Passwords, Biometrics, & the Evolving Legal Status of Encryption

CSS 3XX

University of Washington, Bothell

***Abstract*—An analysis of current trends and important considerations in recent case-law dealing with password protection and personal devices.**

***Keywords*—Biometrics; Encryption; Foregone Conclusion; Legal Precedent; Password; Self-Incrimination**

I. INTRODUCTION

Countries all over the world have found themselves in a constant struggle, as old precedent in legal systems and laws fail to keep pace with today's technological progress. Nowhere is this struggle highlighted better than in the United States with the emergence of digital technologies. Since the U.S. Constitution was adopted as the supreme law of the land, courts, citizens, and governments have battled over just how broadly certain rights guaranteed by the founding document can be interpreted. As new technological opportunities appear to exercise constitutional rights, amendments inevitably have to be re-examined in scope and application for contemporary usage.

The 1st Amendment guarantees the rights of free speech and a free press. Courts have had to determine if such rights – originally intended for publishers of newspapers – apply equally to the radio, television, and internet, where knowledge can spread with faster impact and broader reach. The 2nd Amendment guarantees the civilian right to bear arms. Although originally intended to protect ownership of slow firing muskets, governments are now conflicted by advancements in firearm technology resulting in the modern day ownership of civilian assault rifles.

Finally, with the emergence of personal digital devices such as iPhones and laptops, coupled with the increasing sophistication of digital encryption, courts have now found themselves having to make similarly tough judgments on the extent of the 4th Amendment's right against unreasonable search and seizure [1] and the 5th Amendment's right against self-incrimination [2], the most basic underpinnings of U.S. criminal law.

II. NATURE OF CASES

Currently, criminal syndicates and persons across the country have taken to using digital devices to communicate, organize, and commit crimes. When members of such groups – or suspected individuals – are arrested, investigators and authorities have a keen interest in discovering evidence related to the crime, which may be contained in captured pictures, private communications, and other data. The modern handheld smartphone finds itself as the perfect device for such tasks; criminals can use them on-the-go, scoping out targets, navigating locations, chatting with co-conspirators, and organizing plans-of-action. This makes them among the most valuable pieces of evidence investigators can obtain.

But in the process of obtaining access to suspect's devices, authorities have run into two hard roadblocks: First, due to the very private and sensitive nature of personal phones, without a search warrant, any evidence found on the device may be tossed in court as inadmissible according to the 4th Amendment protection from unreasonable search and seizure [1]. Second, most phones (particularly those utilized by criminals) are password protected, meaning that forcing a suspect to unlock their personal device may run afoul of their 5th Amendment protection against self-incrimination [2]. Revealing a password may be considered 'testimony' which might result in incrimination and finding themselves guilty.

Enter a loophole: The Foregone Conclusion doctrine. The Foregone Conclusion doctrine has been used by a number of courts in recent years to avoid the trouble of 5th Amendment protection, allowing authorities to force a suspect to unlock his or her phone in the specific instance where *the contents behind the lock are already known to the court.* In a hypothetical example, if a suspect all but admitted that the content behind a password is incriminating, the court may believe the password no longer has any legal value, and so it may be surrendered. Versions of this reasoning have already been used against digital passwords for specific cases in the state of New Jersey [3]. The legal precedent in both Foregone Conclusion and password locked devices under digital encryption is

extremely under-developed, resulting in many courts defaulting to case-law from several decades ago in order to justify their judgments.

III. LEGAL PRECEDENT

The closest analogy found for the modern day predicament of a device secured with an encryption lock, is that of a safe or vault secured with a physical lock. In the past, when suspects were arrested, it was sometimes believed that they had hidden criminal evidence in such vaults, preventing authorities from obtaining access to it. Similarly, authorities would then appeal to the judge requesting an order forcing the suspect to reveal the key combination to the lock of the vault. The result on whether this request was granted usually depended on Foregone Conclusion (the contents of the safe or vault are already known to the court). If the suspect was seen by a witness moving illegal items into the vault, then that may be enough justification to authorize officers to force a suspect to unlock the vault. However, if the suspect argued that the vault was not his own, then the act of 'forcing' him to unlock the vault would prove it was his and effectively make him self-incriminate himself. Due to these challenges, judges usually take a dim view of using the Foregone Conclusion doctrine widely, and only in the most narrow of circumstances will permit the doctrine's use.

IV. BIOMETRICS AND PASSCODES

Complicating the issue even further is when a judge indeed orders a suspect to unlock his or her device but the suspect *refuses to comply*. In such cases, the 'type' of key used to secure the locked device is crucial. If the key is of a 'passcode' type, such as a PIN or password, the court may find itself out of luck, since there is no humane or legally accepted way to force a key combination out of a person's mind, disregarding the already troubling 5th Amendment concerns. However, if the key is of a 'biometric' type, such as a faceID or fingerprint pattern, the device may be unlocked by simply forcing the suspect to use his physical features to unlock the device. Actions like this are interpreted in much the same way as taking a suspect's fingerprints after arrest would be, or obtaining a DNA sample for evidence, and since a suspect's physical features are not 'testimony', a forced biometric unlock does not run into as much 5th Amendment defense [4][5].

