20] Several examples from this decade have further demonstrated the security risk of maintaining central databases of encryption keys. *See, e.g.,* Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed," *The New York Times*, June 3, 2011, *available at* http://www.nytimes.com/2011/06/04/technology/04security.html (theft of data about "SecurID" cryptographic tokens from security vendor RSA enabled hackers to breach the network of

3. It would cost the American economy untold billions of dollars. Experts estimated during the original Crypto Wars that building and operating the kind of key escrow infrastructure desired by the government would have cost the government and industry many billions of dollars.[21] Since then, the number of computer and Internet users, and computer and Internet devices, has grown exponentially; so too has the complexity and cost of such a scheme to give the government the universal decryption capability it apparently desires.[22]

That's not even counting the many more billions of dollars that would be lost as consumers worldwide lost confidence in the security of American computing products and online services. American technology companies, which currently dominate the global market, have already been wrestling with diminished consumer trust in the wake of revelations about the scope of the National Security Agency's programs, a loss of trust already predicted to cost our economy billions of dollars.[23] Any new requirement that those companies guarantee that the U.S. government have the technical capability to decrypt their users' data would give foreign users—including major institutional clients such as foreign corporations and governments that especially rely on the security of those products and services—even more incentive to avoid American products and turn to foreign competitors. It would also likely diminish trust in the security of digital technology and the Internet overall, which would slow future growth of the Internet and Internet-enabled commerce and threaten the primary economic engine of the 21st century.

To put it bluntly, foreign customers will not want to buy or use online services, hardware products, software products or any other information systems that have been explicitly designed to facilitate backdoor access for the FBI or the NSA.[24] Nor will many American users, for that

---

Lockheed, the United States' largest defense contractor, and put at risk the security of RSA's 25,000 customers, including Fortune 500 companies and government agencies around the world); Dominic Rushe, "Sim card database hack gave US and UK spies access to billions of cellphones," *The Guardian*, February 19, 2015, *available at* http://www.theguardian.com/us-news/2015/feb/19/nsa-gchq-sim-card-billions-cellphones-hacking (British intelligence agency GCHQ hacked into Gemalto, the world's largest SIM card manufacturer, stealing encryption keys giving it the capability to decrypt telephone and Internet communications made by the billions of cellphones using Gemalto cards).

[21] *See* Abelson et al., *supra* note 19 at 13–16 (describing potentially billions of dollars of direct and indirect costs to "deploy a global key recovery infrastructure").

[22] High costs associated with creating and maintaining such a complex key escrow system - overhead of operating the system; product design and testing costs, which must be rigorous and extensive to assure the highest level of security consistent with key escrow; and costs for all users who are required by law to comply with key escrow requirements. This also includes the potentially irreparable costs to users in the likely event that their communications are compromised. Swire and Ahmad, *supra* note 10.

[23] *See, e.g.,* Danielle Kehl, Kevin Bankston, Robyn Greene, & Robert Morgus, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity* (2014), http://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf; Daniel Castro, Information Technology and Innovation Foundation, *How Much Will PRISM Cost the US Cloud Computing Industry?* (2013), http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry (estimating that the revelations about the NSA's PRISM program could cost the American cloud computing industry $22 to $35 billion over the next three years); James Staten, Forrester Research, *The Cost of PRISM Will Be Larger Than ITIF Projects* (2013), http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects (arguing that ITIF's estimates were low, suggesting that the actual figure could be as high as $180 billion over three years).

[24] Vagle and Blaze, *supra* note 12 ("As Apple, Google, and other similarly situated companies point out, why would customers pay for and use such a system? Companies are now awakening to the fact that, in a post-Snowden world, customers are becoming more savvy about security issues, and will discern between products on this basis.").

matter. Instead, they will turn to more secure products that are available for purchase or for free download from sources outside of the United States, which is a major reason why…

