Research Note: Challenging the Crypto Wars Chronology

June, 2021

Abstract

The conflict over to what degree the state should have access to encrypted electronic communications, or put another way, to what degree citizens should be permitted privacy from the state in the digital age, is known as the crypto wars. This research note argues that a new chronology is needed to account for the full duration of the crypto wars, and to expose the policy contestation for the 27 years preceding 1993, when most consider the crypto wars to have commenced. This note posits that three, rather than the traditional framing of two, crypto wars have occurred spanning 1966-1981, 1991-2002 and 2013 onwards.

Keywords

crypto wars; digital surveillance; digital privacy; cryptography; cyberspace policy

Author

Craig Jarvis, PhD Candidate at Royal Holloway, University of London.

LinkedIn: https://www.linkedin.com/in/craig-jarvis-283013126/

Introduction

Digital privacy, better phrased as privacy in the digital age, is achieved principally via digital security. When considering the base elements of digital security, Professor Keith Martin comments, "cryptography is pretty much the only game in town" (Martin, 2020, p. 2). Cryptography underpins modern societies by enabling digital privacy and by extension, global digital commerce. Yet, the current state of unregulated cryptography in the US was not a foregone conclusion, for generations the state and its citizens have battled over the degree to which digital privacy beyond the government's penetration should be permissible. Today, law enforcement does not consider the status quo tolerable as its use often hinders their access to suspect's data.[1] In 2020, two bills were introduced in Congress which could outlaw encryption which does not include a government access method (commonly referred to as a 'back door') (United States Congress, 2020; United States Senate, 2020). As society once again debates the issue of privacy in the digital age it is vital we have a comprehensive understanding of the previous crypto wars, yet the history of the conflict has received little scholarly attention. In particular, many narratives eschew crypto war events before the Clinton administration's 1993 key escrow policy.[2] Those who fail to recognize events before 1993 include academics, journalists, supra-national bodies, NGOs, and even some crypto wars participants.[3] This myopic reading of history discounts the preceding 27 years of policy contestation, contestation which helped shape the status quo of civil liberties in today's societies. This research note argues the crypto wars should be divided into three, rather than two, conflicts, to allow the development of a comprehensive history, and offers a high-level chronology of the battles within each conflict.

[1] For instance, in 2016 the FBI took Apple to court when they refused to aid FBI attempts to unlock a terrorist suspect's iPhone. The judge rule in Apples favour. (Orenstein, 2016).
[2] For instance, see Kehl, Wilson, and Bankston, 2015; key escrow was a policy whereby the government would retain a copy of citizen's encryption keys which could be used to access their communications upon receipt of a judicial warrant.
[3] For instance, see: Meinrath & Vitka, 2014; Schneier, 2015; Levy, 2016; Oberhaus, 2016; Privacy International, 2018; Rozenshtein, Varia, and Wright, 2018; Soesanto, 2018.

Literature Review

Literature on the crypto wars is sparse. Whilst the most high-profile individual episodes of the conflict, such as the key escrow policy, have received some coverage the majority of the history has been neglected by scholars.[4] Previous research focusing on the use of encryption to enable civil liberties in the digital realm resides within legal scholarship.[5] Consideration is primarily framed around the first and fourth amendments in an effort to understand to what degree the US Constitution can be interpreted as providing protection for digital privacy and freedom of speech. The most extensive analyses of the crypto wars are found within popular literature, with Steven Levy's 2001 *Crypto* being the only attempt to chronicle the full history of the conflict. Simon Singh's 2002 *The Code Book* dedicates some coverage to the crypto wars, though the earliest activities of the crypto wars, much of remained classified at time of Singh's publication, were not acknowledged as a distinct era.[6]

Privacy in the digital age as a broader topic is starting to receive more attention with a number of books, such as Neil Richard's *Intellectual Privacy* explores how we protect civil liberties in digitally infused societies. Shoshana Zuboff's *The Age of Surveillance Capitalism* examines the issue of digital privacy with an economic and philosophical lens. Neither Richards nor Zuboff focus attention on the crypto wars and its chronological framing.

[4] See Frye and Sabett, 1998; Froomkin, 1995.
[5] See Barrett, 1998; Couillard, 2009; Edgett, 2003; Forest, 2000; Fraser, 1997; Koffsky, 1994; Lennon, 1994; Murr, 1997; Simmons, 2007.
[6] For instance, NSA did not declassify their data encryption standard history until 2011 (Juels et al., 2011)

Materials & Methods

This study is the output of a five-year research project to chronicle the crypto wars. Three groups of source data have been analyzed. Firstly, archival documents such as contemporary correspondence, meeting recordings, media coverage, and online posts. Secondly, government documents such as judicial outputs and declassified intelligence documents. Finally, engagement with those directly involved in the crypto wars, such as Bruce Schneier, RSA's Jim Bidzos, and the NSA's Richard 'Dickie' George.

Results & Discussion

Delineation points for any historical phase are highly subjective, the crypto wars especially so as the militant language calls into question what actions constitute a 'war' in this context.[7] For instance, some consider the government's key escrow (Clipper Chip) and the public response to constitute the entirety of the 1990s crypto war.[8] However, a more detailed examination of the period shows a number of separate incidents which in aggregate contributed to the eventual outcome of the war (the relaxation of export regulations) (United States Department of Commerce, 2000). Within the more than fifty year history of the crypto wars there was seldom a period when some degree of policy contestation was not occurring, sometimes these debates were internal to government (e.g. Commerce vs State), or isolated public events which were not critical to the history (such as John Gilmore undermining the NSA voluntary review system [Gilmore, 1989]). This study demarcates its timeline using those events which were crucial to the eventual outcome of each particular war, and around contestation between citizen and state.

[7] Whilst out of scope of this article, the crypto 'wars' are of course not warfare in the traditional sense as perhaps best defined by nineteenth century Prussian philosopher of war General Carl Von Clausewitz who argued warfare comprised three elements: use of (violent) force; instrumental to achieving objectives; political in nature. (Clausewitz, 1909). The crypto wars do not meet these three criteria.

[8] For instance, see Kehl, Wilson, and Bankston, 2015.

Crypto War 1 (1966 – 1981)

Conflict

CW1 was fought over the public's desire to have a fully transparent process in creating encryption standards, indirectly this was also a conflict over whether the government should be afforded the possibility to weaken encryption algorithms to allow NSA access. The conflict was also to establish whether the public had a right to publish academic research absence government censorship.

Combatants

The government was represented by the National Bureau of Standards, and the National Security agency; the public by academic researchers and professors.

Catalyst

CW1 was initiated firstly by the NSA's attempt to censor David Kahn's book on cryptology. Whilst this incident was a public–government contestation of cryptology policy, it was the announcement of the first data encryption standard (DES), and academic researcher's fears that NSA had weakened the algorithm to allow state surveillance, which triggered CW1.

Conclusion

When the NSA and academics agreed a system of voluntary regulation of cryptology research papers.

