THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 15 Article 2

August 2020

Cryptography, Passwords, Privacy, and the Fifth Amendment

Gary C. Kessler
Gary Kessler Associates / Embry-Riddle Aeronautical University - Daytona Beach, kessleg1@erau.edu

Ann M. Phillips
Embry-Riddle Aeronautical University - Daytona Beach, ann.phillips@erau.edu

CRYPTOGRAPHY, PASSWORDS, PRIVACY,AND THE FIFTH AMENDMENT

Gary C. Kessler[1], Ann M. Phillips[2]
[1]Embry-Riddle Aeronautical University
Gary Kessler Associates
Ormond Beach, FL
[2]Embry-Riddle Aeronautical University
Daytona Beach, FL
gck@garykessler.net, ann.phillips@erau.edu

ABSTRACT

Military-grade cryptography has been widely available at no cost for personal and commercial use since the early 1990s. Since the introduction of Pretty Good Privacy (PGP), more and more people encrypt files and devices, and we are now at the point where our smartphones are encrypted by default. While this ostensibly provides users with a high degree of privacy, compelling a user to provide a password has been interpreted by some courts as a violation of our Fifth Amendment protections, becoming an often insurmountable hurdle to law enforcement lawfully executing a search warrant. This paper will explore some of the issues around this complex legal and social issue, including the evolution in the use of digital cryptography and the evolving legal interpretations of privacy.

Keywords: Cryptography, Fifth Amendment, Law, Passwords, Privacy, Self-incriminating testimony

1. INTRODUCTION

While addressing cybersecurity conference attendees at Boston College in 2017, then-FBI Director James Comey observed that the ubiquitous availability and use of strong cryptography was upsetting the delicate balance between privacy and security that is at the very heart of the U.S. social contract (Armerding, 2017). In 2019, Manhattan District Attorney Cyrus Vance, Jr. testified that strong iPhone encryption was Apple's "gift to sex traffickers" ("Written Testimony", 2019, para. 13). Today's digital cryptography truly is military-grade and provides an often insurmountable barrier for law enforcement when trying to execute a search warrant. This raises several questions:

1. How do we, as a society, feel about citizens having access to strong encryption and devices that are impervious to a government-sanctioned search?

2. Did the authors of the Constitution envision a container that could never be opened and, therefore, never be searched?

3. Is compelling a user to provide a password a violation of Fifth Amendment protections?

4. Should crypto products have backdoors for just these reasons?

This paper will explore these issues by examining the growing capabilities of cryptography (Section 2) and the evolving interpretation of privacy and self-incrimination (Section 3). Section 4 will discuss some of the issues as privacy and the needs of the state collide. Section 5 will provide some conclusions.

2. SOME MAJOR EVENTS IN DIGITAL CRYPTOGRAPHY

Cryptography is the science of writing in secret codes. Most historians point to the use of non-standard hieroglyphics in Egypt in 1900 B.C.E. as the beginning of secret code writing although that practice probably appears spontaneously soon after writing was developed (Kahn, 1996; Singh, 1999).

For several thousand years, the primary use of cryptography was for secrecy (aka privacy and confidentiality). It was also the exclusive domain of the literate and, even then, employed almost solely at the nation-state level to protect diplomatic communication and military secrets (Kahn, 1996; Singh, 1999).

While many advances in cryptographic codes appeared in the 1800s, one of the most notable practical contributions came from Auguste Kerckhoffs, a Dutch linguist and cryptographer. In 1883, Kerckhoffs proposed a number of design principles for military ciphers. One that maintains significance today says that the cryptographic system must not rely upon the secrecy of the encryption algorithm but upon the judicious choice, use, and storage of the keys. In fact, it is best to assume that the enemy knows the algorithm (Kahn, 1996; Kerckhoffs, 1883a, 1883b).

Cryptography continued to play a major role in diplomatic and military communication in the 20th century, playing a key role in the military campaigns of both World Wars (Haufler, 2003; Yardley, 1931). Commercial use of crypto, while introduced in the 1920s, started to grow so rapidly in the post-WW II era that the U.S. and most of the allied countries limited its use by civilians. In the U.S., in particular, cryptography was classified as a munition, which placed strict export controls on those products (Kahn, 1996; Levy, 2001).

The 1950s saw the dawn of the computer age in commercial organizations, notably in the financial industry. In the early 1970s, the National Bureau of Standards (NBS, now the National Institute of Standards and technology [NIST]) put out a call for a national standard encryption scheme for use with computers. The Data Encryption Standard (DES), designed by IBM and derived from an earlier IBM cipher called Lucifer, was adopted in 1977 and published as Federal Information Processing Standard (FIPS) Publication 46. The National Security Agency (NSA) had input into the development of DES, which caused many to wonder if they had implemented some sort of backdoor, a purposeful weakening of the algorithm to make is more susceptible to certain kinds of attack. Ironically, the NSA-designed Substitution (S)-boxes removed a mathematical weakness, making the algorithm stronger. However, IBM offered both 56- and 128-bit key versions of DES and the NSA insisted upon use of the smaller key, making it more susceptible to brute force attacks (Schneier, 2004).

Upon adoption, DES became the newest secret key cryptography (SKC) scheme. SKC, also called *symmetric cryptography*, uses a single key for both encryption and decryption. The key, then, is a shared secret between the sending and receiving parties. An important aspect of SKC schemes is the process of key exchange; specifically, how do the sender and

receiver share the key and keep it a secret? In 1977, the best way might be for one party to write it down and send it by armored car to the other party, using the same keys for days or weeks at a time (Kahn, 1996; Singh, 1999).

During this same era, Whitfield Diffie and Martin Hellman proposed a new form of encryption called public key cryptography (PKC). Also called *asymmetric cryptography*, PKC employs two keys, one to encrypt and the other to decrypt. Although the two keys are mathematically related and created as a pair, deriving the value of one of the keys by knowing the value of the other is computationally infeasible. Thus, one of the keys could be widely published and shared, known as the *public key*, while the other key remained a closely held *private key* (Diffie & Hellman, 1976).

The description of PKC was widely hailed as the biggest advance in encryption in hundreds of years. For 4,000 years, encryption was used almost solely to keep secrets. PKC could also provide sender authentication, message integrity, key exchange, and non-repudiation. In terms of key exchange alone, public key methods allowed secret keys to be generated and exchanged in milliseconds (Kahn, 1996; Levy, 2001).

PKC depends upon the existence of trapdoor functions. In this context, a *trapdoor* (as opposed to a *backdoor*) refers to a mathematical function that is easy to compute but where the inverse function is significantly harder to calculate; e.g., it is easier to perform exponentiation than it is to calculate logarithms and multiplication is easier than factorization. The first workable PKC algorithm was published by Rivest, Shamir, and Adleman (1978) and led to the first commercial PKC product, RSA.

In June 1991, Phil Zimmermann uploaded Pretty Good Privacy (PGP) to the Internet. PGP was the first open cryptosystem, combining hashing, compression, SKC, and PKC into a method to protect files, devices, and e-mail. Public keys were shared via a concept known as a Web of Trust; individuals would directly exchange their public keyrings and then share their keyrings with other trusted parties (Zimmermann, 2001).

PGP secret keys, however, were 128 bits or larger, making it a *strong* cryptography product. Export of strong crypto products without a license was a violation of International Traffic in Arms Regulations (ITAR) and, in fact, Zimmermann was the target of an FBI investigation from February 1993 to January 1996. Yet, in 1995, perhaps as a harbinger of the mixed feelings that this technology engendered, the Electronic Frontier Foundation (EFF) awarded Zimmermann the Pioneer Award and *Newsweek Magazine* named him one of the 50 most influential people on the Internet (Sussman, 1995; Zimmermann, n.d.).

