The Law and Encryption Workarounds

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 406: Cyber Law, Professor Amanda Cheney

March 6, 2025

Article Source:

Kerr, O. S. (2016, October 14). *The Law of Encryption Workarounds*. Retrieved from reason: Free Minds and Free Markets: https://reason.com/volokh/2016/10/14/the-law-of-encryption-workarou/

Assignment

Review the article below by Orin Kerr, an important, scholarly voice in so many Fourth Amendment debates, and preferably other sources to help form your opinions about the legal, policy and technical challenges posed by encryption.

The impact of encryption on legitimate law enforcement and national security investigations is no small thing, and it won't go away any time soon. No matter where you stand, there are consequences to the choices we, as a nation and people, make. It's another "wicked" problem - not a simple one - and we need to be willing to think through our choices, in good faith, and rely on the best available facts and what we believe will best promote security and freedom and privacy. Be open-minded. If you think there are easy answers to the challenges of encryption in a free yet secure society, think twice.

Then use what you've learned to:

1. Identify in your initial post **a point(s)** or **general assertion(s)** by Orin Kerr that surprised you, challenged you or led you to agree or disagree with him, and explain why.
    a. In so doing use this article (and perhaps others' articles) as a platform to address the legal, policy, and technical challenges posed by encryption.
    b. In your posts you may also consider what the rest of the world is doing in responding to the challenges of encryption.

Article Summary with Updated Case Law Information

Kerr discusses law enforcement's difficulties with accessing encrypted information about suspects. Unless the government can crack the encryption with its current technological tools or access places where the data is unencrypted, the encryption is impenetrable and can negatively impact investigations (Kerr, 2016). Thus, when suspects and targets encrypt their data, many law enforcement will resort to legal workarounds to decrypt the data or access unencrypted forms of the data for further investigation.

Kerr discusses three situations displaying law enforcement workarounds for encryption (Kerr, 2016). The first example is Apple vs. FBI: a deceased suspect contained encrypted data in their iPhone, and the government could not obtain the password to the device nor decrypt the data themselves. The US government demanded that Apple provide access to the encrypted data on the phone; however, Apple refused to comply for fear of (1) setting a dangerous precedent and weakened security for all its users and (2) a mandated backdoor that could be misused in future cases by the government. The government eventually dropped the case against Apple because it found a non-US third-party contractor to decrypt the phone to gain access to the deceased suspect's data.

The second case Kerr discusses is about the Fifth Amendment and limits to decryption. When Kerr wrote this article in 2016, the following case was still pending; however, in 2019, the Commonwealth v. Dennis Jones case did conclude. The legal issue was "whether and when the Fifth Amendment allows the government to order the defendant to decrypt" devices and hard drives (Kerr, 2016). Investigators had a legal warrant to search the defendant's devices and hard drives for any incriminating evidence about their case; however, the devices and hard drives were encrypted, the investigators could not decrypt the hardware themselves, and they needed the

passwords to access the encrypted information. The government demanded that the defendant surrender the passwords to the investigators to decrypt the data, but the defendant refused. The defendant argued that the password to decrypt the devices and hard drives would violate his constitutional privileges against self-incrimination under the Fifth Amendment (JUSTIA, 2024).

The case eventually reached the Massachusetts Supreme Judicial Court. The court concluded that law enforcement and the Commonwealth had established beyond a reasonable doubt that Jones knew the password to the cell phone, satisfying the foregone conclusion exception. The forgone conclusion exception allows the government "to compel the production of evidence if it can demonstrate that the existence, possession, and authenticity of the evidence are already known, rendering the act of production non-testimonial" (Mehta, 2023). Also, compelling the defendant to enter the password did not violate his privilege against self-incrimination.

The last case Kerr discusses is the Playpen warrant. The phrase "Playpen" refers to a US federal judge in 2015 granting a warrant authorizing government law enforcement to insert malware into specific websites on the dark web depicting illegal and obscene content like child pornography (e.g., the *Playpen website)*. The purpose of the malware was to help government officials track visitor computers for information and work around anonymity protection software used like Tor that hides IP addresses, thereby thwarting the use of many traditional surveillance tools (EFF, 2025). Since 2015, there have been mixed feelings about the legality of the Playpen warrant. Some states have ruled the warrant invalid, while others upheld its use under the good faith exception.

Cautiously agree with Kerr...

I cautiously agree with Kerr's points in the article. Finding legal means to decrypt data related to case targets can make it more difficult for law enforcement to do their jobs swiftly and thoroughly. They also need better technological tools to decrypt the data without compromising its integrity and more streamlined workarounds that do not violate the law. However, increases in checks and balances, accountability, and appropriate punishments for violating the law should match when there are any increases in the power of law enforcement and government.

In the first example of Apple v. FBI, Apple's concerns are valid, and there are a few more. Backdoors may present vulnerabilities or become vulnerable to new forms of technology in the next 5-20 years (e.g., WEP and WPA/2/3 wireless technologies). Unless backdoor security pathways are updated, patched, and enhanced to meet current security demands and compliance regulations, then the backdoor security pathways will become an easy attack vector for hackers to abuse. Also, the public disclosure of a backdoor to an encryption program will create new legal, economic, technological, and interpersonal problems with the organizations' users.