Chronology

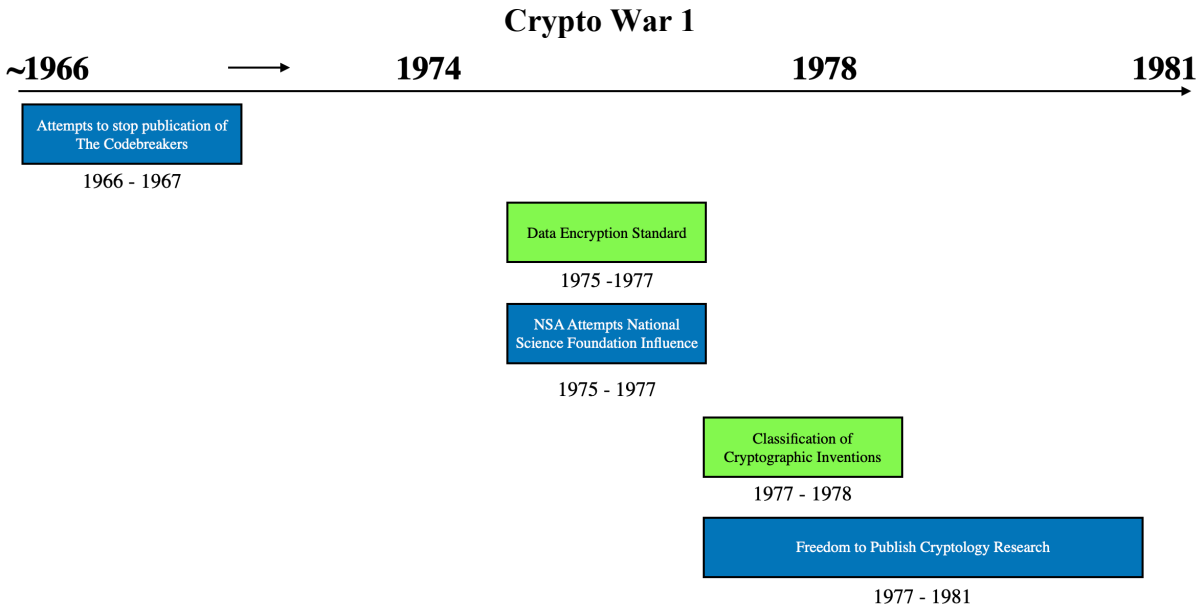

Figure 1: Crypto War 1

Attempts to stop publication of The Codebreakers (1966 – 1967): The earliest crypto wars action occurred in the mid-1960s when the U.S government attempted to prevent publication of David Kahn's The Codebreakers. The Codebreakers was the largest volume of cryptologic information ever compiled outside of classified environments (Friendly, 1967). Kahn was placed on the NSA's MINARET watch list allowing the government to intercept his calls and telegrams (Bamford, 1982, p. 169). Whilst covert measures to prevent publication were considered, the government settled on a subtler approach (Bamford, 1982, pp. 168-170). In 1966, the Defense Department informed Kahn's publisher, Macmillan, that they "deplored" the manuscript, and that, "it would not be in the national interest to publish the book." (Bamford, 1982, p. 170). NSA Director General Marshall S. Carter visited Macmillan to undermine Kahn's credentials:

> I pointed out that Kahn's reputation as a cryptologist was suspect; that he was an amateur; […] that the book […] was sufficiently wrong in sufficient areas to depreciate its validity as the final anthology of cryptology. (Bamford, 1982, p. 171)

Contractually, Macmillan could make no changes to the manuscript without Kahn's consent (Bamford, 1982, p. 171). Realizing Kahn would not remove large sections of the text, NSA

requested the omission of details regarding the NSA's close alliance with Britain's Government Communications Headquarters (GCHQ) (Bamford, 1982, p. 171). Kahn agreed (Bamford, 1982, p. 171). *The Codebreakers* became a best seller, inspired a generation of Cryptologists, and was nominated for the non-fiction Pulitzer prize (Macpherson, 1978; Hastedt, 2011, p. 430).[9]

DES (1975 – 1977)*:* In 1975 a DES was proposed (Federal Register, 1975). A government standard establishes rules to govern a type of activity.[10] Given US technological dominance, the world, with the exception of US adversaries, would also likely adopt DES.

As the National Bureau of Standards exposed the algorithm to public scrutiny there was significant concern that the NSA had weakened the algorithm so they could access any communications using the encryption scheme (Diffie, 1975; Diffie and Hellman, 1976). There were two public concerns. Firstly, that the key size had been reduced, weakening the encryption's strength making it vulnerable to exhaustive attacks, and secondly, code the NSA inserted (substitution boxes, or s-boxes) included a back door facilitating government access (Diffie 1975; Hellman et al,. 1976). The NSA denied the accusations (Inman, 1979, p. 129). Ultimately, DES was launched and became a widely adopted algorithm.

NSA attempts National Science Foundation (NSF) influence (1975 – 1977)*:* The NSA also explored whether they could control the dissemination of cryptology knowledge via the NSF. The NSF provided funding for cryptologic research. If the NSA could exert influence over the NSF, and have a clause inserted into contracts with NSF grant recipients that any resultant

[9] For instance, Diffie was inspired by *The Codebreakers* calling it his *Vedas* (Levy, 2001, Chapter 1).
[10] A government information technology standard is formally known as a Federal Information Processing Standard [FIPS].

inventions would be subject to NSA classification, the government could potentially control a large proportion of cryptologic research.

In April 1977, NSA's Assistant Deputy for Communications Security Cecil Corry met with NSF's Director Fred Weingarten (United States House of Representatives, 1980, p. 764). Corry informed Weingarten an unspecified Presidential Directive provided the NSA with "control" of all cryptologic work, and that in granting funding for research in this area the NSF were violating that directive (United States House of Representatives 1980, p. 764). Weingarten explained a similar claim had been made by a grant recipient several years earlier, and that both NSF and NSA lawyers were unable to locate such a directive (United States House of Representatives, 1980, p. 764). Weingarten agreed to send NSA copies of funding applications for their comment, but added that under no circumstances would the NSF take advice from the NSA should they make recommendations absent justifications - the NSF would not yield to advice such as, "[do not] fund this research, but we can not tell you why." (United States House of Representatives, 1980, p. 764). Had Weingarten taken the NSA's word regarding the presidential directive without challenge it is possible the agency may have gained control of academic cryptology.

***Classification of cryptographic inventions (1977 – 1978)**:* In the late 1970s the government used the Invention Secrecy Act (ISA) to classify two cryptographic technologies emerging from industry and academia. The first invention was created by Professor George Davida and David Wells of Wisconsin University, who created a product to apply a mathematical algorithm to output stream ciphers (Shapley, 1978b, p. 407). The second was created by Carl Nicolai, who created a "phasorphone", a voice scrambler allowing encryption of citizen band radios and telephones (Shapley, 1978, p. 141; Levy, 2001, Chapter 4). Werner Baum, a Wisconsin

University Chancellor, contacted *Science* magazine to publicize NSA's classification. Baum told *Science* magazine the government's approach was reminiscent of McCarthy era tactics against Universities, and challenged the constitutionality of the ISA, "How can some unknown bureaucrat classify an individual's research activity without any justification or due process?" he asked in the article (Shapley, 1978, p. 141). Both orders were rescinded following the media exposure.

***Freedom to publish cryptology research (1977 – 1981)**:* In July 1977, Joseph Meyer wrote to the Institute of Electrical and Electronics Engineers (IEEE) to warn their journals were, "publishing and exporting technical articles on […] cryptography - a technical field which is covered by Federal Regulations," Meyer cited the International Traffic in Arms Regulations (ITAR) legislation, which controlled items from atomic weapons to cryptography (Meyer, 1977). It was subsequently revealed Meyer was an NSA employee (Shapley and Kolata, 1977, p. 1345). Stanford University's Martin Hellman recounts whilst Meyer sent the letter from his home address, "portraying himself as a concerned citizen […] his attempt at intimidation had many hallmarks of NSA," such warning letters Hellman notes, "written from home addresses, pseudonyms, and similar subterfuges were in keeping with its [NSA's] *modus operandi*" (Hellman, 2013, p. 1). NSA later stated, and a subsequent Congressional inquiry assessed, that Meyer acted of his own volition rather than at his employer's behest (United States Senate, 1978, p. 4). However, Meyer's letter had serious implications. As the ITAR was vague, and NSA would not provide clear guidance on what would be considered export, the only way to establish the regulations' bounds was to test them in practice (Rivest, Shamir, and Adleman 1977; Levy, 2001, Chapter 4).