4. It would not succeed at keeping bad actors from using unbreakable encryption. Encryption technology and the ability to create it was already becoming widespread during the original Crypto Wars,[25] and at this point is nearly ubiquitous. And, as was true then, much of that technology is free and open source. For example, there are the open source versions of PGP encryption software that are still the most popular end-to-end email encryption solution, the OpenSSL software library that has long been used to encrypt vast amounts of every-day web traffic, open source disk encryption programs like TrueCrypt, the open source Off-The-Record instant messaging encryption protocol used by a wide variety of IM clients, and the TOR onion routing software originally developed by the Naval Research Laboratory that is now widely used to circumvent oppressive governments' censorship regimes and allow for anonymous online browsing.[26] A government mandate prohibiting U.S. companies from offering products or services with unbreakable encryption is of little use when foreign companies can and will offer more secure products and services, and when an independent coder anywhere on the planet has the resources to create and distribute free tools for encrypting your communications or the data stored on your mobile devices. As former Homeland Security Secretary Michael Chertoff recently put it, "[T]hat genie is not going back in the bottle."[27]

The result is that a U.S. government-mandated backdoor into the encrypted products and services of U.S. companies, while undermining the information security of millions of ordinary Americans and the economic security of the American tech industry, would do little to prevent bad actors from taking advantage of strong encryption. Or, as PGP's inventor Phil Zimmerman famously said in the 90s: "If privacy is outlawed, only outlaws will have privacy."[28] Not only is such a mandate likely to be ineffective, but also…

5. It's unnecessary in order to keep us safe from criminals—but strong encryption is. So far, the opponents of strong device encryption have failed to offer any compelling examples where such encryption seriously hindered a criminal investigation or prosecution. FBI Director Comey did offer, in his October speech on the subject, four examples of cases where cellphone-derived evidence was supposedly critical to a solving a crime, but those examples were quickly debunked by the press.[29] During the same event, Director Comey came up empty when asked for

---

[25] 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. 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

[26] *See* The OpenPGP Alliance at http://www.openpgp.org/, the OpenSSL Project at https://www.openssl.org/, TrueCrypt (once popular but now discontinued due to security concerns) at http://truecrypt.sourceforge.net/, Off-The-Record Messaging at https://otr.cypherpunks.ca/, and the Tor Project at https://www.torproject.org/.

[27] Jason Koebler, "The Man Who Crafted the Patriot Act Now Supports Your Right to Encrypt Data," *Motherboard*, February 27, 2015, *available at* http://motherboard.vice.com/read/the-man-who-crafted-the-patriot-act-now-supports-your-right-to-encrypt-data.

[28] Philip Zimmerman, "Why I wrote PGP," June 1991, *available at* https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

[29] *See* Dan Froomkin and Natasha Vargas-Cooper, "The FBI Director's Evidence Against Encryption is Pathetic," *The Intercept*, October 17, 2014, *available at* https://firstlook.org/theintercept/2014/10/17/draft-two-cases-cited-fbi-dude-dumb-dumb/ ("In the three cases *The Intercept* was able to examine, cell-phone evidence had nothing to do

a real-world example where encryption actually stymied an investigation.[30] And in March he admitted to the House Appropriations Committee in March that he wasn't in a position to offer "a percentage or number" of cases affected by encrypted devices.[31] Meanwhile, in the realm of law enforcement wiretaps of phone and Internet communications, where numbers are available via annual reports by the Administrative Office of the U.S. Courts, the number of cases where encryption has posed a problem is miniscule. Specifically, according to the report issued in 2014, of the over 3,576 wiretaps conducted by federal and state law enforcement in 2013, encryption was encountered in only 41 cases, and the police were able to obtain the plain text of the encrypted communications in 32 of those 41 cases. [32] So, strong encryption posed a problem in only nine of 3,500 wiretaps, and that was a record high.

Indeed, rather than "going dark," there's good reason to believe that thanks to the growing role played by digital technology in nearly all aspects of our lives—and especially thanks to the prevalence of smartphones—law enforcement is in the midst of a "golden age of surveillance" where they can access more data about what we say, where we go, what we do, and with whom we associate and communicate than ever before.[33] Indeed, as a number of law enforcement and intelligence officials have acknowledged, metadata about private communications can be just as revealing if not more revealing than the contents of those messages themselves.[34] This golden

