Texas Law Review Online
Volume 103 | 2025

Opening Pandora's Phone: Bearing Witness in the Digital Age

*Matthew H. Ormsbee**

Introduction

Half of Americans use facial recognition to access their electronic devices, according to one estimate.[1] While such a shortcut around a traditional passcode offers individuals greater convenience and security, it may curtail constitutional privileges when law enforcement seeks to compel the decryption of a device with an individual's biometrics. Courts diverge on whether such compelled decryption violates a user's Fifth Amendment right against self-incrimination. While some courts offer Fifth Amendment protection to citizens compelled to decrypt their devices biometrically, others do not. Thus, the constitutional privilege against self-incrimination currently varies based on a citizen's location and the related precedent.

When the U.S. Supreme Court inevitably resolves this split among the courts, a majority of the Justices may find the Court's current Fifth Amendment jurisprudence most consistent with a

* *Matthew Ormsbee is an active-duty military officer and assistant professor of law at the U.S. Air Force Academy, where he teaches topics in constitutional law. He is a former military prosecutor and defense attorney. The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the U.S. Air Force Academy, the Air Force, the Department of Defense, or the U.S. Government.*

1. *New CyberLink Report Finds Over 131 Million Americans Use Facial Recognition Daily and Nearly Half of Them to Access Three Applications or More Each Day*, BUS. WIRE (Nov. 23, 2022, 9:00 AM EST), https://www.businesswire.com/news/home/20221123005021/en/New-CyberLink-Report-Finds-Over-131-Million-Americans-Use-Facial-Recognition-Daily-and-Nearly-Half-of-Them-to-Access-Three-Applications-or-More-Each-Day [https://perma.cc/CU3G-ZU2B].

holding that compelled biometric decryption is constitutional. This is in line with the Court's earliest cases permitting the compelling of immutable, non-communicative physical characteristics from defendants. Yet, Americans may balk at the paradox arising from those courts affording no constitutional privileges in this context: While biometrics and passcodes perform the same function, compelled biometric decryption of devices receives no Fifth Amendment protection, yet passcodes as simple as 1-1-1-1 commonly receive Fifth Amendment protection. This is because revealing a passcode divulges the contents of one's mind, which is communicative and testimonial in ways not applicable to biometrics.

Complicating matters, smartphones are ever-present and retain the sensitive details of a user's life. Accordingly, there are compelling public policy, privacy, and cybersecurity reasons for the Supreme Court to find that compelled decryption of smartphones through physical characteristics forces one to be a "witness" against oneself in a criminal trial, violating the Fifth Amendment.[2] The Court's jurisprudence on immutable physical characteristics creates a conundrum in which longstanding Supreme Court precedent undermines broad societal concerns. As early as the landmark decision of *Schmerber v. California*,[3] the Justices voiced concern over construing the Fifth Amendment's privilege against self-incrimination as "too narrow and technical."[4] Justice Black notably harkened to *Boyd v. United States*,[5] warning years earlier of a "close and literal construction" of constitutional provisions.[6]

2. U.S. CONST. amend. V. ("No person shall . . . be compelled in any criminal case to be a witness against himself . . . .").
3. 384 U.S. 757 (1966).
4. *Id.* at 777 (Black, J., dissenting).
5. 116 U.S. 616 (1886).
6. *Id.* at 635.

This Article frames the looming problem and proposes solutions, urging the Court to revisit Justice Clarence Thomas's concurrence in *United States v. Hubbell*.[7] In that case, Justice Thomas argued for a Fifth Amendment privilege that protects against the government compelling not just incriminating testimony but any incriminating evidence.[8] Justice Thomas's broader interpretation of the Fifth Amendment privilege—though not broadly accepted today—would protect against the act of compelling a defendant to produce evidence of his guilt by merely entering a passcode, providing a fingerprint, or acceding to facial recognition. In 2000, only Justices Thomas and Scalia were willing "to reconsider the scope and meaning of the Self-Incrimination Clause."[9] Yet, a broader construction of being a "witness" against oneself, grounded in textualism and history, may provide the most apt solution by evading the Court's restrictive Fifth Amendment case law. Given the Court's current composition and pressing privacy concerns relating to cell phones, now is the time to resolve the conundrum of compelled biometric decryption.