Hellman was scheduled to speak at the IEEE Symposium in New York on 10 October 1977, which would be attended by foreign delegates meaning his talk may be classed as an export of knowledge (Plutte, 2011, p. 6). Stanford's general council, John Schwartz, told Hellman he believed ITAR was too broad to be constitutional, but warned:

> the only way to settle this is in a court case. So if you're prosecuted, we will defend you. If you're convicted, we'll appeal. But again, I've got to warn you, if all appeals are exhausted, we can't go to jail for you. (Hellman and McGraw, 2016)

Following Meyer's letter MIT academics Ron Rivest, Adi Shamir and Leonard Adleman took advice from university lawyers regarding whether they could globally disseminate their research article which offered the first mathematical implementation of public key cryptography - the lawyers could not offer definitive legal answers, but believed a "published materials" exemption in the ITAR, whereby the materials in question were already in some form of circulation, permitted publication (Rivest, Shamir, and Adleman, 1977; Levy, 2001, Chapter 4; Legal Information Institute, n.d.). In December, MIT approved the article to be disseminated (Rivest, 2012, 25:33). The government took no action in response to Hellman, Rivest, Shamir and Adleman's actions.

In late 1977, NSA Director Inman briefly decided to pursue new regulations to control cryptography, however he subsequently recognized it was unlikely such legislation would pass given Congress' prevailing trade-friendly climate (Johnson, 1998). Instead, Inman decided negotiations with academia should be attempted in order to manage the emergence of non-governmental encryption.

In order to further the dialogue with cryptologists a Public Cryptography Study Group was convened comprising delegates from academia and government.[11] In 1981, the group accepted

[11] This name should not be confused with public-key cryptography, it is used in this application to denote that the public and government were involved in the study.

“as a working premise” that some cryptologic research ‘could be inimical to the national security’ (American Council on Education, 1981, p. 138). The group recommended a voluntary, “non-statutory [NSA review] system [be] designed to test on an ongoing basis Admiral Inman’s hypothesis, which depends for its success on the voluntary cooperation of those whom NSA might seek to regulate” (American Council on Education, 1981, pp. 138-139). A declassified NSA document reveals the system worked well and, "the committee requested very few changes to proposals, and most of these were easily accomplished” (Johnson, 1998, p. 238).

Crypto War 2 (1991 – 2002)

Conflict

The US government attempted to advocate a key escrow encryption system (Clipper), wherein the state would store a copy of citizen's decryption keys for use by law enforcement agents possessing judicial warrants. The government also attempted to maintain export controls on cryptographic technologies. The public argued for full deregulation of cryptography.

Combatants

The government was represented by the White House, and the FBI. The public were represented by the Cypherpunks, a group of digital activists focused on privacy, and digital non-governmental organizations led by the Electronic Frontier Foundation.

Catalyst

Senator (and later President) Joe Biden included language in a proposed bill arguing that plain-text should be made available to law enforcement when requested, essentially outlawing encryption that did not contain an government exceptional access mechanism.

Conclusion

Two events concluded CW2. Firstly, in 2000 there was a significant relaxation of the export regulations governing cryptography. Secondly, in 2002, an appellate judge in the Bernstein Vs. US Government case confirmed earlier rulings that cryptographic code was protected under the First Amendment of the US Constitution.

Chronology

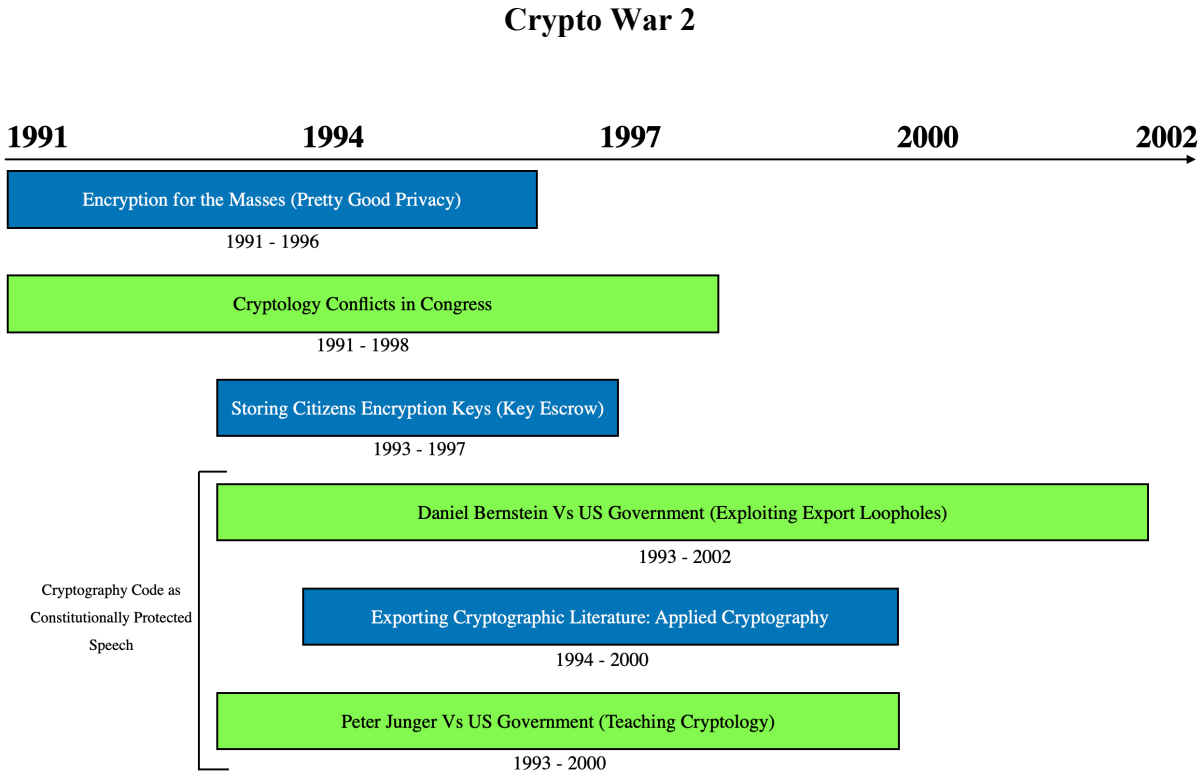

Figure 2: Crypto War 2

Encryption for the masses (Pretty Good Privacy) (1991 – 1996)*:* The second crypto war started in 1991 with the proposed *Comprehensive Counter-Terrorism Act of 1991* (S.266), a clause in which read:

> [This bill] expresses the sense of the Congress that […] that communications systems permit the Government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law. (United States Congress, 1991, Section 2201)

The language indicated cryptographers must either provide a government access method to encrypted communications, or technologies must forgo encryption outright.

Philip R. Zimmermann believed the clause, 'foretold the shape of things to come' and accelerated production of Pretty Good Privacy (PGP), a project which he called, 'public key cryptography for the masses' (Zimmermann, 1991 & 1997). On 5 June 1991, Zimmermann

disseminated PGP for Microsoft's operating system (MSDOS) which was quickly exported via the Internet (Zimmermann, 1991b; Lebkowsky, 1993). In 1993, a grand jury was convened to investigate Zimmermann for violation of the ITAR, prosecution could result in a million-dollar fine and five years imprisonment (Markoff, 1996; Braddock, 1995).

In May 1994, MIT announced it would place its institutional strength and moral authority behind Zimmermann by becoming the hub for PGP 2.5 dissemination (Schiller, 1994). The MIT PGP FTP server did not, theoretically, allow export overseas, but its safeguards were trivial to circumvent (Arachelian, 1994). In hosting the code, MIT were arguably facilitating the export of cryptography.

MIT and Zimmermann subsequently decided to test whether the same PGP code which was ineligible for digital export could be exported in print. The PGP book they published included the full C code for PGP printed in characters suitable for optical character recognition. This allowed the pages to be scanned into a computer and converted back to software post-export, thus circumventing ITAR. This circumvention was achieved in Germany in September 1994 (Hortmann, 1995).

In 1996 the Zimmermann investigation was closed without prosecution (United States Attorney, 1996).

***Cryptology conflicts in Congress (1991 – 1998)**:* Throughout the 1990s Congress was a crypto wars battlefield. The earliest activity was Representative Meldon Levine's 1991 amendment to the reauthorization of the Export Administration Act, which aimed to ease cryptography restrictions (United States Congress, 1991b; United States National Archives & Records Administration, 1992, p. 32148). Another attempt was Representative Maria Cantwell's pro-

cryptography amendment to the Export Administration Act's reauthorisation bill in 1993 (United States Congress, 1993). Both amendments failed.

