Technology's Stories
Vol. 7, no. 1 March 2019

Regulating Contested Reality: The Failure of U.S. Encryption Regulations

Jillian Foley* DOI: 10.15763/jou.ts.2019.03.13.03

Technology regulations, at their core, are based on an idea of what a technology does or what its uses are. Of course, these ideas and the resulting regulations are the product of negotiations, conflicts, and compromises between different people with different stakes. What happens to regulation when people can't even agree on what the technology is?

For the past forty years, academic computer scientists, industry professionals, and government bureaucrats have been fighting over limiting cryptography in the United States.[1] Cryptography—the creation and use of ciphers to disguise communication in plain sight—has become essential to the modern world since the advent of personal computers and the Internet.[2]

Because of the continuing lack of political consensus on this issue, the grounds of debate have shifted from ordinary political conflicts in the mid-1970s to mathematical and engineering conflicts. The U.S. government has tried a variety of different regulatory

---

[1] Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, et al., "Keys Under Doormats," *Communications of the ACM* 58, no. 10 (28 September 2015): 24–26.

[2] Andi Wilson Thompson, Danielle Kehl, and Kevin Bankston, "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," Open Technology Institute, June 2015, https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf.

ISSN 2572-3413 doi:10.15763/jou.ts.2019.03.13.03

tactics, which have mostly fallen under the pressure of public opinion and new technology. With the regulatory arsenal increasingly depleted, the debate about encryption has morphed and shifted until finally, technological reality itself has become fair game.

As former FBI director James Comey put it in 2015, the agency's problem with encryption is "really not a technological problem . . . it's a business model question."[3] In 2017, the Prime Minister of Australia, talking about a law that would require encryption backdoors declared that "the laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia."[4] That law passed at the end of last year.

In the United States, there were effectively no controls on encryption before the 1970s because few people outside of the government used encryption regularly, and no explicit controls were necessary.[5] Existing International Traffic in Arms Regulations (ITAR) applied to exports of cryptosystems as a military technology, but before cryptography became part of computer networks, nobody really noticed. Who would use or export a cryptosystem, besides the military, or perhaps very secretive corporations?

[3] U.S. Congress, Senate, Committee on the Judiciary, *Oversight of the Federal Bureau of Investigation*, 114th Cong., 1st sess., 9 December 2015.
[4] Rachel Roberts, "Prime Minister Claims Laws of Mathematics 'Do Not Apply' in Australia," *Independent*, 15 July 2017, www.independent.co.uk/news/malcolm-turnbull-prime-minister-laws-of-mathematics-do-not-apply-australia-encryption-l-a7842946.html.
[5] B. R. Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector," *Cryptologia* 3, no. 3 (1979): 130.

Headquarters of the National Security Agency (NSA). (Source: Image in the Public Domain.)

But rapid advances in computing technology throughout the 1950s and 1960s made it easier to implement advanced cryptosystems that previously would have been impossible by hand or by rotor machine—the previous state-of-the-art in encryption techniques. By the 1970s, tech-savvy American businesses had seen the economic potential of networked computers. A handful of academic mathematicians and engineers latched onto this synergy of new technology and new demand and started researching cryptography in earnest.[6] The NSA, and later the FBI, scrambled to get authority to control the spread of cryptographic research and technology, sparking the half-century of regulatory fights. But by the turn of the millennium, the Clinton administration had relaxed export controls on encryption and dropped its push for controlling domestic encryption. Many thought the so-called Crypto Wars had been won.[7]

---

[6] Gina Bari Kolata, "Trial-and-Error Game That Puzzles Fast Computers," *Smithsonian*, October 1979, 90–96.

[7] Steven Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age* (New York: Penguin Publishing Group, 2001).

Given the resurgence of this debate in the past few years, not just in the United States but in allied countries around the world, it's important to understand how past debates shifted the political landscape surrounding encryption. Regardless of your own political beliefs about proper regulation, there is no way we can achieve political consensus on this by repeating the ineffective debates of the past.

