"Going Dark":

An Overview and Analysis of Former FBI Director James Comey's Security Concerns about Law Enforcement and Encryption

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 406: Cyber Law, Professor Amanda Cheney

February 26, 2025

Assignment:

a) *Review Lawfare Podcast Episode # 96 below discussion former FBI Director Jim Comey's comments on "Going Dark" and questions from the audience.*

Identify in your initial post a point(s) or general assertion(s) by former FBI Director Comey that surprised you, challenged you or led you to agree or disagree with him, and explain why. In so doing use this podcast as a platform to address the legal, policy, and technical challenges posed by encryption. In your posts you may also consider what the rest of the world is doing in responding to the challenges of encryption.

Source:

Brookings. (2014, October 16). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Retrieved from Brookings: https://www.brookings.edu/events/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course/

https://www.lawfareblog.com/lawfare-podcast-episode-96-james-comey-going-dark

a) Lawfare Podcast Episode #96, discussion with former FBI Director Jim Comey

What is “Going Dark”?

James Comey describes 'Going Dark' as the challenge law enforcement faces when criminals and terrorists use strong encryption protocols and tools to communicate, making it difficult or impossible for authorities to legally access their messages, even with a legal warrant (Brookings, 2014). Those trying to protect the people are not always able to access the evidence they need to prosecute criminals and prevent serious crimes like terrorism, human trafficking, and cybercrime, even with lawful authority. "And when authorities have the legal authority to intercept access communications and information under a court order, they may often lack the technical ability, especially with devices' growing diversity and complexity" (Brookings, 2014). Authorities may also not lawfully be able to switch surveillance between devices, methods, and networks while in pursuit of a criminal when the criminal changes their methods of communication. Thus, the increasing power and complexity of publicly available encryption protocols and tools can become a life-threatening obstacle and a 'double-edged' sword for both authorities and the public.

Comey's Solution

Comey states there are two primary technological challenges when it comes to encryption: (1) Court order interception of real-time data or data in motion, and (2) Court order interception of data at rest or data stored on our devices (Brookings, 2014). To help streamline and speed up the process of fighting against crime using encryption protocols and tools, Comey encourages phone carriers and hardware/software manufacturers to build more straight-forward 'secure backdoors' to encrypted devices and data: this provides law enforcement access points when communications and tech companies are presented legal warrants by the authorities. Comey states

the goal is to keep up with technology to collect the data communications they are legally authorized to do so by the rule/letter of the law, not further expand beyond its Constitutional authority and abuse such power (i.e., government overreach). Therefore, Comey wants the communication providers to build more intercept capabilities or legal pathways for law enforcement to catch only the bad guys, thereby updating and expanding the 1994 Communications Assistance for Law Enforcement Act (CALEA).

According to Comey, one modern-day technological problem is phone manufacturers and carriers designing and enabling their devices with a 'default encryption' mindset, preventing them and the authorities from unlocking the devices to reveal personal information without the required passkeys. For example, an alleged criminal offender may use the latest Apple iPhone or Sony's Samsung Galaxy to conduct illegal activities through encrypted communication methods. Though criminals may have the option to back their data on the cloud, they probably will not do so: saving their phone calls, messages, and other sensitive data on the cloud also saves it on the provider's servers, where authorities can legally access and gather that information without fear of user encryption. Without a simple backdoor to accessing the encrypted information or the password/passphrase, the information is 'lost forever'—a criminal can decline to provide a password to the device and accept a lesser punishment from authorities when compared to sharing the sensitive data to authorities and being prosecuted and punished for more serious crimes. Therefore, without more straightforward access to the sensitive data on a locked phone, Comey states authorities will have more difficulty obtaining information to locate the potential offenders and/or less evidence to use in court prosecutions.