As the second crypto war became more polarized and publicized, a series of bills were introduced, often in a strike-counter-strike pattern, with most operate at either end of the spectrum (i.e. heavily regulating encryption vs removing nearly all regulations) with most having little chance of success. These included the:

- Anti-Electronic Racketeering Act (1995)
- Encrypted Communications Privacy Act (1996).
- Promotion of Commerce On-Line in the Digital Era (PRO-CODE) Act of 1996
- Safety and Freedom Through Encryption (SAFE) Act (1997).
- Secure Public Networks Act (1997).
- Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act (1998).

None of these bills became law.

Storing citizens encryption keys (key escrow) (1993 – 1997)*:* Since at least the early 1990s the NSA had been developing a key escrow capability known as Clipper (Sessions, 1993). Clipper was designed to deliver public key encryption firstly to government users, but also with the possibility of it being used by citizens (Sessions, 1993; National Institute of Standards & Technology & National Security Agency, 1993).

Shortly after the Clinton administration took office Sessions wrote a top-secret memo to the White House on behalf of a working group comprising FBI, NSA and the Justice Department advocating for non-escrowed encryption to be outlawed (Sessions, 1993). Clipper, which was to deliver real-time voice, fax, and data encryption and decryption capability, was announced in 1993 (The White House, 1993b & 1994). Clipper was presented as a voluntary program (The White House, 1994).

NSA were subsequently identified as the "government engineers" of the Clipper algorithm, SKIPJACK, which the White House stated must remain classified to prevent non-escrowed usage (Markoff, 1993; The White House, 1994). The digital rights community offered an overwhelmingly negative response. John Perry Barlow believed citizens were engaged in a, "revolutionary war […] Clipper is a last ditch attempt […] to establish imperial control over cyberspace" (Barlow, 1994). Despite multiple Clipper policy iterations, the proposal failed to gain public and industry acceptance (The White House, 1996 & 1996b). By 1998, Clipper was abandoned.

Cryptography code as Constitutionally protected speech (1993 – 2002)*:* Three major legal challenges to government regulations took place throughout the 1990s, that of Daniel Bernstein, Phil Karn, and Peter Junger. The associated judicial rulings were crucial to the advancement of cryptography. In Bernstein's case, Judge Marilyn Hall Patel recognized computer source code as constitutionally protected speech, stating:

> This court can find no meaningful difference between computer language […] and German or French […] like music and mathematical equations, computer language is just that, language […] this court finds that source code is speech. (United States District Court for the Northern District of California, 1995).

In the summer of 1999, a three Judge panel re-heard the case (United States Court of Appeals for the Ninth Circuit, 1999). They ruled in Bernstein's favor with Judge Betty Fletcher opining:

> Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment.
>
> Because the prepublication licensing regime [export regulations] challenged by Bernstein applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards, we hold that it

> constitutes an impermissible prior restraint on speech. (United States Court of Appeals for the Ninth Circuit, 1999).

In the Junger case, Chief Judge Boyce F. Martin ruled on 4 April 2000, “all ideas having even the slightest redeeming social importance,” including those concerning, “the advancement of truth, science, morality, and arts,” have First Amendment protection (United States Court of Appeals for the Sixth Circuit, 2000). Martin wrote:

> a musical score cannot be read by the majority of the public but can be used as a means of communication among musicians. Likewise, computer source code, though unintelligible to many, is the preferred method of communication among computer programmers. (United States Court of Appeals for the Sixth Circuit, 2000)

Judge Martin ruled as source code is an “expressive means” for the exchange of information and ideas about computer programming it was protected by the First Amendment (United States Court of Appeals for the Sixth Circuit, 2000).

Crypto War 3 (2013 – Present)

Conflict

The government pursued exceptional access methods. The public, or more precisely the big technology companies, sought to develop encryption beyond the state's ability to access, thus protecting their global market.

Combatants

The government's main advocate during the Obama era was the FBI, they were supplemented by the Attorney General during the Trump administration. Whilst digital NGOs were active, big technology firms such as Apple were the public's principal representatives – even though they were pursuing corporate rather than civil objectives.

Catalyst

Edward Snowden's disclosure of NSA's signal intelligence capabilities.

Chronology

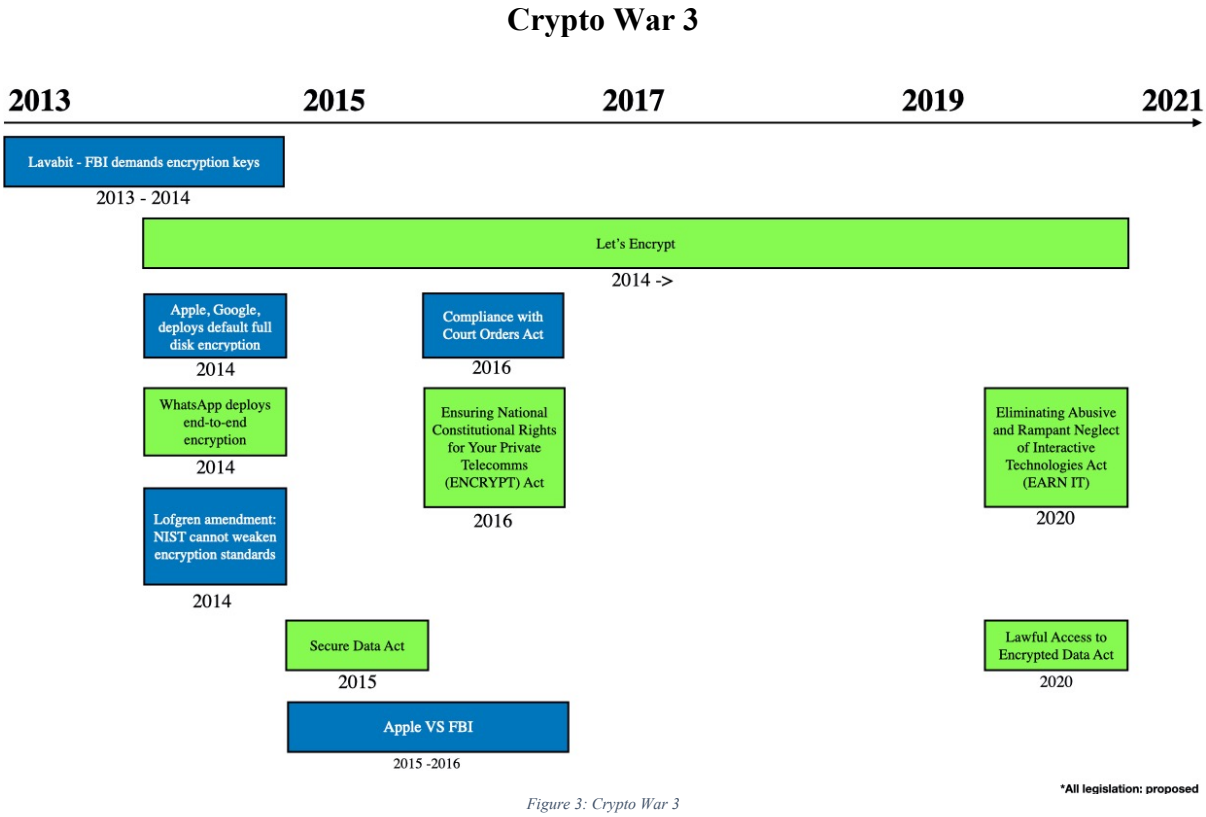

Figure 3: Crypto War 3

Lavabit: FBI demands encryption keys (2013 – 2014)*:* Lavabit owner Ladar Levison was issued a court order instructing him to facilitate the deployment of FBI interception technologies on Lavabit's network to enable collection from Edward Snowden's email account in 2013 (Levison, 2014; United States District Court Eastern District of Virginia, 2013, p. 36). Lavabit offered secure email services designed to frustrate US legal interception capabilities - encryption protected the data in transit and at rest. Lavabit could not read their client's data, therefore they were unable to aid the government even if served with a warrant (Lavabit, 2012). Levison was court ordered to submit Lavabit's encryption keys to enable intercept of Snowden's data. He objected, arguing that if he did so there would be no technical barriers to prevent the FBI intercepting the traffic of all of Lavabit's 410,000 clients (Levison, 2014). The court ordered a $5000 fine be levied against Levison for each day of non-compliance (United States District Court Eastern District of Virginia, 2013, pp. 142, 153-154). Levison surrendered

the encryption keys on 7 August - the same day he closed Lavabit (United States of America, 2013, p. 20). With the company deceased, the encryption keys were of no use to the FBI. Levison commented he had been forced to, “make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit” (Levison, 2013).