---

with the identification or capture of the culprits, and encryption would not remotely have been a factor."); Jack Gillum and Eric Tucker, "Do FBI's Examples Support Encryption Worries?", *Associated Press*, October 17, 2014, *available at* http://bigstory.ap.org/article/e03177df2c9a4e0ebe5b584c909218bf/do-cases-fbi-cites-support-encryption-worries (noting that although in one case, text messages on a phone helped secure a plea deal, "three other examples the FBI director has cited are not so cut and dry. They are cases in which the authorities were tipped off — or even solved the crime — through means other than examining data they took from victims or suspects."). Another example offered in an op-ed by a former FBI official, of a case where encryption would have purportedly prevented the rescue of a kidnapping victim, had to be corrected when it proved to be false. *See* Ronald T. Hosko, "Apple and Google's new encryption rules will make law enforcement's job much harder," *The Washington Post*, September 23, 2014, *available at* http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/ ("Editors note: This story incorrectly stated that Apple and Google's new encryption rules would have hindered law enforcement's ability to rescue the kidnap victim in Wake Forest, N.C. This is not the case. The piece has been corrected.").

[30] *See* C-SPAN, "Comey Flustered When Asked For Actual Real-Live Examples," October 16, 2014, *available at* http://www.c-span.org/video/?c4511673/comey-flustered-asked-actual-real-live-examples.

[31] "FBI Director Continues Crusade Against Encryption, Calls on Congress to Act," *The District Sentinel*, March 25, 2015, *available at* https://www.districtsentinel.com/fbi-director-continues-crusade-against-encryption-calls-on-congress-to-act/.

[32] *See* The Adminstrative Office of the U.S. Courts, "Wiretap Report 2013," *available at* http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx#sa9; *see also* Andy Greenberg, "Rising Use of Encryption Foiled the Cops a Record 9 Times in 2013," *Wired*, July 2, 2014, *available at* http://www.wired.com/2014/07/rising-use-of-encryption-foiled-the-cops-a-record-9-times-in-2013/ ("'So the cryptapocalypse they warned us about in the 90's has come to pass,' University of Pennsylvania computer science professor Matt Blaze noted drily on twitter. 'Strong crypto used in a whopping 0.25% of wiretaps last year.'").

[33] "Consider three areas where law enforcement has far greater capabilities than ever before: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create 'digital dossiers' about individuals' lives." Peter Swire, "'Going Dark' Versus a 'Golden Age for Surveillance," *Center for Democracy & Technology*, November 28, 2011, *available at* https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/; *see also* Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. 335 (2014), *available at* http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones (describing the rapidly declining cost of location tracking by law enforcement).

[34] As former NSA general counsel Stewart Baker put it, "Metadata absolutely tells you everything about somebody's life…. If you have enough metadata you don't really need content…. [It's] sort of embarrassing how predictable we

age of surveillance promises to get even brighter for law enforcement with the rise of the so-called "Internet of Things", where fine-grained data about everything from our electricity consumption to the contents of our refrigerators to the behavior of our medical implants will be available to prosecutors.[35]

Meanwhile, much of the data stored on the encrypted Apple and Android cellphones that have caused so much concern are also backed up to Apple and Google servers in the Internet "cloud" and available via legal process served on those companies.[36] That which is not available via the cloud will in many cases be obtainable simply by having a court compel the suspect to hand over the data or else face jail time for contempt.[37] And for cases where notice to the suspect is not desirable, encrypted data or communications that cannot be obtained from the cloud might even be obtained by government investigators secretly hacking into suspects' devices from afar over the Internet, a law enforcement technique that is worrisomely on the rise despite constitutional concerns.[38]

With few examples of encryption posing a serious challenge for law enforcement, and a wide variety of other ways for law enforcement to obtain a wide variety of information from or about suspects, the necessity of encryption backdoors to better combat crime is unclear at best. What is absolutely clear, however, is a fact that Representative Bob Goodlatte attested to back in 1997:

> Strong encryption *prevents* crime. 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. The blue-ribbon National Research Council said it best, concluding that strong encryption supports both law enforcement efforts and our national security, while protecting the proprietary information of U.S. businesses.[39]

---

are as human beings." Alan Rusbridger, "The Snowden Leaks and the Public," *New York Review of Books*, November 21, 2013, *available at* http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/. Former NSA director Michael Hayden agrees: "[Baker's comment was] absolutely correct… We kill people based on metadata." David Cole, "We Kill People Based on Metadata," *New York Review of Books*, May 10, 2014, *available at* http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/.