* * *

Before the 1970s, cryptography had been an obscure field, pursued by government spies in secret—a monopoly in practice if not in law. But as computers began to spread among universities, banks, and other large companies, the need to keep information confidential pulled cryptography out of the shadows. The U.S. government, by way of the National Bureau of Standards, announced its first public encryption standard in 1976, called the Data Encryption Standard (DES), intended to protect government communications that didn't warrant the protection of top-secret ciphers. NBS also intended DES to be used by American companies, so the agency made the algorithm public.[8]

At around the same time, academic researchers in mathematics, electrical engineering, and computer science started working on cryptography—an unheard-of topic of academic study before then—and made important discoveries that eventually enabled todays' secure internet.[9]

The NSA was not thrilled with these academic developments. Martin Hellman, one of the leading academic cryptographers of the day, later described the agency's response as "apoplectic."[10] Agency leaders tried to tamp down on this new research that challenged their cryptographic supremacy—without much success.

The civilian cryptographers, as Hellman put it, "realized that we had a political problem on our hands…no amount of technical arguing was going to make any

[8] David Kahn, "Cryptology Goes Public," *Foreign Affairs* 58, no. 1 (1979): 141–59.
[9] Perhaps the most important such example is Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* 22, no. 6 (1976): 644–54.
[10] Oral history interview with Martin Hellman, 2004, Charles Babbage Institute, retrieved from the University of Minnesota Digital Conservancy, http://hdl.handle.net/11299/107353, 30.

difference."[11] They brought their concerns about the NSA's involvement in DES and restrictions on publication to the press, where they received a "ground swell of support" for protecting free-speech rights.[12]

Unlike their counterparts in atomic weapons research, the NSA had no legislative foundation for demanding research restrictions, which made it nearly impossible for the agency to stand up against the public outcry about the first amendment. "While some people outside NSA express concern that the government has too much power to control nongovernmental cryptologic activities," said then-NSA director Admiral Bobby Inman in an unprecedented public address, "in candor, my concern is that the government has too little."[13] He wasn't able to change that fact. By 1980, the Justice Department concluded that the few regulations on the books—like ITAR—were unconstitutional when applied to publications.[14] After a few years of remarkably public political battles about an obscure topic, the question of academic research into cryptography seemed to be settled, with freedom of speech tipping the scales in favor of the academics.[15]

But building and selling cryptosystems were more promising avenues for regulation. ITAR let the Department of Defense restrict exports of cryptographic devices. The Invention Secrecy Act allowed for domestic secrecy orders in response to dangerous patent applications like those for cryptosystems.[16] So the NSA, without its own regulatory powers, worked with Defense and the Patent Office to exert some control over what encryption technology went out into the world, at least commercially.[17]

NSA leadership had better success abandoning censorship and cooperating with academics. A study group of government, industry, and academic professionals agreed on a voluntary pre-publication review system, which Inman later held up as exemplary in

---

[11] Ibid., 37–38.
[12] Ibid.
[13] Inman, "The NSA Perspective on Telecommunications Protection," 134.
[14] U.S. Congress, House of Representatives. Subcommittee of the Committee on Government Operations, *The Government's Classification of Private Ideas*, 96th Cong., 2nd sess., 28 February, 20 March, 21 August 1980, 289.
[15] Oral history interview with Peter J. Denning, 2013, Charles Babbage Institute, retrieved from the University of Minnesota Digital Conservancy, http://hdl.handle.net/11299/156515, 64–65.
[16] Invention Secrecy Act, 35 U.S.C. chapter 17 (1951).
[17] Deborah Shapley, "DOD Vacillates on Wisconsin Cryptography Work," *Science* 201 (July 1978): 141.

a Congressional hearing, despite being much weaker than the mandatory prior review he originally wanted.[18] Of the entire twenty-plus-person study group, only one person did not agree with voluntary review. By 1982, twenty-five papers had been submitted to the NSA, without mishap.[19] The study group represented a shared technical understanding of cryptographic research at the time, within a structure of political compromise.

Notably, domestic law enforcement concerns did not appear *at all* in the discussions of this study group, in Congressional hearings, or public debate in the early 1980s. This can perhaps be explained by the technological limitations at the time, with the computing market—and thus encryption—still dominated by businesses, rather than individuals, and thus less of a threat to ordinary police investigations.[20]

Academics, free to publish their research as they saw fit, were mostly placated for the rest of the 1980s. Industry leaders, however, were not as happy with this new status quo. The export restrictions meant American tech companies had little incentive to develop strong encryption products they weren't able to sell internationally, and the Defense Department had no interest in relaxing these restrictions. As the Acting Deputy Undersecretary for Research and Engineering put it in a 1982 Congressional hearing, "We do not want to kill the goose that lays the golden eggs. We just don't want the eggs to fall into the wrong hands."[21]