In the second case, Commonwealth v. Dennis Jones (2019), I agree with the state decision that law enforcement had enough reason that Jones knew the passwords to his devices and hard drives that the encrypted devices had relevant information to the defendant's case. There were no Fifth Amendment rights violations for the defendant when compelled to provide his device passwords. From my understanding, compelling one to provide their password to an encrypted device is like providing the physical key/key code to a person's safe in their house to access secure information that may have evidence for court use. Requesting access to secure information is not self-incrimination and is not a violation of one's Fifth Amendment rights. The information in the secure devices determines whether the defendant is innocent or guilty; giving someone access to

your device, car, house, or safe is not self-incriminating. Other states like Utah and New Jersey have followed the same suit; however, SCOTUS has not taken any similar cases, and Congress has not passed any federal laws specifically addressing whether law enforcement can compel someone to decrypt their device.

In the third case, the Playpen warrant poses several interesting dynamics (EFF, 2025). The good faith exception protects law enforcement when they act under a warrant that is later found to be legally flawed. It is a good step in the right direction due to the absence of any concrete legislation or decision from SCOTUS and Congress. In 2016, there was a change in Rule 41, allowing federal judges to issue warrants for remote searches and remote searches across multiple districts when computers were using concealing tools like Tor (DOJ, 2016)**.** However, the FBI can easily abuse this principle and power worldwide, exceeding their legal warrant's jurisdiction and boundaries, leading to possible Fourth Amendment violations. Also, I understand using a website to draw out specific kinds of people and monitor them like a Honeypot. However, there are ethical and legal concerns when allowing nefarious sites like *Playpen* to stay active and keep running, potentially facilitating the distribution of illegal content.

Conclusion: Global Responses and Encryption Workarounds

Many countries combine technology, law, and severe punitive punishments to work around data encryption of suspected/qualified targets. In the United Kingdom, the Regulation of Investigatory Powers Act (RIPA) allows police to demand compliance with access requests. Refusal to provide PINs, passwords, or biometric data for device access is considered a criminal offense (Leyden, 2025). Other countries that follow a similar path to the United Kingdom are South Africa, France, and the Netherlands. They permit law enforcement with a warrant to order persons

with knowledge of how to access systems to share their expertise, including knowledge of data encryption. Otherwise, the compelled persons may receive hefty fines and/or imprisonment.

The most unique workaround I discovered was that in a global operation led by the US FBI, law enforcement agencies from 16 countries developed an encryption company called ANOM, which provided over 12,000 encrypted devices to criminals (DOJ, 2021). That allowed authorities to eavesdrop and intercept communications. However, increases in checks and balances, accountability, and appropriate punishments for violating the law should match when there are any increases in the power of law enforcement and government. Otherwise, these organizations, governments, and countries will abuse their power and strip many precious rights of their citizens, erasing any concept of privacy and self-autonomy.

References

BBC. (2025, February 7). *UK demands access to Apple users' encrypted data*. Retrieved from BBC: https://www.bbc.com/news/articles/c20g288yldko

DOJ. (2016, June 20). *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*. Retrieved from US Department of Justice (DOJ): https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches

DOJ. (2021, June 8). *FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown*. Retrieved from US Department of Justice (DOJ): https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive

EFF. (2025, January 16). *The Playpen Cases: Frequently Asked Questions*. Retrieved from Electronic Frontier Foundation (EFF): https://www.eff.org/pages/playpen-cases-frequently-asked-questions

Hager, N. (2021, February 22). *SCOTUS Asked If 5th Amendment Bars Compelling Defendants to Unlock Electronic Devices*. Retrieved from The Federalist Society: https://fedsoc.org/commentary/fedsoc-blog/scotus-asked-if-5th-amendment-bars-compelling-defendants-to-unlock-electronic-devices

JUSTIA. (2024, September 10). *Commonwealth v. Jones*. Retrieved from JUSTIA U.S. Law: https://law.justia.com/cases/massachusetts/supreme-court/2019/sjc-12564.html

Kerr, O. S. (2016, October 14). *The Law of Encryption Workarounds*. Retrieved from reason: Free Minds and Free Markets: https://reason.com/volokh/2016/10/14/the-law-of-encryption-workarou/

Leyden, J. (2025, January 31). *How law enforcement agents gain access to encrypted devices*. Retrieved from CSO: https://www.csoonline.com/article/3812874/how-law-enforcement-agents-gain-access-to-encrypted-devices.html

Mehta, G. (2023, November 2). *Foregone Conclusion Doctrine Allows Government to Make Criminal Defendant Disclose Computer Password*. Retrieved from Goldstein Mehta LLC, Attorneys at Law: https://goldsteinmehta.com/blog/foregone-conclusion-doctrine

Secured, A. T. (2025, February 26). *Backup, The UK wants to see your Photos & iCloud*. Retrieved from YouTube: https://www.youtube.com/watch?v=svsvRfpxbNg