With the commercialization of the Internet and dawning of the World Wide Web in the early 1990s, the government realized that there were legitimate needs for public use of strong cryptography. But not without government oversight. In 1993, at the same time as the Zimmermann investigation, NIST and the NSA introduced the Capstone project to provide strong crypto for public use. Capstone comprised several components (Crypto Museum, 2018; Kessler, 2020):

1. *Skipjack:* An SKC block cipher using an 80-bit key, the design of which was classified (a violation of Kerckhoffs' design principle described above)

2. *Clipper:* A tamper-proof computer chip that ran Skipjack, designed with a government-accessible backdoor

3. *Escrowed Encryption Standard (ESS):* A scheme whereby private keys would

be escrowed by NIST and the Treasury Dept.

Irrespective of the government's intentions, pushback against Capstone from privacy advocates and critics of its poor cryptographic practices – including the discovery of a flaw in the Clipper chip's law enforcement backdoor – resulted in the termination of the project by 1996 (Blaze, 1994; Meeks, 1994). Ultimately, Capstone was never adopted (EPIC, n.d.b).

By 1995, electronic-commerce (e-commerce) started to blossom on the Internet. At that time, many people – including the first author of this paper – were actually sending credit card numbers and other private information in unencrypted emails. All of this changed in 1995 with Netscape's release of the Secure Sockets Layer (SSL) protocol, an encryption enhancement employed by the Hypertext Transfer Protocol (HTTP) in Web servers and browsers that were fundamental to supporting the growth of commercial activity on the Internet. Because export of 128-bit keys was still prohibited, browsers in this era – including Internet Explorer and Netscape – had a domestic version with 128-bit keys and an international version with 40-bit keys. In 1996, however, President Bill Clinton issued Executive Order (EO) 13026, re-classifying crypto products as technology rather than munition, which greatly relaxed export controls and key sizes (Clinton, 1996; U.S. Dept. of Commerce, 2000).

While this sea change was ongoing in the mid-1990s, Blaze, Diffie, Rivest, Schneier, Shimomura, Thompson, and Wiener (1996) released a white paper demonstrating that 56-bit keys were too short for practical, commercial purposes and that SKC schemes needed to use longer keys (Figure 1). Given that DES had had a 20-year lifetime in 1996, they concluded that the minimum key size for another twenty years was at least 75 bits.

Showing that 56-bit keys were insufficient was also a harbinger that the useful life of DES was coming to an end. In March 1998, NIST reaffirmed the DES standard for use for one additional five-year cycle but stated that a new standard would be developed. In July, however, the EFF introduced Deep Crack, a chip that could be built for $220K and brute force a DES key in an average of 4.5 days (EFF, 1998). This development effectively killed DES and caused a scramble as interim fixes and variants to DES became available (Kessler, 2020).

The process of developing NIST's next-generation SKC standard, called the Advanced Encryption Standard (AES), started in 1997. The AES process was handled very differently from the one that gave us DES. Whereas DES was developed under a shroud of secrecy, the AES process was an open, international competition. Fifteen proposals were submitted and reviewed, with all algorithms, documentation, and tests were posted on a NIST Web site. In 2001, an algorithm named Rijndael (developed by Belgian cryptographers Joan Daemen and Vincent Rijmen) – employing a 128-, 192-, or 256-bit key – was adopted as FIPS Pub. 197 (NIST, 2018).

It is worth noting several other crypto developments that occurred in the 2000s. Apple's Mac OS X, based on the Unix operating system, became available in 2001 (Painter, 2019). Mac OS X 10.3 (Panther) introduced FileVault in 2003, which could encrypt a user's home directory (Apple Inc., 2003). FileVault 2, a re-design of the original, was released in 2011 with Mac OS X 10.7 (Lion) and supported full startup volume encryption. This product was one of the first to employ AES encryption (Apple Inc., 2018; OSXDaily, n.d.).

In 2004, TrueCrypt, open source encryption for Windows, MacOS, and Linux, was released (TrueCrypt, 2015). TrueCrypt pro-

Attacker	Budget	Tool	Time Per Recovered Key 40-bit	56-bit	Key Length For Protection In Late-1995
Pedestrian hacker	Tiny	PC	1 week	Never	45
	$400	FPGA	5 hours	38 years	50
Small business	$10K	FPGA	12 min.	18 mon.	55
Corporate Dept.	$300K	FPGA	24 sec.	19 days	60
		ASIC	0.18 sec.	3 hours	
Big Company	$10M	FPGA	7 sec.	13 hours	70
		ASIC	5 ms	6 min.	
Government	$300M	ASIC	0.2 ms	12 sec.	75

ASIC = Application-specific integrated circuit
FPGA = Field programmable gate array

Figure 1. Effective key lengths for commercial applications (Adapted from Blaze et al., 1996)

vided a novel capability called *plausible deniability* (Figure 2). When a TrueCrypt encrypted volume is created, the user can define a single encrypted container or two encrypted containers using different passwords. Because the encrypted volume is randomized, it is not possible to tell whether there is a single container or two. If somehow compelled to provide a password, a user can supply the password to the standard TrueCrypt volume and there is no way to know if there is a hidden volume within (TrueCrypt Foundation, 2012). (On 28 May 2014, the TrueCrypt Web site suddenly went dark, announcing that the software was no longer being maintained and that users should seek alternatives. The story of TrueCrypt and the software that followed is beyond the scope of this paper but certainly an interesting twist.)

With the growth in the use of smartphones and the prodigious amount of personal information they contain, default encryption of these devices was inevitable. In 2014, Apple announced that iOS 8 devices would be encrypted by default and Google announced the same for Android 5.0 (Lollipop) (Miller, 2014).

3. SOME MAJOR EVENTS IN THE NOTIONS OF PRIVACY

Although the word "privacy" never appears in the U.S. Constitution or the Bill of Rights, Zimmermann – the author of PGP – suggests that privacy is an inalienable right that was understood by the framers (1999). Given the technology available in the late-1780s, any two people having a conversation knew whether they had privacy or not simply by looking around; if a third person came within earshot, the two people could merely walk away. The printed word was always visible. People had privacy because physics sup-

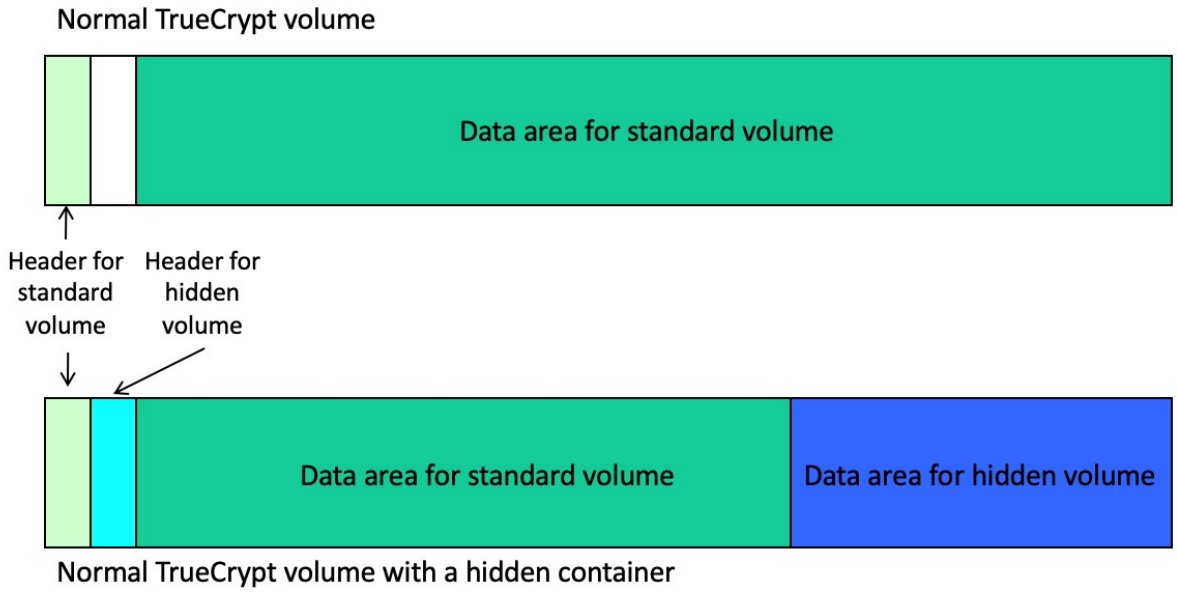

Figure 2. Plausible deniability in TrueCryp

ported it; the framers would no more discuss the right of privacy than they would the right to breathe air.