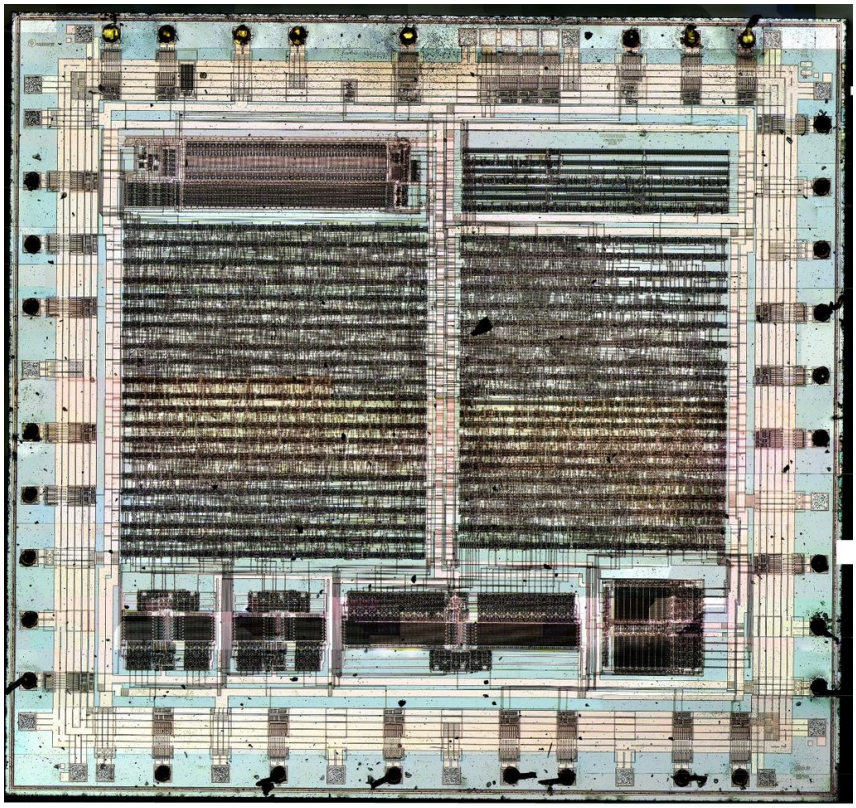
However, because ideas and publications couldn't be restricted, foreign companies could build their own versions of American-developed cryptosystems like DES. The Deputy Undersecretary's wrong goose just made its own golden eggs instead.[22]

---

[18] U.S. Congress, House of Representatives, Subcommittee on Science, Research and Technology and the Subcommittee on Investigations and Oversight of the Committee on Science and Technology, *Impact of National Security Considerations on Science and Technology,* 97th Cong., 2nd sess., 29 March 1982, 11.
[19] Ibid.
[20] Gerald Sturges, "The House Report on Public Cryptography," *Cryptologia* 5, no. 2 (1981): 84–93.
[21] U.S. Congress, House of Representatives, Subcommittee, *Impact of National Security Considerations on Science and Technology*, 21.
[22] Whitfield Diffie and Susan Landau, "The Export of Cryptography in the 20th and the 21st Centuries," *The History of Information Security: A Comprehensive Handbook*, ed. Karl De Leeuw and Jan Bergstra (Amsterdam: Elsevier Science, 2007), 725–36.

* * *

Bill Clinton's administration proposed a new encryption standard in 1993, the first example of which was a telecom encryption chip colloquially known as Clipper. Clipper was comprised of an encryption algorithm, developed in secret by the NSA, and a protocol for breaking an encryption key into two pieces, stored with two different government agencies. This allowed law enforcement to acquire electronic data—mostly wiretaps on encrypted phone lines—by obtaining and combining both pieces via warrant to unlock the data.[23]



Close-up of a Clipper Chip. (Source: Photograph by Travis Goodspeed, CC BY 2.0 License.)