Let’s Encrypt (2014 ->); Apple, Google deploy default full disk encryption (2014); WhatsApp deploys end-to end encryption (2014)*:* Formed in 2013, Let’s Encrypt issued their first free SSL/TLS certificate in July 2015, triggering a rapid advance of web encryption (Aas, 2015). Between 2016 and 2019 global encryption rose from 40% to 80% according to Firefox statistics; Let’s Encrypt had issued over 538 million certificates for 223 million domain names allowing it to claim to be the world’s largest certificate authority (Let’s Encrypt, 2020; Aas et al., 2019).

In September 2014, Apple deployed default full disk encryption, with decryption keys tied to the user’s password, which were stored exclusively on the device (Farivar, 2014). Apple CEO Tim Cook announced, “Apple cannot bypass your passcode […] So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8” (Farivar, 2014).

Google’s Android 5.0 (Lollipop) enabled default full disk encryption in November 2014, as they gradually moved all Google traffic to be encrypted. Google figures show a steady rise from 50% of their traffic being encrypted in 2014, to 94% at the end of 2019 (Greenberg, 2014; Google, 2019). WhatsApp enabled default end-to-end encryption in November 2014 (Donohue, 2014).

Over the coming months and years almost all major services announced plans for similar default encryption, and vocally projected their privacy credentials to a post-Snowden global market apprehensive of US surveillance.

Lofgren amendment NIST cannot weaken encryption standards (2015)*:* In Congress Representatives Thomas Massie and Zoe Lofgren attempted to prevent the NSA and CIA from negatively modifying encryption standards in 2014 by offering an amendment to the 2015 National Defense Appropriations Act. The Massie-Lofgren amendment read:

> None of the funds made available by this Act may be used by the National Institute of Standards and Technology to consult with the NSA or the CIA to alter cryptographic computer standards, except to improve information security. (Massie, 2014)

The amendment was prompted by reports the NSA had undermined global encryption standards (Perlroth, Larson, and Shane, 2013). The amendment passed the House of Representatives 291-123 in June (Reitman, 2014). However, in December 2014, during negotiations between the House and Senate to pass the Appropriations Act the amendment was removed. Massie commented, "A veto-proof majority of Republicans and Democrats voted for my NSA reform amendment this summer. If this amendment is killed in a back room is that the will of the people?" (Massie, 2014b).

Secure Data Act (2015)*:* The same day the Massie-Lofgren amendment failed Senator Ron Wyden introduced the Secure Data Act (United States Congress, 2014). The bill stipulated:

> no agency may mandate that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency. (United States Congress, 2014)

The bill failed to pass.

***Apple vs FBI (2016)**:* The FBI requested Apple unlock the iPhone associated with the San Bernardino terrorist attack using an All Writs Act court order issued on 16 February 2016 (United States Department of Justice, 2016). The order instructed Apple to provide "reasonable technical assistance" to disable the device's auto-erase function, which would activate should too many incorrect pins be inputted. The FBI also required Apple modify the device to allow a passcode to be inputted electronically, rather than manually, making it easier to unlock iPhones with an exhaustion attack (Cook, 2016).

Apple CEO Tim Cook responded to what he labelled the FBI's "unprecedented" request stating:

> While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect (Cook, 2016).

Cook argued:

> Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks. (Cook, 2016)

Cook stated Apple could identify no precedent for such a use of the 1789 All Writs Act (Cook, 2016). The All Writs Act allows courts to, "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law" (Legal Information Institute, n.d.). The question was whether the issuance of such an order in this case was a circumvention of Congressional responsibility to pass laws.

The court case did not have the opportunity to unfold - on 20 March the FBI found an un-named third party to provide access to the device (United States District Court for the Central District of California, 2016, 3).

The FBI's withdrawal of the case was likely also influenced by a recent, though less publicized, ruling in New York where the FBI petitioned the courts using the All Writs Act to compel Apple to unlock seized iPhones (Orenstein, 2016). Orenstein found in favor of Apple, stating, "what the government seeks here is to have the court give it authority that Congress chose not to confer" (Orenstein, 2016, p. 30). Orenstein stated the government:

> has made the considered decision that it is better off securing such crypto-legislative authority from the courts […] rather than taking the chance that open legislative debate might produce a result less to its liking. (Orenstein 2016, p. 29)

Compliance with Court Orders Act (2016)*:* In April 2016, Senators Richard Burr and Dianne Feinstein released draft legislation entitled the *Compliance with Court Orders Act of 2016*, which stated:

> all persons receiving an authorized judicial order for information or data must provide, in a timely manner, responsive, intelligible information or data, or appropriate technical assistance to obtain such information or data. (Unite States Senate, 2016, p. 2).

The bill died in committee (Volz, 2016).

Ensuring National Constitutional Rights for your Private Telecomms (ENCRYPT) Act (2016)*:* The ENCRYPT Act proclaimed no government entity may:

> mandate or request that a manufacturer, developer, seller, or provider of covered products or services design [or] alter the security functions […] to allow […] surveillance […] or to allow the physical search of such product […] or have the ability to decrypt or otherwise render intelligible information that is encrypted (United States Congress, 2016)

Nor could a product be excluded from the market due to its use of encryption (United States Congress, 2016). The Encrypt Act did not progress beyond committee.

The bill was likely in response to failed activity in the state legislatures of California, Louisiana, and New York, where similar bills proposed fining technology companies $2500 for each

device they built which could not be decrypted – this was later refined to each device which could not be decrypted when the provider was served with a warrant (Cooper, n.d.; California Legislative, 2016; Electronic Frontier Foundation, 2016; Reitman, 2016; James, 2016; WAFB, 2016; New York State Senate, 2016).

Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT) (2020) & Lawful Access to Encrypted Data Act (LAEDA) (2020)*:* In 2020, Senator Lindsey Graham introduced the EARN IT Act, which would remove technology companies' section 230 liability protection if they did not comply with best-practice recommendations which would be generated by a new commission (United States Congress, 2020).[12] The commission's structure would likely give the Attorney General control over the recommendations. In a leaked earlier draft of the bill the Attorney General could simply replace the commission's recommendations with his own if he disapproved (United States Congress, 2020b). The bill was widely opposed. Senator Wyden commented, "This terrible legislation is a Trojan horse to give Attorney General Barr and Donald Trump the power to control online speech" (Wyden, 2020). The bill was substantially revised, whilst Senator Leahy added an amendment to protect encryption from being outlawed as part of the recommendations, the revised bill removed technology companies' section 230 liability protections with regard to child sexual abuse material, rather than making those protections conditional as per the earlier bill (CSAM) (United States Senate, 2020b & 2020c). This would allow states to modify their own CSAM regulations, potentially to include the removal of encryption, and take legal action against technology companies if they did not comply.

Shortly following EARN-IT's introduction, Senator Graham introduced LAEDA (United States Senate, 2020). LAEDA was more direct in its intent than EARN-IT, stipulating

[12] Section 230 of the Communications Decency Act places legal accountability for user-generated content with the user, rather than the technology platform.

technology manufacturers and services should proactively design their offerings to provide the government with decrypted data when required, for both data at rest and data in motion. Neither EARN-IT nor LAEDA advanced before the Congress concluded.