Most people today associate our expectation of privacy with the Fourth Amendment:

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).

One hundred years after the ratification of the U.S. Constitution, the invention of the camera – and an invasive press – brought the concept of privacy into public discussion. The right to privacy was first described by Warren and Brandeis (1890) and introduced the foundational concept that most Americans just want the "right to be let alone."

The Fourth Amendment protects against overly invasive government searches but also provides guidelines around when the government *can* access an individual's personal effects. In particular, a *search* is an:

1. Action by the state
2. Infringes upon one's reasonable expectation of privacy
3. Is legal only if there is a search warrant *or* a valid warrant exception

In this regard the Fourth Amendment can be viewed as involving a level of "taking" some level of privacy by a government entity.

The understanding of Fourth Amendment protections has changed over time with the current decisional law suggesting that they apply to people, not places (*Katz v. U.S.*, 1967; *Olmstead v. U.S.*, 1928). *Katz* also provides a guideline of what "reasonable expectation of privacy" means; namely, a *subjective expectation of privacy that is objectively reasonable.* This standard is met if

a person expects privacy (subjective) and society agrees that that expectation is reasonable (objective). As an example, a person standing inside of an enclosed, glass phone booth might have a reasonable expectation of privacy for a telephone conversation but probably does not have a reasonable expectation of privacy if they are taking their clothes off.

The Electronic Communications Privacy Act (ECPA, 1986), which governs electronic surveillance in the United States, has always drawn a distinction between user data and transactional data. *User data*, also called *content*, is the information that is under direct control of the user, such as the words typed into a file or words said during a telephone conversation. *Transactional data*, also called *non-content*, is the metadata needed by an entity such as a communications carrier, file system, or operating system to actually control or manage the data flow. The distinction between user content and metadata is consistent with the established legal doctrines regarding the privacy of content and the sharing of date under the third-party doctrine. By refusing to include content in the electronic surveillance data, the traditional *Katz* doctrine is being followed. Similarly, allowing metadata to be included in electronic surveillance comports with the third-party doctrine.

The third-party doctrine emanated from *Smith v. Maryland* (1979). In this case, Smith stole a woman's purse. A few days later, the woman started to receive harassing phone calls. Following the procedures of the ECPA, police placed a trap and trace device on her line to determine the numbers calling the woman; this process linked calls to Smith's number. Again, following ECPA provisions, police placed a pen register on Smith's line, showing that he was calling the woman. Smith was arrested, tried, and convicted. He appealed the conviction by asserting his expectation that his telephone calls were private. The Court upheld conviction, noting that a) police did not view the content of his calls and b) he had already shared the fact that he was calling the woman with a third party, namely the telephone company. These points are important to this discussion largely because metadata is typically not encrypted while content might be. Thus, metadata would seemingly always be available to law enforcement; it is content where the issue of encryption might be directly at issue. And content is where incriminating and exculpatory evidence of crime would be found.

The Fifth Amendment addresses, among other things, issues related to self-incriminating testimony and says, in part, "No person... shall be compelled in any criminal case to be a witness against himself" (U.S. Const. amend. V). This concept was novel at the time because the prevailing jurisprudence in the 1700s was that a suspect was guilty until proven innocent. The U.S. system of criminal justice is based upon the notion that a defendant is innocent until proven guilty and the state has the burden of proving guilt beyond a reasonable doubt. In this way, the Fifth Amendment can be seen as protecting against a person having to "give" evidence. Not forcing a defendant to testify is a way of implementing this precept; a criminal suspect does not have to speak and not speaking is not an implication of guilt.

Fisher v. U.S. (1976) introduced two relevant clarifications to Fifth Amendment protections, namely the Act of Production Doctrine and the Foregone Conclusion Doctrine. The Act of Production Doctrine says that a compelled act is testimonial when the act asserts information – i.e., the contents of one's mind – with some aspect of communication. In this case, the Court observed that *doing* something can convey information the same

as *saying* something. Thus, if a teacher asks a group of students to raise their hands if they read a certain paper, the act of raising the hand is testimonial since it conveys information that is in the students' heads. Courts have, therefore, come to interpret the Fifth Amendment as protecting both forms of compulsion, namely, testimony and production.

It is important to note that knowing a password and knowing the contents of an encrypted device are two different things. It is often the case people besides the owner of a device may know or be aware of the code needed to unlock the device; family members and friends, for example, often exchange or share this information for myriad reasons. Therefore, knowledge of a password is not a valid test that the person actually knows the contents and, therefore, is not in and of itself incriminating.

The Act of Production Doctrine considers a person's communication implicit in the act, not what communications may result from the act. How incriminating the production may be, or what the computer does when a person unlocks is, does not change the testimony implicit in the act of unlocking it. *In re Search Warrant Application* (2017) notes that use of biometry to access a device does not gain testimonial significance based on the information revealed; such an argument "...relies on conflating what it means for an act to be inherently testimonial versus an act yielding an incriminating result" (Section II, para. 11). In a sense, the passcode is akin to a fingerprint or a physical key; it can be used to open the device to further exploration, but neither the code nor the fingerprint nor the physical key creates any information to be decrypted; the information either exists or it doesn't irrespective of the unlocking of the device. Thinking of the issue in this regard overcomes the dichotomy of being able to use a fingerprint to unlock a device, but not obtain a passcode.

The Foregone Conclusion Doctrine says that compelling a person to produce information under certain circumstances is not testimonial if the state already, independently knows that the person has the information. So, as an example, if the state compels a person to open a safe by using a combination, the *act* of entering the correct combination is not incriminating testimony that the person knows the combination if the state can show that it had authentic, *a priori* knowledge that the person knew the combination. The elements of the Forgone Conclusion Doctrine are met when:

1. The state has knowledge of the existence in some specified location of the demanded evidence (*reasonable particularity)*
2. The person is known to have possessed or controlled the evidence
3. The evidence is authentic

The Foregone Conclusion Doctrine has two elements that apply more to the access to and acceptance of physical documents than to digital passwords. Reasonable particularity, the first such element, is a level of specificity that does not really apply to passwords; the state is seeking a single password with which to access a single device (*Commonwealth v. Jones*, 2019; Kerr, 2018; *U.S. v. Spencer*, 2018). The other element, authenticity, should not be an issue with passwords since they are self-authenticating; if the password works, it is clearly authentic (*Commonwealth v. Gelfgatt*, 2014; *In the Matter of the Search*, 2018; *State of Florida v. Stahl*, 2016).

Doe v. U.S. (1988) provides additional insight into when Fifth Amendment protections attach. According to *Doe*, "...an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information" (*Doe*, para. 3) in order to be

considered testimonial. Thus, Fifth Amendment privileges can only be invoked when these three elements apply:

1. Compulsion
2. Testimonial communication or act
3. Incrimination

Without these components, there is no Fifth Amendment issue. Per *Doe* (1988), "If a compelled statement is 'not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence'" (footnote 6). This relates to the question about whether providing a passcode is testimonial. If the initial compelled communication is testimonial, then any derivative evidence would be inadmissible; if, however, such information is not testimonial, then any derivative information would be properly admitted into evidence.

U.S. v. Hubbell (2000) further clarifies the limits of the Fifth Amendment. As part of a plea agreement, Hubbell agreed to provide certain documents relevant to a government investigation. After the government issued a subpoena to Hubbell to produce those documents, he asserted his Fifth Amendment privilege against self-incrimination before a Grand Jury. The prosecutor obtained a court order for the documents and offered immunity to Hubbell who, in turn, provided the documents, thus was in compliance with the original plea bargain. The government then used the documents to indict Hubbell for additional crimes. The Supreme Court dismissed the indictment, observing that the Fifth Amendment privilege against self-incrimination protects an individual from being compelled to disclose the existence of, much less produce, incriminating documents of which the prosecution has no *a priori* knowledge, thus is unable to describe with reasonable particularity. The Court also ruled that if an individual produces such documents pursuant to a grant of immunity, the government may not use them to pursue additional criminal charges against that person.