Many supporters of digital liberties bristled at the idea of the government storing copies of encryption keys. Even in the days before the Snowden revelations, the NSA was not known for its respect of American citizens' privacy, with accusations as early as

[23] Dorothy E. Denning, "The Case for 'Clipper,'" *Technology Review* 98, no. 5 (July 1995): 48–55.

the 1970s that the agency was listening in on Americans' phone calls.[24] The spread of personal computing and telecom products by the 1990s had pulled domestic law enforcement into the fray, and activists also didn't like the idea of J. Edgar Hoover's lingering spirit gaining access to communication. Opposition was immediate and vociferous.[25]

Academic researchers were (and are) mostly opposed to key escrow as an inherent security flaw.[26] Even assuming the government were trustworthy, escrowing keys anywhere creates a target for hackers—go after one key, get them all. Security researchers also took issue with the secrecy of the underlying encryption algorithm used in the Clipper chip, which was kept under tight wraps by the NSA. Without transparency, they were unconvinced that the algorithm didn't have security flaws or an intentional back door. Martin Hellman described Clipper as "an unworkable proposal thrown together much too rapidly. The government was encouraging us to put all our eggs in the Clipper chip basket when it hadn't yet been woven."[27] The one big-name researcher who publicly supported Clipper, Dorothy Denning, "took a huge amount of heat for it."[28]

In a mirror image from the last decade, academics vehemently opposed the new proposal, while industry leaders supported it, agreeing to manufacture or sell Clipper-compatible products.[29] With government-escrowed keys, export restrictions could safely be eased, opening a new market to tech companies looking to expand their encryption offerings.

The Clipper debates in the press and in government hearings grew so heated that they triggered a backlash of articles that will be familiar to readers of today's news,

---

[24] Caitlin Dewey, "How the NSA spied on Americans before the Internet," *Washington Post*, 23 August 2013, www.washingtonpost.com/news/the-switch/wp/2013/08/23/how-the-nsa-spied-on-americans-before-the-internet/.
[25] Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests Over Lotus MarketPlace and the Clipper Chip* (New Haven: Yale University Press, 1997).
[26] Abelson et al., "Keys Under Doormats."
[27] Hellman Oral History, 47–48.
[28] Oral history interview with Dorothy E. Denning, 2013, Charles Babbage Institute, retrieved from the University of Minnesota Digital Conservancy, http://hdl.handle.net/11299/156519, 55.
[29] Susan Landau, Stephen Kent, Clint Brooks, Scott Charney, Dorothy Denning, Whitfield Diffie, Doug Miller, David Sobel, Anthony Lauck, and Peter Neumann, "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," *Report of a Special Panel of the ACM U.S. Public Policy Committee*, Association for Computing Machinery, 1994, 62.

claiming to cut through the politics and get to the facts. As we see today, this type of claim to have access to pure truth without the unnecessary rhetoric generally means there is actually a disagreement about facts, not just politics.

One of these, a policy piece commissioned by the Association of Computing Machinery, explicitly attempted to "present the issues carefully and correctly, removing rhetoric and replacing it with facts," based on technical analysis from well-known researchers.[30] The facts at hand were not just security vulnerabilities, but also the technological capabilities of law enforcement. Supporters of encryption accused the FBI of making a bad-faith argument about losing investigatory capabilities, setting up encryption as a straw man. The report stated that "despite the remarkable developments of cryptography, the communications *intelligence* products are now better than ever."[31]

Several policy scholars were so fed up by the back-and-forth that they wrote a piece to illustrate the overblown rhetoric. The piece was structured around a chart comparing how extreme the *proposed* cryptographic regulations were in comparison to the relatively tame *actual* regulations. A series of black dots connected by a line show completely steady domestic cryptography controls and even slowly relaxing export controls. Overlaid on top of this is a series of open dots, connected by a dashed line showing wild swings in proposed controls on both sides. The proposals demonstrated "a wide fluctuation that portrays the varied, and almost religious, convictions of their proponents"—hardly a sensible discussion of policy based on a shared understanding of technological reality.[32]

The outcry over Clipper meant it was never widely adopted. In 1994, an AT&T researcher discovered a vulnerability in the Clipper protocol, which drove the last nail in the coffin. President Clinton signed an executive order in 1996 that relaxed export controls by removing cryptography from the list of munitions. On top of that, new

[30] Ibid., iv.
[31] Ibid., 24.
[32] Kenneth A. Mendelson, Stephen T. Walker, and Joan D. Winston, "The Evolution of Recent Cryptographic Policy in the United States," *Cryptologia* 22, no. 3 (1998): 206.

products like the PGP encrypted email suite started to spread via the Internet. The Crypto Wars had been won, and free technology ruled. Right?[33]

* * *

Wrong. Cryptographer Peter Denning, husband to pro-Clipper Dorothy Denning, saw that in hindsight, "we diffused the [anti-encryption] argument back then [after Clipper], but didn't eliminate it; we never found a good solution to it."[34]

The rapid spread of cell phones, email, electronic banking, and other Internet-enabled technologies brought all of this back to the forefront. The NSA, as we know now from the Snowden revelations, pursued aggressive tactics to remain ahead of the technological curve, abandoning their earlier public regulatory lobbying in favor of shadier technology. The FBI is now the most vocal American champion of encryption regulations.[35]

Computer security expert Ross Anderson reflected on the cyclical nature of these debates in 2015, shortly after a think-tank session that featured Ed Snowden as a speaker.