Regardless of a suspect's willingness to unlock a passcode-type encrypted device, a judge has the ability to hold the suspect in 'contempt of court'. This means the suspect may be jailed for as long as they do not comply with the judge's order to unlock the device. This has occurred on one high profile occasion where a judge ruled a man as in contempt for refusing to decrypt a number of external harddrives suspected to contain illegal material; the suspect was held in jail under the contempt order for four years before a federal court acted, ruling that the upper limit on such punitive jailtime was limited to eighteen months [6].

The legal landscape around forced device searches and unlocks is varied across the nation. For every case where a judge may appear to force a suspect to unlock their phone, there also exists examples in the opposite direction, pointing towards constitutional rights; some have ruled that even turning a suspect's phone on without a warrant and seeing the lock screen is illegal. A recent example in Washington state even had a man sue the FBI over taking a picture of his phone's lock screen since the agency did not receive prior approval from a court to 'search' the phone, making the a single picture of evidence a violation of the suspect's 4th Amendment rights.

V. COMPANIES' LEGAL ROLES

Looking at the device user's side of the investigation may also obscure other areas the prosecution may leverage in discovering evidence. The clearest and highest profile instance of this was the FBI-Apple Encryption Dispute in the wake of the 2016 San Bernardino terror attacks in California. Both suspects were killed in a shootout with police, and both had destroyed their personal phones before the firefight. However, one of the suspect's had left an operable work-phone behind, one that the FBI believed might have more information on the attack and if it had any links to international terror groups.

However, the iPhone had Apple encryption on it due to a password being set. The FBI went straight to Apple and attempted to strong-arm them into breaking their own encryption, but the company refused to comply with the agency arguing that it would permanently weaken their device security [7]. The FBI filed suit against Apple in response, leading to a months-long legal battle. The FBI, realizing their bid to force Apple into opening the phone wasn't working out as planned, contracted an outside company to extract the contents of the phone [8]. Although the phone was set to delete all its data if too many incorrect passwords were attempted, the firm used a hardware-level lightning-port exploit allowing infinite attempts. Eventually the phone's password was brute-forced and the contents were opened to the FBI, however nothing pertinent to the investigation was discovered.

What is the lesson that can be taken from Apple's dispute with the FBI? Primarily, that for best security a suspect must not only watch what type of lock type he utilizes (ideally passcode), but also what company he trusts on the software and hardware end to not compromise and break their security under government pressure. From this incident, it's clear that companies such as Apple are a fairly good choice, and they have set a standard for protecting their customer's security in criminal cases, to the point where they will even risk being sued for such protection.

VI. CONCLUSION

Although more and more cases involving digital passwords rights are popping up every year, the U.S. court system remains heavily divided on to what extent authorities can force compliance out of suspects in unlocking their personal devices. Eventually, the issue of digital devices will likely find itself being debated in the Supreme Court. Until then, different jurisdictions across the country will hold differing standards and precedent, creating a complicated legal framework that still has yet to be fully navigated. In the meantime, the best protection a suspect might have is rejecting biometric locks in favor of passcode locks, and placing trust in companies with proven track records of not compromising their devices security. For investigators, the most powerful tool has worked out to be establishing that any evidence behind a lock falls under the 'Foregone Conclusion' doctrine, as well as flexing government muscle at companies who may be willing to compromise their customers' devices.

REFERENCES

[1] K. Cox, "Just turning your phone on qualifies as searching it, court rules," *Ars Technica*, 21-May-2020. [Online]. Available: https://arstechnica.com/tech-policy/2020/05/just-turning-your-phone-on-qualifies-as-searching-it-court-rules/.

[2] D. Goodin, "Suspect can't be compelled to reveal '64-character' password, court rules," *Ars Technica*, 23-Nov-2019. [Online]. Available: https://arstechnica.com/tech-policy/2019/11/police-cant-force-child-porn-suspect-to-reveal-his-password-court-rules/.

[3] B. D. Greenberg, "The 'Foregone Conclusion' Doctrine Requires a Criminal Defendant to Reveal the Passcode to His Passcode-Protected Cellphone," *Appellate Law NJ Blog*, 11-Aug-2020. [Online]. Available: http://appellatelaw-nj.com/the-foregone-conclusion-doctrine-requires-a-criminal-defendant-to-reveal-the-passcode-to-his-passcode-protected-cellphone/.

[4] C. Long, "Can law enforcement make you unlock your phone using your fingerprint?," *Neighborhood Justice Center*, 06-Jul-2020. [Online]. Available: https://www.njcinc.org/resourcecenter/can-law-enforcement-use-your-fingerprint-to-unlock-your-phone.

[5] C. Burt, "U.S. judge allows law enforcement to compel suspect to unlock smartphone with biometrics: Biometric Update," *Biometric Update* |, 26-Apr-2019. [Online]. Available: https://www.biometricupdate.com/201904/u-s-judge-allows-law-enforcement-to-compel-suspect-to-unlock-smartphone-with-biometrics.

[6] T. B. Lee and skyywise Ars Scholae Palatinae jump to post, "Man who refused to decrypt hard drives is free after four years in jail," *Ars Technica*, 12-Feb-2020. [Online]. Available: https://arstechnica.com/tech-policy/2020/02/man-who-refused-to-decrypt-hard-drives-is-free-after-four-years-in-jail/.

[7] "Customer Letter," *Apple*. [Online]. Available: https://www.apple.com/customer-letter/.

[8] R. A. Ellen Nakashima, "The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm.," *The Washington Post*, 14-Apr-2021. [Online]. Available: https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/.