Conclusion

This research note has argued that a new chronology is needed to account for the full duration of the crypto wars, and rather than there being two crypto wars as commonly believed, the conflict should be divided into three conflicts. This chronology expands our understanding of the crypto wars, and acknowledges the full duration of the conflict, rather than limiting our narrative to the post-1993 period. However, whilst 1966 may be the start of the modern crypto wars, further research is required to help us understand the conflict throughout history.

Acknowledgments

The author would like to thank Professor Keith Martin of Royal Holloway, University of London, for his reviews of this research note.

References

Aas, J. (2015, June 16). Let's Encrypt Launch Schedule. Retrieved from https://letsencrypt.org/2015/06/16/lets-encrypt-launch-schedule.html

Aas, J., Barnes, R., Case, B., Durumeric, Z., Eckersley, P., Flores- López, A., … Warren, B. (2019). Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web. Retrieved from https://zakird.com/papers/lets-encrypt.pdf

American Council on Education. (1981). Report of the Public Cryptography Study Group. *Cryptologia* 5(3), 130-142.

Arachelian, A. R. (1994, November 30). Censorship in Cyberspace 5/6 [MessageID: '9411302012.AA01012@photon.poly.edu']. Cypherpunk Mail List Archives 1992-1998.

Bamford, J. (1982). *The Puzzle Palace: Inside the National Security Agency*. New York: Penguin Books.

Barlow, J. P. (1994, April 1). Jackboots on the Infobahn. Retrieved from https://www.wired.com/1994/04/privacy-barlow/

Barrett, G. B. (1998). Law of Diminishing Privacy Rights: Encryption Escrow and the Dilution of Associational Freedoms in Cyberspace. *New York Law School Journal of Human Rights* 15(1),115-140.

Braddock, C. A. (1995, January 7). (fwd) Re: Phil Zimmermann [MessageID: '53ae08506afed0671ca88cb1b531a06e@NO-ID-FOUND.mhonarc.org']. Cypherpunk Mail List Archives 1992-1998.

Bulkeley, W. M. (1994, April 28). Cipher Probe: Popularity Overseas of Encryption Code Has the U.S. Worried. *Wall Street Journal*. p. 1.

California Legislative. (2016). *AB-1681 Smartphones (2015-2016)*. Retrieved from https://leginfo.legislature.ca.gov/faces/billVersionsCompareClient.xhtml?bill_id=201520160AB1681&cversion=20150AB168199INT

Callas, J. (2013). To Our Customers. Retrieved from https://silentcircle.wordpress.com/2013/08/09/to-our-customers/

Cook, T. (2016, February 16). A Message to Our Customers. Retrieved from https://www.apple.com/customer-letter/

Cooper, J. (no date). Jim Cooper Biography. Retrieved from https://a09.asmdc.org/article/biography

Couillard, D. A. (2009). Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing. *Minnesota Law Review* 93(6), 2205-2239.

Clausewitz, C. V. (1909). On War. Retrieved from https://www.gutenberg.org/files/1946/1946-h/1946-h.htm

Cypherpunks. (1992-1998). Cypherpunks Mail List Archive 1992-1998. Retrieved from https://lists.cpunks.org/pipermail/cypherpunks/2013-September/000741.html

Diffie, W. (1975, May 22). Preliminary Remarks on the National Bureau of Standards Proposed Standard Encryption Algorithm for Data Protection. Retrieved from https://stacks.stanford.edu/file/druid:wg115cn5068/1975%200522%20ltr%20to%20NBS.pdf

Diffie, W. and Hellman, M. (1976). Exhaustive Cryptanalysis of the NBS Data Encryption Standard. *Computer* 10(6), 2-12.

Donohue, B. (2014, October 23). Android 5.0 Data Better Protected with New Crypto System. Retrieved from https://www.kaspersky.com/blog/full-disk-encryption-android-5/6423/

Edgett, S. J. (2003). Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy. *Pepperdine Law Review* 30(2), 339-366.

Electronic Frontier Foundation. (2016, April 7). Coalition Letter Opposing CA AB 1681. Retrieved from https://www.eff.org/document/coalition-letter-opposing-ca-ab-1681

Farivar, C. (2014, September 18). Apple Expands Data Encryption Under iOS 8, Making Handover to Cops Moot. Retrieved form https://arstechnica.com/gadgets/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/

Federal Register. (1975). *Federal Register* 40(52): 12067-12250.

Forest Wolfe, D. (2000). The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption. *Emory Law Journal* 49(2), 711-744.

Fraser, J. A. (1997). The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution. *Virginia Journal of Law and Technology* 2(2), 1-45.

Friendly, A. (1967, December 1). Secrets of Code-Breaking. *The Washington Post*, p. 1.

Froomkin, A. (1995). The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. *University of Pennsylvania Law Review* 143(3), 709-897.

Frye, E. & Sabett, R. V. (1998). Key recovery in a public key infrastructure. *Jurimetrics* 38(3), 485-96.

George, R. (2014). Richard 'Dickie' George - Keynote – Life at Both Ends of the Barrel: An NSA Targeting Retrospective. Retrieved from https://vimeo.com/97891042

George, R. (2016). CERIAS - The Role of the NSA in the Development of DES. Retrieved from https://www.youtube.com/watch?v=u80M009eSDk

George, R. (2020, April 29-30). Correspondence with author.

Gilmore, J. (1989, July 13). Subject: Merkle's "A Software Encryption Function" now published and available. Retrieved from https://tech-insider.org/data-security/research/1989/0713.html

Google. (2019). Transparency Report: HTTPS Encryption on the Web. Retrieved from https://transparencyreport.google.com/https/overview?hl=en_GB

Greenberg, A. (2014, November 18). WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users. Retrieved from https://www.wired.com/2014/11/whatsapp-encrypted-messaging/

Hastedt, G. P. (2011). *Spies, Wiretaps, and Secret Operations An Encyclopaedia of Espionage. Volume 1: A-J.* California: ABC-CLIO.

Hellman, M. (2013). Unpublished Autobiography. Retrieved from https://stacks.stanford.edu/file/druid:kq639bj2341/Ch_1.pdf

Hellman, M., & McGraw, G. (2016, April 26). Show 121: Marty Hellman Discusses Cryptography and Nuclear Non-Proliferation. Retrieved from https://www.synopsys.com/software-integrity/resources/podcasts/show-121.html

Hellman, M., Merkle, R., Schroeppel, R., Washington, L., Diffie, W., … Schweitzer P. (1976, September 9). Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption. Retrieved from https://web.archive.org/web/20201119113832/http://www.merkle.com/papers/Attempt%20to%20Cryptanalyze%20DES%201976-11-10.pdf

Hellman, M., W. Diffie, P. Baran, Branstad, D. and others not named. (No date). DES (Data Encryption Standard) Review at Stanford University. Retrieved from https://web.archive.org/web/20130707114841/http://www.toad.com/des-stanford-meeting.html

Hortmann, M. (1995, September 22). New source of PGP sourcecode [MessageID: ‘199509221554.RAA22108@bettina.informatik.uni-Bremen.de’]. Cypherpunk Mail List Archives 1992-1998.

Inman, B. R. (1979). The NSA Perspective on Telecommunications Protection in the NonGovernmental Sector. *Cryptologia* 3(3), 129-135.

James, E. T. (2016). House Bill No. 1040. Retrieved from http://www.legis.la.gov/legis/ViewDocument.aspx?d=991170

Johnson, T. R. (1998). American Cryptology During the Cold War, 1945-1989. Book III: Retrenchment and Reform, 1972, 1980. Retrieved from https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-histories/cold_war_iii.pdf

Juels, A., Diffie, W., George, R., Hellman, M., Rivest, R., & Shamir, A. (2011). RSA Conference 2011 Keynote - The Cryptographers' Panel. RSA Conference. Retrieved from https://www.youtube.com/watch?v=0NlZpyk3PKI

Kahn, D. (1967). *The Codebreakers: The Story of Secret Writing*. New York: Scribner.