[35] Bruce Schneier, "Will giving the Internet eyes and ears mean the end of privacy?" *The Guardian*, May 16, 2013, *available at* http://www.theguardian.com/technology/2013/may/16/internet-of-things-privacy-google; Mike Wheatley, "Big Brother's Big Data: Why We Must Fear the Internet of Things," *Silicon Angle*, January 10, 2013, *available at* http://siliconangle.com/blog/2013/01/10/big-brothers-big-data-why-we-must-fear-the-internet-of-things/.

[36] Micah Lee, "Apple Still Has Plenty of Your Data for the Feds," *The Intercept*, February 22, 2014, *available at* https://firstlook.org/theintercept/2014/09/22/apple-data/.

[37] Andy Greenberg, "Google and Apple Won't Unlock Your Phone, But a Court Can Make You Do It," *Wired*, September 22, 2014, *available at* http://www.wired.com/2014/09/google-apple-wont-unlock-phone-court-can-make/.

[38] Fed. Jud. Center, *Public Hearing on Proposed Amendments to the Federal Rules of Criminal Procedure* 34–40 (Nov. 5, 2014) (testimony of Kevin S. Bankston), available at http://www.newamerica.org/downloads/OTI_Rule_41_Testimony_11-05-14_final.pdf (summarizing constitutional concerns).

[39] Bob Goodlatte, "Let's Open Up Encryption," *The Washington Post*, June 12, 1997, *available at* http://www.washingtonpost.com/wp-srv/politics/special/encryption/stories/ocr061297.htm (emphasis added), citing Dam and Lin, *supra* note 9.

It is even more true now than it was nearly twenty years ago: encryption makes us all safer,[40] and default encryption on smartphones especially so. 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.[41] The vast amount of personal information on those devices makes them especially attractive targets for criminals aiming to commit identify theft or other crimes of fraud, or even to commit violent crimes or further acts of theft against the phone's owner.Yet over a third of consumers fail to activate even the simplest security mechanisms on their mobile devices.[42] That is why the FBI itself used to advise consumers with smartphones to turn their encryption on—until abruptly changing course and deleting that advice from its website last month.[43] By taking this step for their customers and turning on encryption by default, mobile operating system vendors have completely eliminated the risk of those crimes occurring, significantly discouraged thieves from bothering to steal smartphones in the first place, and ensured that those phones' contents will remain secure even if they are stolen. A necessary consequence, of course, is that the contents will also remain secure if the phone is seized by law enforcement.

6. It would undermine and turn on its head the Fourth Amendment right to be secure in our papers and effects.

The Fourth Amendment gives individuals the right to be secure in their papers and effects, prohibiting unreasonable searches and seizures and requiring that any warrant authorizing such a government invasion be issued by a court based on a showing of probable cause.[44] As indicated by recent Supreme Court cases, the need for vigorous enforcement of that right has become even more acute in the context of powerful digital technologies. Most recently, a unanimous Supreme Court in the case of *Riley v. California* decided to require warrants for the search of a cellphone in the possession of an arrestee, based on the unprecedented amount of private data that may be stored on such devices even though such searches incident to arrest have traditionally been allowed without a warrant.[45] As the Court explained, many cell phones "are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries,

[40] Nuala O'Connor, "Encryption Makes Us All Safer" *Center for Democracy & Technology*, October 8, 2014, *available at* https://cdt.org/blog/encryption-makes-us-all-safer/.
[41] "Smart phone thefts rose to 3.1 million last year, Consumer Reports finds," *ConsumerReports.org*, May 28, 2014, *available at* http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.
[42] *Id*.
[43] The FBI previously included the following recommendation in a consumer safety guide on its website: "Depending on the type of phone, the operating system may have encryption available. This can be used to protect the user's personal data in the case of loss or theft." *See* Mike Masnick, "FBI Quietly Removes Recommendation To Encrypt Your Phone... As FBI Director Warns How Encryption Will Lead To Tears," Techdirt, March 26, 2015, *available at* https://www.techdirt.com/articles/20150325/17430330432/fbi-quietly-removes-recommendation-to-encrypt-your-phone-as-fbi-director-warns-how-encryption-will-lead-to-tears.shtml. However, the same advice is still available via a separate FBI press release, "Smartphone Users Should be Aware of Malware Targeting Mobile Devices and the Safety Measures to Help Avoid Compromise," October 22, 2012, *available at* http://www.fbi.gov/sandiego/press-releases/2012/smartphone-users-should-be-aware-of-malware-targeting-mobile-devices-and-the-safety-measures-to-help-avoid-compromise.
[44] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.
[45] *Riley v. California*, 134 S. Ct. 2473, 2485 (U.S. 2014).