4. PRIVACY V. THE NEEDS OF THE STATE

The evolution and widespread availability of strong cryptography made it inevitable that an individual's expectation of privacy would be on a collision course with the legitimate needs of the state to execute a valid search warrant.

4.1 Compelling an Individual's Password

Since the early days of PGP, everyone from pundits and researchers to legal scholars and technocrats have wondered, "What happens if law enforcement issues a search warrant for an encrypted device and the user chooses not to comply?" It took more than 15 years for a court case to address this question (Nakashima, 2008).

U.S. v. Boucher (2007, 2009) is the first known case in the U.S. involving an encrypted computer and the question of self-incrimination. Boucher, a Canadian citizen, was stopped at a U.S. border crossing in Vermont. Upon examination, images of child pornography were found on his computer, which was encrypted using PGP Desktop software. The computer was powered down upon seizure and was unable to be further examined by law enforcement (Cohen & Park, 2018; Nakashima, 2008; Sacharoff, 2018). Police then asked a judge to compel Boucher to provide the password. In 2007, a U.S. Magistrate Judge ruled that compelling a password violated Boucher's Fifth Amendment protections against self-incrimination. Upon the government's appeal in 2009, a U.S. District Judge ordered Boucher to supply police with

an unencrypted version of the hard drive. At that point, Boucher accepted a plea agreement, was sentenced to three years in prison, and then subsequently deported.

During public discourse of the various Boucher rulings, many physical world analogies were made to this cyber world case. Most notably, the password was the same as a key to a locked room; providing the key is not incriminating even if the contents of the room are. But, in light of the Act of Production Doctrine, is revealing the key's location testimonial? One can be compelled to give a fingerprint, cheek swab, hair sample, blood, or other DNA; why not a password? But, perhaps a more fundamental question: Did the framers of the Constitution in 1878 ever conceive of a Fourth Amendment container that could not somehow be opened by physical means?

When applying for search warrants for physical documents, the government needs to meet the constitutional threshold of probable cause, i.e., that there is a fair probability that a search will result in evidence of a crime being discovered (U.S. Const. amend. IV). The government must also, as specific as is possible, describe the place to be searched, and the persons or things to be seized. The standard for searching for data on a digital device should not be higher. The standard for compelling the production of a password does not have to do with the eventual recovery of evidence. Rather, as some courts have held, the proper question is whether the government can demonstrate that it is a foregone conclusion that the defendant can decrypt the device (Kerr, 2018, 2019; *U.S. v. Apple MacPro Computer*, 2017).

The Foregone Conclusion Doctrine was significant in the Boucher Order. Boucher accessed his laptop at the Immigration and Customs Enforcement (ICE) agent's request at the border, where the agent ascertained the presence of child pornography. Because of that act, the Government knew of the existence and location of the hard drive and its files. Compelling Boucher to provide access to the unencrypted drive did not add to the sum total of the Government's information about the presence of possibly incriminating files (Kerr, 2019; Sacharoff, 2018; *U.S. v. Boucher*, 2009).

In addition, Boucher's act of producing an unencrypted version of the drive was not needed to authenticate it since he had already admitted to possession of the computer and provided the Government access to the drive. Since the Government could link Boucher with the files on his computer without making use of his production of an unencrypted version of the drive and stated that it would not use his act of production as evidence of authentication, there was no violation of his Fifth Amendment privileges (Kerr, 2018; *U.S. v. Boucher*, 2009).

The Boucher case did not provide guidance necessarily followed by other courts. In a similar case five years later in Massachusetts, suspect Gelfgatt was charged with multiple counts of forgery. Relevant evidence was known to be on his computers. Prior to trial, a motion to compel Gelfgatt to "...enter his password into encryption software" was denied by a Superior Court judge, who referred the point of law to the Supreme Judicial Court (SJC). The SJC reversed the denial, arguing that the motion violated neither the Fifth Amendment nor Article 12 of Massachusetts Declaration of Rights since the compelled decryption would not communicate facts of a testimonial nature beyond what Gelfgatt had already admitted to investigators (*Commonwealth v. Gelfgatt*, 2014).

Yet, five years after that, the state issued a *Gelfgatt* order for Jones – indicted for sex trafficking – to "provide... in writing... the PIN code" to a mobile phone (*Commonwealth v. Jones*, 2019). But *entering* and *revealing* a password are different things, and revealing

the password is not supported by *Gelfgatt*. Once the Commonwealth changed the request to entering the password, the order was upheld due to the Foregone Conclusion Doctrine (Kerr, 2019).

Requiring the disclosure of a password can be compared to the required disclosure of a private document, which may have some Fifth Amendment protection. The required oral disclosure of a password is often equated to incriminating testimony which is proscribed by the Fifth Amendment (Kerr, 2019).

Inconsistencies in rulings have appeared within states and between federal courts. Two cases in Florida provide a classic example. In *State of Florida v. Stahl* (2016), Stahl was arrested for video voyeurism (in this case, taking upskirt photos) in Sarasota. Stahl gave consent for the search of his mobile phone, confirmed the phone number, and provided police with the location of the phone – and then withdrew consent. The State's motion to compel Stahl to provide the password to police officers was denied by the trial judge, yet Florida's Second District appellate court quashed the trial judge's order, allowing the State to compel the password (Kerr, 2019).

In 2018, G.A.Q.L., a 17-year-old, was an inebriated driver in a high-speed collision in the southeastern part of the state, resulting in the death of a passenger in his vehicle (*G.A.Q.L. v. State of Florida*, 2018). The State made a motion to compel an iPhone 7 and iTunes password pursuant to a search warrant for the phone, for which they had credible belief that relevant evidence would be found. The trial court ordered the passwords to be provided, per *Stahl*. In this case, Florida's Fourth District appellate court quashed the trial judge's order, protecting the password on Fifth Amendment grounds. The appellate judges ruled that the Foregone Conclusion Doctrine did not apply because the State did not show "reasonable particularity."

Given that two Florida appellate courts have made different rulings, this question will likely go to the Florida Supreme Court at some point. The Court in *G.A.Q.L.* openly disagreed with Florida's Second District Court of Appeal and cited a U.S. 11th Circuit Court of Appeals case that found that the privilege against compelled decryption applies unless the government can describe the incriminating files that are on the device with reasonable particularity (*In Re Grand Jury Subpoena*, 2012).

There are other cases that have resulted in conflicting decisions, showing that there is no clear precedent, among them:

1. *U.S. v. Fricosu* (2012): Citing the All Writs Act, ordered the defendant to supply an unencrypted copy of an encrypted hard drive for which the Government had a search warrant.

2. *U.S. v. Apple MacPro Computer* (2017): Found that compelled decryption did not violate prior decisional law and did not violate Fifth Amendment privilege against self-incrimination.

3. *U.S. v. Spencer* (2018): Held that the appropriate test to determine whether the Foregone Conclusion Doctrine applied was whether the government could show that it was a foregone conclusion that the defendant could decrypt the devices; if so, it allowed compelled decryption.

4. *Seo v. State* (2018): Found that ordering the defendant to unlock a mobile phone was a violation of Fifth Amendment protections against self-incrimination, largely because of the unlimited nature of the search warrant and the fact that the device is an intimate record of a

person's thoughts and actions. The ruling was upheld by the Indiana Supreme Court in 2020 (Lee, 2020; *Seo v. State*, 2020).