Kehl, D., Wilson, A., and Bankston, K. (2015, June). Doomed to repeat history: Lessons from the crypto wars of the 1990s. Retrieved from https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf

Koffsky, M. I. (1994). Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and The Particularity Clause. *High Tech Law Journal* 9(1), 131-149.

Kolata, G. B. (1977) Computer Encryption and the National Security Agency Connection. *Science* 197(4302), 438-440.

Lavabit. (2012). Security Through Asymmetric Encryption. Retrieved from http://web.archive.org/web/20120502035558/http:/lavabit.com/secure.html

Legal Information Institute. (No date). 22 CFR § 120.11 - Public domain. Retrieved from https://www.law.cornell.edu/cfr/text/22/120.11

Let's Encrypt. (2020). Let's Encrypt Stats. Retrieved from https://letsencrypt.org/stats/

Lebkowsky, J. (1993). THE INTERNET CODE RING! An Interview with Phil Zimmerman, creator of PGP. Retrieved from https://tucops.info/tucops3/etc/crypto/live/aoh_pgpup.htm

Lennon, T. B. (1994). The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 Be Like 1984. *Albany Law Review* 58(2), 467-508.

Levison, L. (2013). Lavabit Closing Letter. Retrieved from https://web.archive.org/web/20131105161450/https://lavabit.com/

Levison, L. (2014, May 20). Secrets, Lies and Snowden's Email: Why I Was Forced to Shut Down Lavabit. Retrieved from https://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email

Levy, S. (2001). *Crypto: Secrecy and Privacy in the New Cold War*. New York: Viking Penguin.

Levy, S. (2016, March 11). Why Are We Fighting the Crypto Wars Again? Retrieved from https://www.wired.com/2016/03/why-are-we-fighting-the-crypto-wars-again/

Lokshina, T. (2013, July 12). Facebook Post 00:25. Retrieved from https://www.facebook.com/tanya.lokshina/posts/515881045133478%20

Macpherson, M. (1978, June 9). The Secret Life of David Kahn. *The Washington Post*. Retrieved from https://www.washingtonpost.com/archive/lifestyle/1978/06/09/the-secret-life-of-david-kahn/1209f0d6-e1e1-422c-8171-93a53e8ae29d/

Markoff, J. (1996, January 12). Data-Secrecy Export Case Dropped by I.S. New York Time, 12 January. Retrieved from https://www.nytimes.com/1996/01/12/business/data-secrecy-export-case-dropped-by-us.html

Martin, K. (2020). *Cryptography: The Key to Digital Security, How It Works, and Why It Matters*. London: W. W. Norton & Company.

Massie, T. (2014). Amendment to H.R. 2578, As Reported Offered By Mr. Massie of Kentucky. Retrieved from https://repcloakroom.house.gov/uploadedfiles/cjs16massie4.pdf

Massie, T. (2014b, December 4). Facebook Post 0721. Retrieved from facebook.com/RepThomasMassie/posts/word-is-spreading-that-the-massielofgrensensenbrennerholt-nsa-amendment-to-stop-/910370438987121

Markoff, J. (1993, April 16). Electronics Plan Aims to Balance Government Access With Privacy. New York Times. Retrieved from https://www.nytimes.com/1993/04/16/us/electronics-plan-aims-to-balance-government-access-with-privacy.html

May, T. C. (1988). Crypto-Anarchist Manifesto. activism.net. Retrieved from https://www.activism.net/cypherpunk/crypto-anarchy.html

Meinrath, S. D. & S. Vitka. (2014). Crypto War II. *Critical Studies in Media Communication* 31(2),123-128.

Meyer, J. A. (1977, July 7). Letter to Mr E. K. Gannet (Staff Secretary, IEEE Publications Board) from Joseph. A. Meyer. Retrieved from https://web.archive.org/web/20180609172620/https://cryptome.org/hellman/1977-0707-Meyer-letter.pdf

Murr, R. A. (1997). Privacy and Encryption in Cyberspace: First Amendment Challenges to ITAR, EAR and their Successors. *San Diego Law Review* 34(3), 1401-1462.

National Institute of Standards & Technology, & The National Security Agency. (1989, March 23-24). Memorandum of Understanding between NIST and NSA. Retrieved from https://web.archive.org/web/20010617230041/https://www.epic.org/crypto/csa/nist_nsa_mou.html

New York State Senate. (2016). Assembly Bill A8093A. Retrieved from https://www.nysenate.gov/legislation/bills/2015/a8093

Oberhaus, D. (2016, August 16). How the Government Is Waging Crypto War 2.0. Retrieved from https://www.vice.com/en_us/article/jpgvy3/encryption-debate-the-end-of-end-to-end

Orenstein, J. (2016, February 29). Memorandum and Order. Retrieved from https://cdn1.vox-cdn.com/uploads/chorus_asset/file/6124209/Orenstein-Order-Apple-iPhone-02292016.0.pdf

Perlroth, N., Larson, J., & Shane, S. (2013, September 6). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *New York Times*. Retrieved from

https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all

Plutte, J. (2011, March 28). Whitfield Diffie Interview: Computer History Museum. Retrieved from http://archive.computerhistory.org/resources/access/text/2015/04/102743051-05-01-acc.pdf

Privacy International. (2018, May 2). Winning and Losing and Still Fighting the Crypto Wars. Retrieved from https://privacyinternational.org/impact/winning-and-losing-and-still-fighting-crypto-wars

Rivest, R. (2012). Ronald Rivest's Killian Lecture at MIT: The Growth of Cryptography. Retrieved from https://www.youtube.com/watch?v=QOQ9b8STMec

Rivest, R., Shamir, A., & Adleman, L. (1977). Technical Memo Number 82: A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Retrieved from https://people.csail.mit.edu/rivest/Rsapaper.pdf

Rozenshtein, A. Z., Varia, M., & Wright, C. (2018, June 5). Retrieved from https://www.lawfareblog.com/how-congress-can-de-escalate-second-crypto-war-fund-research-and-broker-crypto-armistice

Schiller, J. (1994). MIT PGP announcement. Retrieved from https://town.hall.org/cyber94/pgp.html

Schneier, B. (2015, June 22). History of the First Crypto Wars. Retrieved from https://www.schneier.com/blog/archives/2015/06/history_of_the_.html

Sessions, W. S. (1993, February 19). Letter to George J. Tenet, Special Assistant to the President and Senior Director for Intelligence Programs, National Security Council. Retrieved from https://www.epic.org/crypto/clipper/foia/crypto_threat_2_19_93.html

Shapley, D. (1978). DOD Vacillates on Wisconsin Cryptography Work. *Science* 201(4351), 141.

Shapley, D. (1978b). Intelligence Agencies seek "Dialogue" with Academics. *Science* 202(4366), 407-410.

Shapley, D. & G. B. Kolata. (1977). Cryptology: Scientists Puzzle Over Threat to Open Research, Publication. *Science* 197(4311), 1345-9.

Simmons, R. (2007). Why 2007 Is Not like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence. *The Journal of Criminal Law and Criminology* 92(2), 531-568.

Singh, S. (2002). *The Code Book: The secret history of codes and code-breaking*. London: Fourth Estate.

Soesanto, S. (2018). No Middle Ground, Moving on from the Crypto Wars. Retrieved from https://web.archive.org/web/20200922162323/https://www.ecfr.eu/publications/pr/no_middle_ground_moving_on_from_the_crypto_wars

Reitman, R. (2014, June 19). EFF Statement on Passage of Massie-Lofgren Amendment Regarding NSA Backdoors. Retrieved from https://www.eff.org/deeplinks/2014/06/eff-statement-massie-lofgren-amendment-passing-house

Reitman, R. (2016, April 13). Victory: California Smartphone Anti-Encryption Bill Dies in Committee. Retrieved from https://www.eff.org/deeplinks/2016/04/victory-california-smartphone-anti-encryption-bill-dies-committee

Richards, N. (2017). *Intellectual Privacy: Rethinking civil liberties in the digital age.* Oxford: Oxford University Press.