albums, televisions, maps, or newspapers."[46] These devices, with "immense storage capacity," can hold "every picture [their users] have taken, or every book or article they have read," and "even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on."[47] Ultimately, as the Supreme Court explicitly held, the search of a modern electronic device such as a smartphone or a computer is more privacy invasive than even "the most exhaustive search of a house."[48]

As the Court concluded in *Riley*, "We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost."[49] The court did not pretend that requiring warrants for searches of cellphones seized incident to arrest did not risk diminishing law enforcement's effectiveness—it simply recognized that allowing such warrantless searches posed an even greater risk to our Fourth Amendment rights considering the scope of data available on those phones. The court made a similar calculus in the 2012 case of *U.S. v. Jones* when it decided that the comprehensive long-term tracking of a car's movements on public roads using GPS technology constituted a search under the Fourth Amendment, even though tracking that only reveals information that would have been visible from public space would not traditionally be considered to violate a suspect's Fourth Amendment-based reasonable expectation of privacy.[50] Both the *Jones* and *Riley* cases can be viewed as the Court's attempt to compensate for the sharp increase in the government's surveillance capabilities thanks to digital technology by ratcheting up legal protections against government searches.[51] The use of encryption on cellphones can be seen as a similar means of compensating for the government's newfound technical powers during this "golden age of surveillance," using technology instead of the law to help restore the balance between government power and individual power to something closer to what the Founding Fathers intended.

Encryption opponents would push in the other direction and flip our Fourth Amendment rights on their head by instead casting the Fourth Amendment as a right of the government—a right to dictate that the contours of the physical and digital worlds be redesigned to facilitate even easier surveillance.[52] But there is no precedent for such a reading of the Fourth Amendment. As former computer crime prosecutor Marc Zwillinger recently put it,

---

[46] *Id.* at 2489.
[47] *Id.*
[48] *Id*. at 2491.
[49] *Id.* at 2493.
[50] See *United States v. Jones*, 132 S. Ct. 945, 955-57 (2012) (Sotomayor, J., concurring), 957-963 (Alito, J., Ginsburg, J., Breyer, J., and Kagan, J., concurring).
[51] *See generally* Bankston & Soltani, *supra* note 33.
[52] James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *Remarks at the Brookings Institution*, October 16, 2014, *available at* http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (*e,g,*, encryption is "the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?"); Vance, *supra* note 3 (Vance, the Manhattan District Attorney, describing how Apple and Google's new features "push mobile devices beyond the reach of warrants and thus beyond the reach of government law enforcement. This would make mobile devices different from everything else. Even bank security boxes — the "gold standard" of the pre-digital age — have always been searchable pursuant to a judicial warrant.").

> I don't believe that law enforcement has an absolute right to gain access to every way in which two people may choose to communicate… And I don't think our Founding Fathers would think so, either. The fact that the Constitution offers a process for obtaining a search warrant where there is probable cause is not support for the notion that it should be illegal to make an unbreakable lock. These are two distinct concepts.[53]

Zwillinger's comments echoed those made by Senator John Ashcroft during the original Crypto Wars: "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?"[54] Or, as a more recent commentator put it:

> This argument [that encryption foils the police's right to obtain evidence with a search warrant] misunderstands the role of the search warrant. A search warrant allows police, with a judge's approval, to do something they're not normally allowed to do. It's an instrument of permission, not compulsion. If the cops get a warrant to search your house, you're obliged to do nothing except stay out of their way. You're not compelled to dump your underwear drawers onto your dining room table and slash open your mattress for them. And you're not placing yourself 'above the law' if you have a steel-reinforced door that doesn't yield to a battering ram.[55]

The law has never prohibited the creation of unbreakable locks, nor required us to hand our keys over to the government just in case it might need them for an investigation, whether those keys are physical or digital. Indeed, the Founders themselves used ciphers to communicate with each other,[56] and presumably would have viewed a demand that they hand over the key to their encryption scheme as abhorrent to their rights—not only their Fourth Amendment right against government intrusion but also their First Amendment right to speak and associate both freely and anonymously.