It seems that inconsistencies at the Federal level (e.g., *Boucher*, in the U.S. 2nd Circuit, conflicts with *In Re Grand Jury Subpoena*, decided in the U.S. 11th Circuit) suggest that this issue has to eventually be adjudicated by the U.S. Supreme Court. One could argue that the Supreme Court has already missed one opportunity to address this question. The defendant in *Commonwealth v. Jones* (2019) filed a writ of certiorari with the Court in 2019 (Reidy & Nathanson, 2019). The specific questions in the writ were:

Does the Fifth Amendment's act of production doctrine apply to compelled decryption? If so, what does the foregone conclusion exception to the act of production doctrine require the government to show before an order to compel decryption can issue? (Reidy & Nathanson, p. i)

Public defenders in Massachusetts filed an *amicus curiae* brief arguing that *Fisher's* ruling regarding the Act of Production Doctrine should not be applied to compelled decryption (Rangaviz, 2019). The Supreme Court declined to hear the case as they denied certiorari (U.S. Supreme Court, 2019).

4.2 Product and Encryption Backdoors

In December 2015, a mass shooting in San Bernardino, California resulted in 14 people being killed and an additional 21 people wounded. The shooters – a married couple – were both killed in a shootout with police. According to FBI investigators, the couple were lone operator terrorists; "homegrown violent extremists" radicalized over several years of consuming "poison on the Internet" and inspired by foreign terrorist groups committed to jihadism and martyrdom, yet not directed by any particular group (Schmidt & Pérez-Peña, 2015).

The FBI believed that access to the iPhone 5C found in the couple's vehicle would advance their investigation. As iPhone encryption has evolved, law enforcement has requested assistance from Apple many times to retrieve information so as to advance criminal investigations. When Apple complied, it employed existing capabilities to access the devices (Cohen & Park, 2018; Sacharoff, 2018).

In 2016, the Court issued an order requiring a custom operating system be created and installed by Apple without unlocking or otherwise changing the data on the phone (*In re Apple AWA Order*, 2016). What was new in this request was that Apple was asked to develop a new capability to break the advanced security features found in Apple's devices. The basis of the FBI's request to Apple was the All Writs Act of 1789 that allows the government to issue all necessary and appropriate orders in the furtherance of their rightful duties (*In re Apple AWA Application*, 2016). Apple opposed the order on the grounds that it was unlawful and unconstitutional because it essentially conscripted Apple into writing hacking code for the government. Further, they argued that if the order was granted, it would undermine the security of all Apple devices and set a dangerous precedent for future cases (Cohen & Park, 2018; EPIC, n.d.a; *In re Apple Motion to Vacate*, 2016). Subsequently, the FBI found another way into the phone and the matter was dropped (Blum, 2018; Cardozo & Crocker, 2018).

In December 2019, conflicts between the government and Apple resurfaced after a terrorist shooting at Naval Air Station Pensacola (Florida). A member of the Saudi Arabian military in flight training at the air station, later found to have ties with al Qaeda, killed three people and wounded eight others with a handgun before being killed by responding

authorities. Law enforcement wanted to gain access to two of the assailant's phones, an iPhone 5 and iPhone 7. Attorney General William Barr requested Apple's assistance in unlocking the phones and Apple, as in the past, refused the government's request. A.G. Barr was very public in his displeasure that Apple would not assist in this case while Apple made it clear that they had assisted the government in substantive ways, including responding rapidly to their requests and turning over several terabytes of data; Apple merely would not unlock the phones (Feiner, 2020; Lucas, 2020). Eventually, the FBI was able to break into the phones and although they opined that Apple's assistance earlier on would have been helpful, they did not address what new type of information was recovered (Brewster, 2020).

In early 2020, the U.S. Senate introduced the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2020. While the umbrella mission "To establish a National Commission on Online Child Sexual Exploitation Prevention..." is noble, the Trump Administration's publicly stated rationale is because child predators use virtually unbreakable encryption (S.3398, 2020). Of course, so do terrorists and criminals, as well as journalists, political activists, victims of domestic abuse, and other ordinary citizens. While the EARN IT Act does not specifically address encryption, it provides a clear path for the government to force content platforms to eliminate its use (Newman, 2020; Pfefferkorn, 2020).

Section 230 of the Communications Decency Act (CDA) holds Internet social media services, such as Facebook and Twitter, immune from liability for the content on their unmoderated platforms. Thus, if Party A defames Party B on Facebook or Twitter, Party B can sue Party A but cannot sue Facebook or Twitter (47 U.S. Code §?230, 1996). Without Section 230 protections, it is unlikely that social media platforms would exist as they do today (for good or for bad).

The EARN IT Act would remove Section 230 immunity unless social media and other content-hosting platforms comply with a set of guidelines that would be created by an unelected National Commission and could be changed unilaterally at the whim of the U.S. Attorney General. Furthermore, these guidelines are not laws or rules that go through any legislative or formal rulemaking process, although compliance with them provides immunity to the provider (Pfefferkorn, 2020). Clearly, this approach provides a way to incent – or coerce – platforms to do what the Government wants them to do (Cope, Mackey, & Crocker, 2020).

A threat to the use of end-to-end encryption is not explicit in the EARN IT Act; in fact, the only mention of the word "cryptography" is to require that two members of the National Commission be knowledgeable about the subject (S.3398, 2020). But the potential is there for the commission to decide to limit the immunity of a platform that employs end-to-end encryption (Pfefferkorn, 2020). It might also require content providers to examine the content being posted, which would not only bypass the use of encryption but would also make the content provider an agent of the state without a search warrant (Cope et al., 2020). At the time of this paper's submission, the bill is under consideration by the Senate (Ng, 2020).

5. CONCLUSION

Even before the shooting in Pensacola, the Apple-FBI conflict had re-energized the debate about the government's need and ability to get past strong encryption. Once again, discussion started about requiring manufacturers to install backdoors in all encryption products or on ways to ban end-to-end encryption. While this is an idea that might

sound good on paper – as it did two decades earlier – it is impossible to implement cryptographic backdoors without weakening the overall security of any product (Abelson et al., 2015). Many practical issues crop up, as well, including (Claburn, 2019):

1. Who determines who the Good Guys are that get access to the backdoor features?
2. How would use of the backdoor be controlled?
3. How would access to the backdoor ever be rescinded?

But is this not the same idea that the government posed – and the marketplace rejected – in the 1990s with Capstone (IEEE, 2018; Stepanovich & Karanicolas, 2018; Young & Yung, 1996)? And, yet, it seems to remain an attractive idea to governments; as recently as June 2019, senior members of the Trump administration were exploring potential legislation to crack down on end-to-end encryption (Abel, 2019; Claburn, 2019). Indeed, U.S. Attorney General William Barr and officials in Australia and the U.K. have warned high-tech companies that continued use of strong end-to-end encryption could result in stronger regulations and laws limiting such use ("Attorney General", 2019). Interestingly, the European Union Agency for Cybersecurity (ENISA) and Europol released a joint statement in 2016 calling for mechanisms to circumvent commercial encryption methods although they acknowledged that weakened cryptography was not the correct forward path ("On lawful", 2016).

A cryptographic backdoor is a slight variant on *kleptography*, the "...study of stealing information securely and subliminally" (Young & Yung, 1997, p. 63). Unlike a backdoor that weakens a crypto algorithm, kleptography refers to an attack on a cryptosystem from within. Consider this example: Imagine a trusted, black box cryptosystem that generates PKC key pairs. Presumably, the private key cannot be derived from the widely-distributed public key. Suppose that a trapdoor function – called a Secretly Embedded Trapdoor with Universal Protection (SETUP) – is embedded into the cryptosystem that allowed an attacker to access or derive the private key from the public key by weakening the key generation process (Esslinger, 2013; Young & Yung, 1996, 1997). For a practical application of kleptography, consider Edwards Snowden's revelation in 2013 that the NSA deliberately weakened NIST pseudo-random number generator (PRNG) standards, the methods at the very heart of generating secret keys and public key pairs (Zetter, 2013).

This paper poses several questions about reconciling personal privacy with the legitimate needs of the state to conduct investigations. This paper is not intended to answer those questions but to inform the debate. Other related questions might include:

1. Were any of us – as citizens and consumers – ever asked what we wanted, in terms of strong encryption?
2. Is the need for an individual's personal privacy superior to the State's need to investigate crimes?
3. Do we alter the government's duty to provide security with the implementation of processes that could block tools used to reach that objective?
4. Is the subjective expectation of privacy when using encryption so absolute that it meets the "objectively reasonable" test? In particular, does society agree?
5. How did we manage for the last 230 years without this level of protection from the State?