Rowan, D. (2014). WhatsApp: The Inside Story. Retrieved from https://www.wired.co.uk/article/whatsapp-exclusive

The White House. (1993, April 16). Statement of the White House Press Secretary, 16 April 1993. Retrieved from https://web.archive.org/web/20000118230308/http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1993/4/19/6.text.1

The White House. (1993b, April 15). Presidential Directive Authorizing the Clipper Initiative, 15 April 1993. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/clipper-directive.html

The White House. (1994b, July 29). White House Responses to Questions Submitted by the Digital Privacy and Security Working Group, 29 July 1994. Retrieved from https://web.archive.org/web/19970320191301/http://www.eff.org/pub/Privacy/Clipper/wh_clipper.answers

The White House. (1996, July 12). Administration Statement on Commercial Encryption Policy. Retrieved from https://www.epic.org/crypto/key_escrow/wh_cke_796.html

The White House. (1996b, October 1). Vice President on Clipper 4. Retrieved from https://www.epic.org/crypto/key_escrow/clipper4_statement.html

United States Attorney [posted by D. McCullagh]. (1996, January 12). US DoJ Zimmermann Press Release [MessageID: gkxRbZe00YUqBRA6Nd@andrew.cmu.edu]. Cypherpunk Mail List Archives 1992-1998.

United States Congress. (1991, January 24). S.266 - Comprehensive Counter-Terrorism Act of 1991. Retrieved from https://www.congress.gov/bill/102nd-congress/senate-bill/266

United States Congress. (1991b). H.R.3489 - Omnibus Export Amendments Act of 1991. Retrieved from https://congress.gov/bill/102nd-congress/house-bill/3489/text?q=%7B%22search%22%3A%5B%22johnson%22%5D%7D

United States Congress. (1993). H.R.3627 - To amend the Export Administration Act of 1979 with respect to the control of computers and related equipment. Retrieved from https://www.congress.gov/bill/103rd-congress/house-bill/3627/text

United States Congress. (1995). S.974 - Anti-Electronic Racketeering Act of 1995. Retrieved from https://www.congress.gov/bill/104th-congress/senate-bill/974

United States Congress. (1996). S.1587 - Encrypted Communications Privacy Act of 1996. Retrieved from https://www.congress.gov/bill/104th-congress/senate-bill/158

United States Congress. (1996b). S.377 - Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997. Retrieved from https://www.congress.gov/bill/104th-congress/senate-bill/1726?s=1&r=17

United States Congress. (1997). H.R. 695 - Security and Freedom Through Encryption (SAFE) Act. Retrieved from https://www.congress.gov/bill/105th-congress/house-bill/695/text

United States Congress. (1997). S.909 - Secure Public Networks Act. Retrieved from https://www.congress.gov/bill/105th-congress/senate-bill/00909

United States Congress. (1998). Introduction of Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act, S. 2067. Retrieved from https://cyber.harvard.edu/eon/ei/elabs/security/crime1.htm

United States Congress. (2014). H.R.5800 - Secure Data Act of 2014. Retrieved from https://www.congress.gov/bill/113th-congress/house-bill/5800/text

United States Congress. (2016). H.R.4528 - ENCRYPT Act of 2016. Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/4528/text

United States Congress. (2020). S.3398 - EARN IT Act of 2020. Retrieved from https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

United States Congress. (2020b). Draft Discussion Text 3398 - EARN IT Act of 2020. Retrieved from https://assets.documentcloud.org/documents/6746282/Earn-It.pdf

United States Court of Appeals for the Ninth Circuit. (1999, May 6). Daniel J. Bernstein Vs United Department of State et al: Opinion. Retrieved from https://cr.yp.to/export/1999/0506-order.html

United States Court of Appeals for the Sixth Circuit. (2000, April 4). Opinion: Boyce F. Martin. Retrieved from https://casetext.com/case/junger-v-daley

United States Department of Commerce. (2000, January 14). Revisions to Encryption Items. Retrieved from https://www.govinfo.gov/content/pkg/FR-2000-01-14/html/00-983.htm

United States Department of Justice. (2016, February 16). All Writs Act Order. Retrieved from https://www.justice.gov/usao-cdca/apple-litigation

United States District Court Eastern District of Virginia. (2013, June 10). Court Documents. Retrieved from https://www.documentcloud.org/documents/801182-redacted-pleadings-exhibits-1-23.html

United States District Court for the Central District of California. (2016, March 21). Government's Ex Parte Application for a Continuance. Retrieved from https://epic.org/amicus/crypto/apple/191-FBI-Motion-to-Vacate-Hearing.pdf

United States House of Representatives. (1980, February 28; March 20; August 21). The Government's Classification of Private Ideas: Hearings Before a Subcommittee of the Committee on Government Operations House of Representatives. Retrieved from https://babel.hathitrust.org/cgi/pt?id=mdp.39015082027817;view=1up;seq=3

United States of America. (2013, November 12). Brief of the United States. Retrieved from https://www.eff.org/document/government-lavabit-brief

United States National Archives and Records Administration. (1992, July 20). Federal Register 57:139, July 20. Retrieved from https://www.govinfo.gov/content/pkg/FR-1992-07-20/pdf/FR-1992-07-20.pdf

United States Senate. (1978, April). Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard - Staff report of the Senate Select Committee on Intelligence. Retrieved from https://www.intelligence.senate.gov/sites/default/files/publications/95nsa.pdf

United States Senate. (2016). Compliance with Court Orders Act of 2016. Retrieved from https://www.dailydot.com/layer8/encryption-fbi-harvard-berkman-study/

United States Senate. (2020). The Lawful Access to Encrypted Data Act. Retrieved from https://www.judiciary.senate.gov/imo/media/doc/S.4051%20Lawful%20Access%20to%20Encrypted%20Data%20Act.pdf

United States Senate. (2020b). Leahy Amendment To S.3398 [OLL20683]. Retrieved from https://www.judiciary.senate.gov/imo/media/doc/Leahy%20Amendment%20to%20S.%203398%20-%20OLL20683.pdf

United States Senate. (2020c). Revised S. 3398 EARN-IT. Retrieved from https://www.judiciary.senate.gov/imo/media/doc/Graham's%20Amendment%20To%20S.3398%20-%20OLL20670.pdf

Volz, D. (2016, May 27). Push for encryption law falters despite Apple case spotlight. Retrieved from https://www.reuters.com/article/usa-encryption-legislation-idUSL2N18O0BM

WAFB. (2016, May 2). 'Brittney Mills' Act Fails to Pass in La. Retrieved from https://www.wafb.com/story/31866353/brittney-mills-act-fails-to-pass-in-la-house-committee/

Wyden, R. (2020, March 5). Tweet, 1856hrs, 5 March 2020. Retrieved from https://twitter.com/RonWyden/status/1235640470015008768/photo/1

Zimmermann, P. (1991). PGP Guide. Retrieved from http://www.erresoft.com/firmadigitale/PGP_Guide_vol_1.html

Zimmermann, P. (1991b, June 5). PGP: RSA Public Key Cryptography for the Masses. Retrieved from http://tech-insider.org/free-software/research/acrobat/910605.pdf

Zimmermann, P. (1997). Author's preface to the book: "PGP Source Code and Internals". Retrieved from https://philzimmermann.com/EN/essays/BookPreface.html

Zimmermann, P. (1999). Why I Wrote PGP', Phil Zimmermann's Personal Website. Retrieved from https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. London: Profile Books.

Biographical note

Craig Jarvis is a cyber security strategist completing a PhD in Cyber Security & History at Royal Holloway, University of London. Craig holds master's degrees in Cyber Security, International Security, and Classical Music, and studied history at Oxford University. Craig's first book, *Crypto Wars - The Fight for Privacy in the Digital Age: A Political History of Digital Encryption*, was published by CRC Press in December 2020.