7. It would threaten First Amendment rights here and free expression around the world.

Repeated court challenges to export controls on encryption during the Crypto Wars illustrate how any attempt by the government to limit the distribution of encryption software code, which is itself speech, would raise serious First Amendment concerns. As one federal district court held when considering a First Amendment challenge to 90s-era encryption export controls,

---

[53] *See* Nakashima and Gellman, *supra* note 17.
[54] John Ashcroft, *Keep Big Brother's Hands Off the Internet* (1997), *available at* http://rense.com/general31/keepbigbrothershands.htm.
[55] Kevin Poulsen, "Apple's iPhone Encryption is a Godsend, Even if Cops Hate It," *Wired*, October 8, 2014, *available at* http://www.wired.com/2014/10/golden-key/.
[56] *See* "Thomas Jefferson Used Encryption," *Laissez Faire*, September 1, 2012, *available at* https://lfb.org/thomas-jefferson-used-encryption/ (describing how James Madison, Thomas Jefferson and James Monroe correspondence in code to protect against the U.S. government reading their letters). The Jefferson's Wheel Cipher remained immune from attacks for over 150 years, gaining Thomas Jefferson the title "Founder of American Cryptography." Alexander Stanoyevitch, *Introduction to Cryptography with Mathematical Foundations and Computer Implementations* 107 (2010).

> This court can find no meaningful difference between computer language…and German or French. All participate in a complex system of understood meanings within specific communities {in this case, that of programmers and mathematicians}.... Contrary to defendants' suggestion, the functionality of language does not make it any less like speech.... Instructions, do-it-yourself manuals, recipes, even technical information about hydrogen bomb construction, are often purely functional; they are also speech.[57]

The Ninth Circuit Court of Appeals agreed, holding that the challenged encryption export regulations constituted a prior restraint on speech that offends the First Amendment. [58] Therefore, not only would attempting to police the distribution of strong encryption code inside the United States require an endless and ineffective game of Internet whack-a-mole as old and new encryption code proliferated across cyberspace, but the extensive censorship that would be necessary to fight that losing battle would also likely violate the freedom of speech. Similarly, a legal regime that forced individuals to cede their private encryption keys to the government or to their communications providers for law enforcement purposes would also raise novel issues of compelled speech under the First Amendment.

However, the free speech impact of a mandate against unbreakable encryption and in favor of backdoors for government would reach far beyond just the communication of encryption code, and chill a wide variety of online expression. When individuals believe that they may be under surveillance, there is a "chilling effect" that can curb free speech and the free flow of information online.[59] If individuals must assume that their online communications are not secure but may instead be acquired by the U.S. government or by anyone else who might exploit an encryption backdoor, they will be much less willing to communicate freely. By contrast, encouraging the availability of strong encryption free of surveillance backdoors can enable free expression both in the United States and around the world,[60] including by stymieing the censorship and surveillance efforts of governments with less respect for human rights than our own.

8. It would encourage countries with poor human rights records to demand backdoor access of their own.

The governments of countries like China, [61] India, [62] and the United Arab Emirates[63] have proposed a variety of measures that would require companies to implement key escrow systems

[57] *Bernstein v. U.S. Dept. of State*, 922 F.Supp 1426, 1431 (N.D. Cal. 1996).
[58] *See Bernstein v. United States Dept. of Justice*, 176 F.3d 1132 (9th Cir. 1999).
[59] A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Penn. L. Rev. 709, 815-822 (1995) (discussing "Chilling Effect on Speech" and "Anonymity and the Freedom of Association"); Human Rights Watch & The American Civil Liberties Union, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy* (2014), *available at* https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf.
[60] *See* Kehl et al., *supra* note 4.
[61] In February 2015, China put forth a proposal that would require tech companies operating in the country — including American companies — to provide them with copies of encryption keys and other means to defeat security measures. The United States government sent a letter objecting to the measure, and U.S. Trade Representative Michael Froman said that "[t]he Administration is aggressively working to have China walk back from these troubling regulations." Quoted in Lorenzo Franceschi-Bicchierai, "The United States Is Angry That China Wants Crypto Backdoors, Too," *Motherboard*, February 27, 2015, *available at* http://motherboard.vice.com/read/the-united-states-is-angry-that-china-wants-crypto-backdoors-too.

or other forms of backdoors or stop doing business in those countries, proposals that the United States government has criticized.[64] Yet how can the United States credibly criticize, for example, the Chinese government for proposing an anti-terrorism bill that would require U.S. companies to hand over their encryption keys, if we impose a similar requirement here at home? And how are U.S. companies to argue that they cannot implement such requirements and hand over the keys to foreign governments—even those with a history of human rights abuses—if they have already had to do so for the U.S. government?