6. Who gave Apple, Google, et al. the right to have unilaterally made the decision about use of strong cryptography without an informed debate?

7. How do we resolve conflicts between the protections of two amendments?

The evolution of technology has always moved faster than the legislative process and the fact that both use a different vernacular does not help in the mutual understanding necessary for the implementation of good laws and regulations (Kessler, 1999). Society, however, cannot address these questions if we are not having the discussion. We cannot move forward toward any type of solution if the various stakeholders continue to hold on to decades-old arguments; our way of thinking about this topic must evolve since neither technology nor the law can afford to stand still.

In June 2020, the Lawful Access to Encrypted Data (LAED) Act was introduced in the U.S. Senate (Bradbury, 2020; Committee on the Judiciary, 2020; Franceschi-Bicchierai, 2020; S.4051, 2020). Legislators are again insisting that technology companies insert cryptographic backdoors into their products and requires similar backdoors in any platform supporting end-to-end encryption, so that they can comply with search warrants. The debate continues.

6. REFERENCES

1. 47 U.S. Code §230. Protection for private blocking and screening of offensive material. (1996, February). U.S. Code, Title 47. Telecommunications, Chapter 5. Wire or Radio Communication, Subchapter II. Common Carriers, Part I. Common Carrier Regulation. Retrieved from https://www.law.cornell.edu/uscode/text/47/230

2. Abel, R. (2019, July 1). Cellebrite Claims it Can Crack any iPhone or Android, Trump Admins Weigh Encryption Ban. *SC Magazine*. Retrieved from https://www.scmagazine.com/encryption-data-security/isreali-data-extraction-firm-cellebrite-announced-the-ability-to-break-into-any-iphone-or-android-device-for-law-enforcement-agencies-as-feds-weigh-banning-tough-encryption/

3. Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B., Specter, M., & Weitzner, D.J. (2015, July 6). *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*. MIT Computer Science and Artificial Intelligence Laboratory Technical Report (MIT-CSAIL-TR-2015-026). Retrieved from https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

4. Apple Inc. (2003, June 23). Apple Previews Mac OS X "Panther." *Press release*. Retrieved from https://www.apple.com/newsroom/2003/06/23Apple-Previews-Mac-OS-X-Panther/

5. Apple Inc. (2018, November 30). Use FileVault to Encrypt the Startup Disk on Your Mac. Retrieved from https://support.apple.com/en-us/HT204837

6. Armerding, T. (2017, March 8). Comey: Strong Encryption "Shatters" Privacy-Security Bargain. *CSO*. Retrieved from https://www.csoonline.com/article/3178299/comey-strong-encryption-shatters-privacy-security-bargain.html

7. Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security. (2019, July 23). Remarks as prepared for delivery, U.S. Department of Justice. Retrieved from https://www.justice.gov/opa/speech/ attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber

8. Blaze, M. (1994, August 20). Protocol Failure in the Escrowed Encryption Standard. In *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, pp. 59–67. Retrieved from http://www.mattblaze.org/papers/eesproto.pdf

9. Blaze, M., Diffie, W., Rivest, R.L., Schneier, B., Shimomura, T., Thompson, E., & Wiener, M. (1996, January). Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists. Retrieved from https://www.schneier.com/academic/paperfiles/paper-keylength.pdf

10. Blum, S. (2018, October 25). Apple Just Made Its Phones Impossible For Police to Hack. *Popular Mechanics*. Retrieved from https://www.popularmechanics.com/ technology/security /a24219241/apple-greykey-ios12-police-hacking/

11. Bradbury, D. (2020, July 8). LAED Act Poses Direct Threat to End-to-End Encryption. *infosecurity*. Retrieved from https://www.infosecurity-magazine.com/infosec/laed-act-threat-encryption/

12. Brewster, T. (2020, May 19). FBI Hacks iPhones in Pensacola Terrorist Shooting Case, But the War With Apple Goes On. *Forbes*. Retrieved from https://www.forbes.com/sites/thomasbrewster/2020/05/18/feds-hack-iphones-in-pensacola-case-apple-not-needed-after-all/#1f50e57575e9

13. Cardozo, N., & Crocker, A. (2018, April 2). The FBI Could Have Gotten Into the San Bernardino Shooter's iPhone, But Leadership Didn't Say That. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2018/04/fbi-could-have-gotten-san-bernardino-shooters-iphone-leadership-didnt-say

14. Claburn, T. (2019, December 10). Americans Should Have Strong Privacy-Protecting Encryption... That the Feds and Cops can Break, say Senators. *The Register*. Retrieved from https://www.theregister.co.uk/2019/12/10/us_congress_encryption_backdoor_hearings/

15. Clinton, B. (1996, November 15). *Executive Order (EO) 13026: Administration of Export Controls on Encryption Products*. Homeland Security Digital Library. Retrieved from https://www.hsdl.org /?abstract&did=799501

16. Cohen, A., & Park, S. (2018, Fall). Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries. *Harvard Journal of Law & Technology*, *32*(1), 169-234. Retrieved from https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech169.pdf

17. *Commonwealth v. Gelfgatt* (468 Mass 512, 2014). Retrieved from https://law.justia.com/cases/massachusetts/supreme-court/2014/sjc-11358.html

18. *Commonwealth v. Jones* (Mass SJC-12564, 481 Mass. 540, 552 n.14, 2019). Retrieved from https://cases.justia.com/massachusetts/supreme-court/2019-sjc-12564.pdf

19. Cope, S., Mackey, A., & Crocker, A. (2020, March 31). The EARN IT Act Violates the Constitution. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2020/03/earn-it-act-violates-constitution

20. Crypto Museum. (2018, November 25). Clipper Chip. Retrieved from https://www.cryptomuseum.com /crypto/usa/-clipper.htm

21. Diffie, W., & Hellman, M.E. (1976, November). New Directions in Cryptography. *IEEE Transactions on Information Theory*, *IT-22*(6), 644-654. Retrieved from https://ee.stanford.edu/∼hellman/publications/24.pdf

22. *Doe v. U.S.* (487 U.S. 201, 210, 1988). Retrieved from https://supreme.justia.com/cases/federal/us/487/201/

23. Electronic Communications Privacy Act (ECPA) of 1986 (18 U.S.C. §§ 2510-2523). Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

24. Electronic Frontier Foundation. (1998). *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. Sebastopol, CA: O'Reilly & Associates.

25. Electronic Privacy Information Center (EPIC). (n.d.a). Apple v. FBI. Retrieved from https://epic.org /amicus/crypto/apple/

26. Electronic Privacy Information Center (EPIC). (n.d.b). The Clipper Chip. Retrieved from https://www.epic.org/crypto/clipper/

27. Esslinger, B. (2013, February 20). The Dark Side of Cryptography: Kleptography in Black-Box Implementations (P. Vacek, Trans.). *Info Security*. Retrieved from https://www.infosecurity-magazine.com/magazine-features/the-dark-side-of-cryptography-kleptography-in/

28. Feiner, L. (2020, January 14). Apple Refuses Government's Request to Unlock Pensacola Shooting Suspect's iPhones. *CNBC*. Retrieved from https://www.cnbc.com/2020/01/14/apple-refuses-barr-request-to-unlock-pensacola-shooters-iphones.html

29. *Fisher v. U.S.* (425 U.S. 391, Case No. 74-18, 1976). Retrieved from https://caselaw.findlaw.com/us-supreme-court/425/391.html and https://supreme.justia.com/cases/federal/us/425/391/

30. Franceschi-Bicchierai, L. (2020, June 24). Republicans Who Don't Understand Encryption Introduce Bill to Break It. *Motherboard*. Retrieved from https://www.vice.com/en_us/article/y3z3z7/republican-encryption-bill-privacy-signal

31. *G.A.Q.L. v. State of Florida* (Case No. 4D18-1811, Fla 4th DCA, 2018). Retrieved from https://www.documentcloud.org/documents/5021228-181811-1704-10242018-09282906-I.html

32. Committee on the Judiciary. (2020, June 23). Graham, Cotton, Blackburn Introduce Balanced Solution

to Bolster National Security, End Use of Warrant-Proof Encryption That Shields Criminal Activity. *U.S. Senate*. Retrieved from https://www.judiciary.senate.gov/press/rep/releases/graham-cotton-blackburn-introduce-balanced-solution-to-bolster-national-security-end-use-of-warrant-proof-encryption-that-shields-criminal-activity

33. Haufler, H. (2003). *Codebreakers' Victory: How the Allied Cryptographers Won World War II*. New York: New American Library.