> It struck me that the lawyers present, who were most of the audience, had forgotten all the arguments from the crypto wars . . . these issues tend to come up again and we face the same task that we did 20 years ago in educating lawyers, lawmakers, special advisors to ministers, and so on in terms of what's practical and what's plain stupid when it comes to defining the possible frontiers between technological innovation and sensible regulation.[36]

The biggest changes to this debate over the years have been the technological landscape itself and the failure of past attempts at regulation. Federal law enforcement officials belabor a concept they call "going dark," when everyone has such perfect

---

[33] Thompson et al., "Doomed to Repeat History?"
[34] Oral history interview with Peter J. Denning, 2013, Charles Babbage Institute, retrieved from the University of Minnesota Digital Conservancy, http://hdl.handle.net/11299/156515, 65.
[35] Russell Brandom, "Why the NSA is staying out of Apple's fight with the FBI," *The Verge*, 9 March 2019, www.theverge.com/2016/3/9/11186868/apple-fbi-nsa-encryption-exploit-hack.
[36] Oral history interview with Ross Anderson, 2015, Charles Babbage Institute, retrieved from the University of Minnesota Digital Conservancy, http://hdl.handle.net/11299/174607, 52.

encryption that they can no longer intercept or read any communications from any criminals, ever. However, the FBI has limited political opportunities to push for regulation, because the circuitous debates of the previous few decades eliminated most of their practical options.

So, instead of pushing for legal frameworks that have already crumpled under political pressure, the FBI now contests the technology itself. Then-Deputy Attorney General Sally Yates testified before Congress in 2015 that the Justice Department was "not seeking a frontdoor, backdoor or direct access, but just to work with industry to be able to respond to these [access] orders."[37] Cryptographers and security experts have long held that—especially in end-to-end encrypted systems where even the service provider doesn't have the encryption keys—any way to provide outside access is *by definition* a "backdoor." Regardless of what type of door you label it, the existence of an access point for responding to warrants is also an access point for malicious attackers or overreaching government surveillance.

Former Home Secretary Amber Rudd published an op-end in the *Telegraph* claiming the exclusivity of end-to-end encryption and law enforcement access "might be true in theory. But the reality is different."[38] Current FBI director Christopher Wray has embraced the same views in public. "The idea that we can't solve this problem as a society," he said this year, referring to secure law enforcement access, "I just don't buy it."[39] If Americans could land a man on the moon, he suggested, why not build a secure backdoor? Matt Blaze, the researcher who found the flaw in Clipper, railed against this particular comparison by likening it to saying, "If we can put a man on the moon, well surely we can put a man on the sun."[40]

---

[37] U.S. Congress, Senate, Committee on the Judiciary, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, 114th Cong., 1st sess., 8 July 2015.
[38] Amber Rudd, "We Don't Want to Ban Encryption, but Our Inability to See What Terrorists Are Plotting Undermines Our Security," *Telegraph*, 31 July 2017, www.telegraph.co.uk/news/2017/07/31/dont-want-ban-encryption-inability-see-terrorists-plotting-online/.
[39] "A Chat with the Director of the FBI," YouTube video, 57:54, posted by "The Aspen Institute," 18 July 2018, https://youtu.be/NoFqNFxBECU.
[40] "Encryption: Last Week Tonight with John Oliver (HBO)," YouTube video, 18:00, posted by "Last Week Tonight," 13 March 2017, https://youtu.be/zsjZ2r9Ygzw.

Though this resurgence of the Crypto Wars predates the current U.S. president and is not limited to the United States, the Trump administration's fondness for "alternative facts" and the longer political trend of disputing scientific consensus makes contesting technological reality politically appealing. Unable to gather a political will to enact regulations that failed in the past, the FBI and its allies instead challenge cryptographers on their own knowledge, accusing them of not trying hard enough. Meanwhile, security researchers working with the FBI on alternatives to back doors are essentially shunned.

I don't have any answers. I don't think *no* regulation is the answer any time people disagree. But clearly, when a political desire for technology regulation is stymied that political desire can respond by burrowing inside to challenge technological reality itself.