As Marc Zwillinger has pointed out, if the U.S. mandates backdoor access to encrypted data, "multinational companies will not be able to refuse foreign governments that demand [the same] access. Governments could threaten financial sanctions, asset seizures, imprisonment of employees and prohibition against a company's services in their countries. Consider China, where U.S. companies must comply with government demands in order to do business."[65] Such a result would be particularly ironic considering the U.S.'s foreign policy goal of promoting Internet Freedom worldwide and in China especially, including the promotion of encryption-based tools to protect privacy and evade censorship.[66]

Internet Freedom begins at home, and a failure by the United States to protect Americans' ability to encrypt their data will undermine the right to encrypt and therefore human rights around the world.[67] The U.S. government supports the use of strong encryption abroad as part of our foreign policy objectives, and it should support the same for Americans here in the United States. This is especially true considering that…

---

[62] Anandita Singh Mankotia, "Government, BlackBerry dispute ends," *Times of India*, July 10, 2013, http://timesofindia.indiatimes.com/tech/tech-news/telecom/Government-BlackBerry-dispute-ends/articleshow/20998679.cms.

[63] In 2010, United Arab Emirates, citing encryption concerns, threatened to suspend Blackberry mobile services (including email and text messaging) because of the strong encryption Blackberry used. (Barry Meier and Robert F. Worth, "Emirates to Cut Data Services of BlackBerry," *The New York Times*, August 1, 2010, *available at* http://www.nytimes.com/2010/08/02/business/global/02berry.html.)

[64] *See, e.g.,* Jeff Mason, "Exclusive: Obama sharply criticizes China's plans for new technology rules," *Reuters*, March 2, 2015, *available at* http://www.reuters.com/article/2015/03/02/us-usa-obama-china-idUSKBN0LY2H520150302 (Says President Obama, "Those kinds of restrictive practices I think would ironically hurt the Chinese economy over the long term because I don't think there is any U.S. or European firm, any international firm, that could credibly get away with that wholesale turning over of data, personal data, over to a government.").

[65] *See* Marc Zwillinger, "Should Law Enforcement Have the Ability to Access Encrypted Communications? NO: It Violates Our Rights—Without Improving Security," *The Wall Street Journal*, April 19, 2015, *available at* http://www.wsj.com/article_email/should-law-enforcement-have-the-ability-to-access-encrypted-communications-1429499474-lMyQjAxMTE1NjI5MDMyMzA2Wj.

[66] Since 2009, the American government has invested over $125 million in programs to support Internet Freedom abroad, including "work to support counter-censorship and secure communications technology," much of which relies on encryption. Scott Busby, "10 Things You Need to Know About U.S. Support for Internet Freedom," *IIP Digital*, May 29, 2014, *available at* http://iipdigital.usembassy.gov/st/english/article/2014/05/20140530300596.html#axzz32vEtH3C9.

[67] Cynthia Wong, "Global Internet Freedom Begins at Home," *Index on Censorship*, June 21, 2011, *available at* https://www.indexoncensorship.org/2011/06/global-internet-freedom-begins-at-home/. ("As the US government debates emerging internet policy challenges, it must face an inconvenient truth: the US is often viewed as the standard bearer for many (though not all) aspects of internet regulation and its laws can and will have an effect far beyond American borders.")

9. An overwhelming majority of the House of Representatives and the President's own hand-picked advisors have already rejected the idea.