34. IEEE. (2018, June 24). In Support of Strong Encryption. *IEEE Position Statement*. Retrieved from http://globalpolicy.ieee.org/wp-content/uploads/2018/06/IEEE18006.pdf

35. *In re Apple AWA Application*. (ED No. 15-0451M, C.D. Cal, 2016). Retrieved from https://epic.org/amicus/crypto/apple/In-re-Apple-FBI-AWA-Application.pdf

36. *In re Apple AWA Order*. (No. ED 15-0451M, C.D. Cal, 2016). Retrieved from https://epic.org/amicus/crypto/apple/In-re-Apple-AWA-Order.pdf

37. *In re Apple Motion to Vacate*. (ED No. CM 16-10 (SP), C.D. Cal, 2016). Retrieved from https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf

38. *In Re Grand Jury Subpoena*. (670 F.3rd 1335, 11th Cir. 2012). Retrieved from https://www.courtlistener.com/opinion/624132/in-re-grand-jury-subpoena-duces-tecum/

39. *In re Search Warrant Application* (279 F. Supp. 3d 800, 805–06, N.D. Ill. 2017). Retrieved from https://www.leagle.com/decision/infdco20171011995

40. *In the Matter of the Search of a Residence in Aptos, California 95003*. (Case No. 17-mj-70656-JSC-1, 2018 WL 1400401, N.D. Cal, 2018). Retrieved from https://www.leagle.com/decision/infdco20180321a43

41. Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, revised ed. New York: Scribner.

42. *Katz v. U.S.* (389 U.S. 347, 88 S.Ct. 507, 19 L.Ed. 2d 576, 1967). Retrieved from https://supreme.justia.com/cases/federal/us/389/347/case.html

43. Kerckhoffs, A. (1883a, January). La Cryptographie Militaire. *Journal des sciences militaires*, *9*, 5-38.

44. Kerckhoffs, A. (1883b, February). La Cryptographie Militaire. *Journal des sciences militaires*, *9*, 161-191.

45. Kerr, O. (2018, April 29). Suspect Can Be Compelled to Decrypt Devices If Government Proves He Has The Ability To Do So, Court Rules. *The Volokh Conspiracy*. Retrieved from https://reason.com /2018/04/29/suspect-can-be-compelled-to-decrypt-devi

46. Kerr, O.S. (2019, March). Compelled Decryption and the Privilege Against Self-Incrimination. *Texas Law Review*, *97*(4), 767-799. Retrieved from https://texaslawreview.org/wp-content/uploads/2019/03/Kerr.V97.4.pdf

47. Kessler, G.C. (1999, September). Catch My Drift? Can You Define "Digital Signature" in Non-Technical Terms? The Future of E-Commerce Law May Depend on it. *Information Security Magazine*. Retrieved from https://www.garykessler.net/library/is_language.html

48. Kessler, G.C. (2020, June 1). An Overview of Cryptography. Retrieved from https://www.garykessler.net/library/crypto.html

49. Lee, T.B. (2020, June 24). It's Unconstitutional For Cops to Force Phone Unlocking, Court Rules. *Ars Technica*. Retrieved from https://arstechnica.com/tech-policy/2020/06/indiana-supreme-court-its-unconstitutional-to-force-phone-unlocking/

50. Levy, S. (1999, April). The Open Secret. *WIRED Magazine*, *7*(**??**). Retrieved from http://www.wired.com/wired/archive/7.04/crypto.html

51. Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age.* New York: Viking Press.

52. Lucas, S. (2020, January 13). Apple Said it is Helping in the Pensacola Shooting Investigation, But it Won't Unlock the Shooter's iPhone. *BuzzFeed News*. Retrieved from https://www.buzzfeednews.com/article/scottlucas/william-barr-apple-request-unlock-iphones

53. Marks, L. (1998). *Between Silk and Cyanide: A Codemaker's War, 1941-1945*. New York: The Free Press (Simon & Schuster).

54. Meeks, B.N. (1994, September 1). Clipping Clipper: Matt Blaze. *WIRED*. Retrieved from https://www.wired.com/1994/09/clipping-clipper-matt-blaze/

55. Miller, J. (2014, September 19). Google and Apple to Introduce Default Encryption. *BBC News*. Retrieved from https://www.bbc.com/news/technology-29276955

56. Nakashima, E. (2008, January 16). In Child Porn Case, a Digital Dilemma. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2008/01/15/AR2008011503663.html

57. National Institute of Standards & Technology (NIST). (2018, October 10). *Cryptographic Standards and Guidelines: AES Development*. Information Technology Laboratory, Computer Security Resource Center. Retrieved from https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development

58. Newman, L.H. (2020, March 5). The EARN IT Act is a Sneak Attack on Encryption. *WIRED*. Retrieved from https://www.wired.com/story/earn-it-act-sneak-attack-on-encryption/

59. Ng, A. (2020, July 2). Why Your Privacy Could be Threatened by a Bill to Protect Children. *CNET*. Retrieved from https://www.cnet.com/news/why-your-privacy-could-be-threatened-by-a-bill-to-protect-children/

60. *Olmstead v. U.S.* (277 U.S. 438, 19 F. (2d) 842, 848, 850, affirmed, 1928). Retrieved from https://www.law.cornell.edu/supremecourt/text/277/438

61. On Lawful Criminal Investigation That Respects 21st Century Data Protection. (2016, May 20). Europol and ENISA Joint Statement. Retrieved from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

62. OSXDaily. (n.d.). What is FileVault? FileVault for Mac Explained. Retrieved from http://osxdaily.com /what-is-filevault/

63. Painter, L. (2020, June 22). Complete List of Mac OS X & MacOS Versions. *Macworld*. Retrieved from https://www.macworld.co.uk/feature/mac/mac-os-x-macos-version-code-names-3662757/

64. Pfefferkorn, R. (2020, January 30). The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning it. *The Center for Internet and Society at Stanford Law School*. Retrieved from https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it

65. Rangaviz, D.R. (2019, October 22). Brief Of Amicus Curiae Committee For Public Counsel Services In Support Of Petition For A Writ Of Certiorari: Dennis Jones, Petitioner, v. Commonwealth Of Massachusetts, Respondent (No. 19-6275). Retrieved from http://www.supremecourt.gov/DocketPDF/19/19-6275/120068/20191024102615254_Jones%20v.%20Massachusetts%20CPCS%20Amicus%20Brief.pdf

66. Reidy, J.A., & Nathanson, D. (2019, August 7). Petition for a Writ of Certiorari: Dennis Jones, Petitioner v. Commonwealth of Massachusetts, Respondent (No. 19-6275). Supreme Court of the United States. Retrieved from http://www.supremecourt.gov/DocketPDF/19/19-6275/118752/20191010183703372_Jones%20Cert%20Petition%20Final.pdf

67. Rivest, R.L., Shamir, A., & Adleman, L. (1978, February). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126. Retrieved from https://people.csail.mit.edu/rivest/Rsapaper.pdf

68. S.3398. (2020, March 5). EARN IT Act of 2020: A Bill to Establish a National Commission on Online Child Sexual Exploitation Prevention, and for other purposes. *116th Congress (2019-2020)*. Retrieved from https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

69. S.4051. (2020, June 23). Lawful Access to Encrypted Data Act. *116th Congress (2019-2020)*. Retrieved from https://www.judiciary.senate.gov/download/s4051_-lawful-access-to-encrypted-data-act