I. Biometric Security Technology

The advent of biometric authentication in personal digital devices has revolutionized user access while simultaneously creating novel challenges for law enforcement investigations.[10] When law enforcement believes that a suspect's smartphone contains incriminating evidence but the individual refuses to comply with a police or court order to unlock the device, investigators face a technological and legal quandary. Courts may order a suspect to unlock their phone via biometrics, but suspects

7. 530 U.S. 27, 49–56 (2000) (Thomas, J., concurring).
8. *Id.* at 49.
9. *Id.*
10. *See, e.g.*, Erin M. Sales, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, 69 U. MIA. L. REV. 193, 194–96 (2014).

will claim this compelled decryption is testimonial and, therefore, unconstitutional.[11] This situation arises as biometric security features, particularly facial recognition, have become commonplace in modern smartphones.

Facial recognition technology in modern devices relies on sophisticated algorithms that create a detailed geometric map of the user's facial features.[12] This map is intricate and unique to everyone, like a fingerprint. The technology commonly uses the device's front-facing camera to capture a three-dimensional image of the user's face.[13] This image is then analyzed for specific nodal points, such as the distance between the eyes, the width of the nose, the depth of the eye sockets, and the shape of the cheekbones.[14] These measurements are converted into a complex mathematical identifier, creating a so-called faceprint that is unique to the individual and stored on the device.[15]

When a user attempts to unlock their device, the facial recognition system captures a new image, creates a new faceprint, and compares it to the stored data.[16] If the two faceprints match within a certain threshold of similarity, the device unlocks.[17] This process occurs in a fraction of a second, providing security and

11. *See* Doe v. United States, 487 U.S. 201, 219 (1988).
12. Apple Platform Security, *Face ID Security*, APPLE, INC. (Dec. 19, 2024), https://support.apple.com/guide/security/biometric-security-sec067eb0c9e/web [https://perma.cc/E8HR-33G2].
13. Anil K. Jain et al., *An Introduction to Biometric Recognition*, 14 IEEE TRANSACTIONS ON CIRS. AND SYS. FOR VIDEO TECH. 4, 9 (2004).
14. *Id.*
15. Megasis Network, *AI and Facial Recognition: The Science Behind Unlocking Your Phone*, MEDIUM (Feb. 9, 2024), https://megasisnetwork.medium.com/ai-and-facial-recognition-the-science-behind-unlocking-your-phone-b8bdc7b7c90c [https://perma.cc/M62Q-M83G].
16. *About Face ID Advanced Technology*, APPLE, INC. (Dec. 9, 2024), https://support.apple.com/en-us/102381 [https://perma.cc/7T2F-NEGP].
17. *Id.*

convenience.[18] However, the intricacy and personal nature of this biometric data raise significant questions when law enforcement seeks to compel its use. The fundamental issue is whether forcing an individual to use their face to unlock a device constitutes being a "witness" against oneself, in violation of the Fifth Amendment's self-incrimination clause.[19]

This context requires a critical examination of Fifth Amendment jurisprudence related to technological advancements. To fully understand the legal implications of compelled biometric decryption, it is necessary to trace the evolution of Fifth Amendment interpretations through key Supreme Court decisions. Beginning with *Boyd v. United States*, which established a broad notion of what it means to be a "witness," through *Fisher v. United States*,[20] and up to the present day, the following historical analysis provides a foundation for considering a broader conception of the Fifth Amendment's self-incrimination clause.