Other countries are implementing a wide variety of stricter laws governing encryption or outright banning it from public use. For example, countries like Australia (TOLA Act, 2018) and

India (Intermediary Guidelines, 2021) require tech companies to provide law enforcement backdoors to access encrypted data. Some countries like Russia (Yarovaya Law, 2016) and China (Cybersecurity Law, 2017) are forcing tech companies to store user data for many months on their servers, implement extensive surveillance using AI monitoring, and decrypt it and communications upon request from authorities. Today, the UK is banning Apple's iCloud encryption (deal, 2025).

Problems with Comey's Solution

There are numerous problems with creating one or more backdoors for law enforcement to use to fight against crime. The first concern is government overreach and their abuse of power. We have seen this many times in the past, and sometimes none of the law enforcement, whether federal or state officials are held accountable and punished for the crimes they have committed using various technological tools like Sting Rays, Xaver, and Range-R Technology (Hampton Law, 2024a; Hampton Law, 2024b; Hampton Law, 2025). Also, James Comey is not the ideal role model when it comes to being a man of honesty and integrity because of his history of doing the opposite with the Hillary Clinton Email Investigation (2016), his firing by President Donald Trump (2016), the Steele Dossier and FBI's Russia Probe, and under current investigation for unethical acts and off-the-books operation targeting 2016 Trump campaign using honeypot operations (Picket, 2025). Though some of his arguments are logically valid, and it is a logical fallacy to leave my rebuttal at that (i.e., Ad Hominem Tu Quoque), it does not do Comey justice or any better if people have a difficult time believing a person who represents the opposite of transparency, honesty, and integrity.

Second, 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. Third, the public disclosure of a backdoor to an encryption program will create new legal, economic, technological, and interpersonal problems. An example is the 2016 vs. FBI dispute over the San Bernardino shooter's iPhone (epic.org, 2025; Wikipedia, 2025). The FBI demanded that Apple create a backdoor version of iOS; however, Apple refused to honor their request because it would set a dangerous precedent and weaken security for all its users. Apple insisted that a government-mandated backdoor could be misused.

Fourth, restricting and banning encryption resembles the government's past and current attempts to restrict our First and Second Amendment rights. The weakening of privacy protection will negatively impact law-abiding citizens and authorities, making them more at risk of government and non-government threats and attacks. According to the Heritage Foundation (2022), for example, more gun control does not fix gun violence but restricts the rights and power of law-abiding citizens to protect themselves and society: creating new vulnerabilities and attack vectors in society will increase the likelihood of more gun violence crime, including places like public schools and college campuses (MacDonald, 2018). Some of the most gun violence-ridden areas in the US contain the most restrictive gun laws and policies and make up most reporting of gun violence in the US (MacDonald, 2018). Also, criminals will continue to disobey the law and bypass many restrictions by finding other tactics and solutions to continue their heinous activities. It is often said that the Second Amendment ("right to bear arms") protects our First Amendment ("freedom of speech, religion, press, assembly, and petition"), and I would now indirectly include our right to privacy within the digitalized world.

America's Real Concern and a Proposed Solution

I do not think Comey understands nor addresses the fear of the public when it comes to government overreach regarding their communications and data. Comey questions the audience, "Have we become so mistrustful of government and law enforcement that we are willing to let bad guys walk away, willing to leave victims in search of justice" (Brookings, 2014). In other words, because governments have financial and security interests in the people, the people should automatically grant more trust and access to their data to authorities to better protect and secure them from hostile threats, both domestic and foreign.

The primary reason the public encrypts their data is the strong possibility of individuals and organizations unlawfully intercepting their data in transit and data at rest. There are plenty of examples made public of both the government and non-government individuals/organizations already doing the abovementioned without any proper form of accountability and punishment for Said activities. Examples include COINTELPRO (1956-1971), FBI surveillance of activists including MLK and Malcolm X), NSA's warrantless wiretapping post 9/11 through the 'Stellarwind' program, the DHS and NSA tracking of Americans' phone data (2021-Present), and the IRS and DEA bulk data collection scandals over the past two decades.