70. Sacharoff, L. (2018). Unlocking the Fifth Amendment: Passwords and Encrypted Devices. *Fordham Law Review*, *87*(1). Retrieved from https://ir.lawnet.fordham.edu/flr/vol87/iss1/9

71. Schmidt, M.S., & Pérez-Peña, R. (2015, December 4). F.B.I. Treating San Bernardino Attack as Terrorism Case. *The New York Times*. Retrieved from https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html

72. Schneier, B. (2004, October 6). The Legacy of DES. *Schneier on Security*. Retrieved from https://www.schneier.com/blog/archives/2004/10/the_legacy_of_d.html

73. *Seo v. State* (109 N.E.3d 418, 425–31, Ind. Ct. App. 2018). Retrieved from https://www.leagle.com/decision/ininco20180821261

74. *Seo v. State* (Supreme Court Case No. 18S-CR-595, 2020). Retrieved from https://www.eff.org/files/2020/06/23/opinion_issued_reversed_and_rem.pdf

75. Singh, S. (1999). *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography.* New York: Doubleday.

76. *Smith v. Maryland* (442 U.S. 735, 1979). Retrieved from https://supreme.justia.com/cases/federal/us/442/735/

77. *State of Florida v. Stahl* (206 So. 3d 124, 136–37, Fla 2nd DCA, 2016). Retrieved from https://www.leagle.com/decision/inflco20161207102

78. Stepanovich, A., & Karanicolas, M. (2018, March 2). Why An Encryption Backdoor for Just the "Good Guys" Won't Work. *Just Security*. Retrieved from https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

79. Sussman, V. (1995, March 26). Lost in Kafka Territory. *U.S. News & World Report*. Retrieved from https://web.archive.org/web/20130616165334/http://www.usnews.com/usnews/news/articles/950403/archive_010975.htm

80. TrueCrypt. (2015, July 31). TrueCrypt Version History. Retrieved from https://www.truecrypt71a.com/documentation/version-history/

81. TrueCrypt Foundation. (2012, February 7). *TrueCrypt User's Guide*, version 7.1a. Retrieved from https://www.grc.com/misc/truecrypt/ TrueCrypt%20User%20Guide.pdf

82. *U.S. Const. amends. IV, V.*

83. U.S. Department of Commerce. (2000, January 10). *Revisions to Encryption Items.* Bureau of Export Administration, 15 CFR Parts 734, 740, 742, 770, 772, and 774. Retrieved from https://epic.org /crypto/-export_controls/regs_1_00.html

84. U.S. Supreme Court. (2019, October 16). Petition for a Writ of Certiorari Related to Dennis Jones, Petitioner v. Massachusetts (No. 19-6275). Retrieved from https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/19-6275.html

85. *U.S. v. Apple MacPro Computer* (851 F.3d 238, 248 & n.7, 3d Cir. 2017). Retrieved from https://www.leagle.com/decision/infco20170320056

86. *U.S. v. Boucher* (2007 WL 4246473, 2009). Retrieved from http://www.volokh.com/files/Boucher.pdf

87. *U.S. v. Fricosu* (841 F. Supp. 2d 1232, 1237, D. Colo. 2012). Retrieved from https://www.leagle.com/decision/ inadvfdco120925000244

88. *U.S. v. Hubbell* (530 U.S. 27, 2000). Retrieved from https://supreme.justia.com/cases/federal/us/530/27/

89. *U.S. v. Spencer* (No. 17-CR-00259-CRB-1, 2018 WL 1964588, N.D. Cal, 2018). Retrieved from https://orinkerrblog.files.wordpress.com/2018/04/usvspencer.pdf

90. Warren, S., & Brandeis, L. (1890, December 15). The Right to Privacy. *Harvard Law Review*, *4*, 193. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

91. Written Testimony for the United States Senate Committee on the Judiciary on Smartphone Encryption and Public Safety. (2019, December 10). Manhattan District Attorney's Office. Retrieved from https://www.manhattanda.org/written-testimony-for-the-united-states-senate-committee-on-the-judiciary-on-smartphone-encryption-and-public-safety/

92. Yardley, H.O. (1931). *The American Black Chamber*. Indianapolis: The Bobbs-Merrill Company.

93. Young, A., & Yung, M. (1996). The Dark Side of Black-Box Cryptography, or: Should We Trust Capstone? In N. Koblitz (Ed.), *Advances in Cryptology – CRYPTO '96: 16th Annual International Cryptology Conference*, Santa Barbara, California, August 18–22 (pp.89-103). New York: Springer. Retrieved from https://www.researchgate.net/publication/225139661_The_Dark_Side_of_Black-Box_Cryptography_or_Should_We_Trust_Capstone

94. Young, A., & Yung, M. (1997). Kleptography: Using Cryptography Against Cryptography. In W. Fumy (Ed.), *Advances in Cryptology - EUROCRYPT '97: International Conference on the Theory and Application of Cryptographic Techniques*, Konstanz, Germany, May 11-15 (pp.62-74). New York: Springer-Verlag. Retrieved from https://www.researchgate.net/publication/221348188_Kleptography_Using_Cryptography_Against_Cryptography

95. Zetter, K. (2013, September 24). How a Crypto 'Backdoor' Pitted the Tech World Against the NSA. *Wired Magazine*. Retrieved from https://www.wired.com/2013/09/nsa-backdoor/

96. Zimmermann, P. (n.d.). Philip Zimmermann. Retrieved from https://philzimmermann.com/EN/background/index.html

97. Zimmermann, P. (1999). Why I Wrote PGP. Retrieved from https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

98. Zimmermann, P. (2001, June 5). PGP Marks its 10th Anniversary. Retrieved from http://www.philzimmermann.com/EN/news/PGP_10thAnniversary.html

Privacy issues and the law	Timeline	Issues and events
	2600 BCE	Writing appears
	1900 BCE	Secret writing appears
U.S. Constitution ratified	1789	
Bill of Rights ratified	1791	
"The Right to Privacy"	1890	
	1914-1918	Cryptography in WW I
Olmstead v. U.S.	1928	
	1939-1945	Cryptography in WW II
	1948	Cryptography classified as a munition
Katz v. U.S.	1967	
	1969	Advanced Research Projects Agency Network (ARPANET)
Fisher v. U.S.	1976	PKC concept described
	1977	DES released
	1978	RSA described
Smith v. Maryland	1979	
	1985	National Science Foundation Network (NSFNET)
Electronic Communications Privacy Act	1986	
Doe v. U.S.	1988	
	1991	PGP released on the Internet
		Commercialization of the Internet
	1993	FBI starts Zimmermann investigation
		Capstone program proposed
	1995	Zimmermann receives EFF Pioneer Award
		SSL introduced
	1996	FBI closes Zimmermann investigation
		Capstone project dead
		EO 13026 released
		Blaze et al.: "56-bit keys are dead"
	1997	NIST starts AES process
		"Kleptography" defined
	1998	EFF Deep Crack chip: "DES is dead"
U.S. v. Hubbell	2000	Commerce Dept. reclassifies cryptography
	2001	AES adopted
	2003	FileVault (home directory) released
	2004	TrueCrypt and plausible deniability released
U.S. v. Boucher	2009	
	2011	FileVault 2 (full volume) released
In Re Grand Jury Subpoena U.S. v. Fricosu	2012	
	2013	Snowden revelations about NSA
Commonwealth v. Gelfgatt	2014	Android 5.0 introduces default encryption
		Apple iOS 8 introduces default encryption
	2015	San Bernardino terrorist shooting
State of Florida v. Stahl	2016	FBI versus Apple
U.S. v. Apple MacPro Computer	2017	Crypto backdoors back in public discussion
G.A.Q.L. v. State of Florida	2018	
U.S. v. Spencer		
Seo v. State		
Commonwealth v. Jones	2019	NAS Pensacola terrorist shooting
SCOTUS denies certiorari in Jones		
EARN IT Act introduced in U.S. Senate	2020	
LAED Act introduced in U.S. Senate		
Seo v. State upheld		

Table 1. Timeline