Echoing the House's overwhelming support for the SAFE Act during the Crypto Wars of the 90s, an overwhelming and bipartisan majority of the House of Representatives already rejected the idea of encryption backdoors just last year. [68] That's when, by a vote of 293 to 123,[69] the House approved the Sensenbrenner-Massie-Lofgren amendment to the Defense Appropriations Act, H.R. 4870. That amendment, responding to reports of that the NSA had worked to insert surveillance backdoors into a variety of hardware and software products, would have prohibited the NSA or the CIA from using any funds "to mandate or request that a person…alter its product or service to permit the electronic surveillance…of any user of said product or service for said agencies."[70] Although the amendment, which was supported by a quickly organized activist campaign[71] and a broad coalition of Internet companies and civil society organizations like Google and the American Civil Liberties Union,[72] did not make it into the final "CRomnibus" spending bill,[73] it was still a potent indicator that Congress is skeptical of U.S. government efforts that would weaken the security of American hardware and software products.

Equally skeptical of encryption backdoors were the five experts hand-picked by the President to review the NSA's surveillance activities. Echoing the conclusions of the National Academies in their groundbreaking study from 1997, the final report of the President's Review Group on Intelligence and Communications Technologies included this strongly worded recommendation prompted by its conclusion that strong encryption was necessary to the United States' national and economic security:

> **Recommendation 29**
> We recommend that, regarding encryption, the US Government should:
> (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.[74]

---

[68] Ellen Nakashima and Andrea Peterson, "House votes to curb NSA "backdoor" U.S. data searches," *The Washington Post,* June 20, 2014, *available at* http://www.washingtonpost.com/world/national-security/house-votes-to-curb-nsa-backdoor-us-data-searches/2014/06/20/54aacd28-f882-11e3-a3a5-42be35962a52_story.html

[69] The final vote count is *available at* http://clerk.house.gov/evs/2014/roll327.xml.

[70] Text of the amendment is *available at* https://www.eff.org/document/sensenbrenner-massie-lofgren-amendment-2014.

[71] *See* "Shut the NSA's Backdoor to the Internet," *available at* https://shutthebackdoor.net/.

[72] *See* "OTI Joins With Privacy Groups and Tech Companies To Tell Congress: End the NSA's Backdoor Access to Internet Users' Data," *New America's Open Technology Institute*, June 18, 2014, *available at* http://newamerica.net/node/114440.

[73] Sean Vitka, "This Meaningful Surveillance Reform Had Bipartisan Support. It Failed Anyway." *Slate*, December 10, 2014, *available at* http://www.slate.com/blogs/future_tense/2014/12/10/massie_lofgren_surveillance_reform_amendment_fails_despite_bipartisan_support.html.

[74] "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," December 12, 2013, at p. 36, *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Therefore, not only the House of Representatives but a blue-ribbon panel of experts including a former CIA Director and the White House's former anti-terrorism czar, have already concluded: mandating or even requesting the insertion of encryption backdoors into U.S. companies' products and services is a bad idea. As demonstrated by their support for the Sensenbrenner-Massie-Lofgren amendment, the Internet industry and the Internet activists agree, which is why…

10. It would be vigorously opposed by a unified Internet community.

Decades before the massive online advocacy campaign that stopped the SOPA and PIPA copyright bills in 2012,[75] The Crypto Wars—and, in particular, the battle against the Clipper Chip—represented the Internet community's first major political engagement. And it was a rousing success. An unprecedented alliance of Internet users, technologists, academics, the technology industry, and newly-emerging Internet rights advocacy organizations like the Electronic Frontier Foundation, the Center for Democracy and Technology, and the Electronic Privacy Information Center, flexed its muscles for the first time and made a huge difference in the political process. They organized experts to speak on panels, testified before Congress, and circulated electronic petitions, including one that got over 50,000 signatures — an extraordinary number in the early days of Internet activism.[76] That Internet community, which won the first Crypto Wars two decades ago and more recently blocked SOPA and PIPA, has only grown larger and more vocal in the intervening years, and will certainly make its voice heard if another round of Crypto Wars were to begin now.

That conflict can be avoided, however. Especially considering all of the above arguments, many of which are just as true if not moreso than they were twenty years ago, Congress can and should leave the idea of encryption backdoors in the dustbin of history where it belongs. Instead, policymakers should heed the lessons of the past and the advice of the President's Review Group by considering policies that will promote rather than undermine the widespread use of strong encryption and thereby help guarantee a more secure and prosperous future for America.

Thank you, and I welcome your questions on this important matter.

[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), *available at* http://shop.fightforthefuture.org/products/on-internet-freedom-by-marvin-ammori.

[76] Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip* 34 (1997).