Instead, how about the government earn back the trust of the American public? Show the public that the government is an entity of integrity and is willing to be transparent and undergo more routine and extensive audits to weed out corruption and wasteful spending of taxpayer dollars. If a person or organization does me harm, says they are 'Sorry,' but moves on from that experience without demonstrably overcompensating to show their repentance, I cannot trust that person or organization any further. The government has done this ad nauseam, trampling the trust of many other Americans. I believe the public has faithfully responded to Comey's past concerns

now with their votes: In the wake of the 2024 presidential election and new appointments made by President Donald Trump, the public is prioritizing the use of taxpayer dollars and their privacy and security in the hope of more government transparency, accountability, and justice for all members of the government. Focus on word AND deed, and then the public will be more willing to work with the government for greater security.

Conclusion

Comey states, "The public should grant more trust and access to authorities to protect better and secure their communities from threats" (Brookings, 2014). Comey fears that the increase in technological advances in encrypting data will make it more difficult and possibly impossible to catch criminals in the future swiftly and with enough evidence to prosecute them to the full extent of the law. 'Going Dark' is the growing chasm of law enforcement using the rule and letter of the law and its ability to keep pace with the growing enhancement and complexity of encryption. "If the challenges to real-time data inception threaten to leave us in the dark, encryption threatens to lead us down to a black hole we may never return or recover from" (Brookings, 2014). However, with the strong possibility of the government abusing its power and overreach in unlawful ways and the ever-growing threat from individual and organizational hackers, Americans are further incentivized to fully encrypt their data in transit and at rest, making it more difficult for unauthorized personnel from accessing it, whether for good or bad. Until the government provides more transparency and accountability to the public, it is a 'hard pill' for Americans to swallow and accept them to surrender more of their rights and privileges to the government. As the saying goes, "Actions speak louder than words."

References

Bombal, D. (2025, February 2). *Are VPNs even safe now? Hacker Explains*. Retrieved from YouTube: https://www.youtube.com/watch?v=Qqd9KzPVBb8

Brave. (2025, February 15). *Brave vs Chrome*. Retrieved from Brave: https://brave.com/compare/chrome-vs-brave/

Brookings. (2014, October 16). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Retrieved from Brookings: https://www.brookings.edu/events/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course/

deal, U. B. (2025, February 26). *All Things Secured*. Retrieved from YouTube: https://www.youtube.com/watch?v=svsvRfpxbNg

epic.org. (2025, February 16). *Apple v. FBI*. Retrieved from epic.org: https://epic.org/documents/apple-v-fbi-2/

Law, H. (2024a, June 17). *How to Stop Cops From "Seeing Through Walls" to Spy on Your Home!* Retrieved from YouTube: https://www.youtube.com/watch?v=ZfvmdX631Gc

Law, H. (2024b, July 1). *How to Stop Cops from SPYING on Your Home with Cameras!* Retrieved from YouTube: https://www.youtube.com/watch?v=Vej1-l71lvs

Law, H. (2025, January 19). *LAWYER: How to Stop Cops From COVERING Your Porch Camera*. Retrieved from YouTube: https://www.youtube.com/watch?v=8nno8ejpi7g&list=PLUuoizVaZR8ha3OW0Ev98jNQsEGiTs3_g&index=6

MacDonald, C. (2018, March 24). *Heritage Foundation: Eight Stubborn Facts Regarding Gun Violence in America (VIDEO)*. Retrieved from The Gateway Pundit: https://www.thegatewaypundit.com/2018/03/heritage-foundation-eight-stubborn-facts-regarding-gun-violence-in-america-video/

Picket, K. (2025, February 25). *FBI looking into Comey's off-the-books 'honeypot' operation targeting 2016 Trump campaign*. Retrieved from The Washington Times: https://www.washingtontimes.com/news/2025/feb/25/fbi-looking-james-comeys-books-honeypot-operation-targeting-2016/

Wikipedia. (2025, February 24). *Apple–FBI encryption dispute*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Apple%E2%80%93FBI_encryption_dispute

Yubico. (2024, October 9). *What is a Sim Swap?* Retrieved from Yubico: https://www.yubico.com/resources/glossary/sim-swap/