II. Relevant Precedent

The Fifth Amendment states in relevant part: "No person shall be . . . compelled in any criminal case to be a witness against himself."[21] The Supreme Court views the purpose of the Fifth Amendment's self-incrimination clause as protecting defendants "from having to reveal, directly or indirectly, [] knowledge of facts relating [them] to the offense or from having to share [their] thoughts and beliefs with the Government."[22] Despite this straightforward view of the self-incrimination clause, the jurisprudence concerning compelled biometric decryption of

18. *Id.*
19. Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEXAS L. REV. 767, 768–69 (2019).
20. 425 U.S. 391 (1976).
21. U.S. CONST. amend. V.
22. Doe v. United States, 487 U.S. 201, 213 (1988).

personal devices presents a complex interplay between established Fifth Amendment principles and evolving technology.

The Supreme Court's 1886 decision in *Boyd v. United States* established revolutionary protections against compelled self-incrimination, marking the Court's first significant interpretation of the Fifth Amendment's scope. The Court rejected the government's attempts to compel the production of private papers and records.[23] Through this landmark ruling, the Court recognized the intimate connection between Fourth and Fifth Amendment protections, particularly when the government seeks to compel evidence that could incriminate the accused.[24] While later decisions have narrowed Boyd's sweeping protections, its fundamental insight into the relationship between privacy and self-incrimination remains influential, particularly in cases involving personal electronic devices that contain the modern equivalent of private papers.

This broad interpretation of constitutional protections starkly contrasts with the Court's later physical evidence doctrine established in *Schmerber v. California*, which drew a sharp line between testimonial communications and bodily evidence. The Court's decision in *Schmerber* laid the early groundwork for understanding how physical characteristics circumvent the privilege against self-incrimination. In *Schmerber*, the Court held that compelling a blood sample did not violate the Fifth Amendment since it was not communicative or testimonial in nature.[25] *Schmerber* distinguished between testimonial communications, which are constitutionally protected, and physical evidence, like blood samples, which are not constitutionally protected.[26] Courts have applied this precedent to other physical

23. Boyd v. United States, 116 U.S. 616, 634–35 (1886).
24. *Id.* at 633.
25. Schmerber v. California, 384 U.S. 757, 761 (1966).
26. *Id.* at 764.

characteristics, including handwriting exemplars,[27] voice exemplars,[28] criminal lineups,[29] and wearing clothing,[30] which courts do not view as "testimonial communications."

Still, *Schmerber*'s application for smartphone decryption is complex. Using biometrics to unlock a device may involve an implied assertion of fact about access to the phone, raising questions about whether this action is purely physical or comes with testimonial baggage. The Court's trilogy of *Fisher v. United States*, *Doe v. United States*, and *United States v. Hubbell* provides a framework for analyzing these implied assertions of fact. First, in *Fisher*, the Court introduced the concept of "foregone conclusion," suggesting that if the government can independently prove documents' existence, possession, and authenticity, compelling their production does not violate the Fifth Amendment because the defendant has not conveyed any new information.[31]

Doe further clarified that producing documents could be testimonial if it involved implicit statements of fact.[32] *Doe* also introduced the oft-cited metaphor distinguishing between compelling someone to "surrender a key to a strongbox" (unprotected) versus forcing them to give "the combination to a wall safe" (protected).[33] In the context of decryption, the "key" could be analogized to facial characteristics, while the "combination" is analogized to a phone's passcode. Finally, *Hubbell* refined the foregone conclusion doctrine, affirming that the government must have prior knowledge of the existence and location of the documents in question and be able to prove this with "reasonable particularity."[34] *Hubbell* also held that forcing defendants to

27. Gilbert v. California, 388 U.S. 263, 266–67 (1967).
28. United States v. Dionisio, 410 U.S. 1, 7 (1973).
29. United States v. Wade, 388 U.S. 218, 222–23 (1967).
30. Holt v. United States, 218 U.S. 245, 252–53 (1910).
31. Fisher v. United States, 425 U.S. 391, 411 (1976).
32. Doe v. United States, 487 U.S. 201, 209–10 (1988).
33. *Id.* at 210 n.9.
34. United States v. Hubbell, 530 U.S. 27, 32–33, 44–45.

use their mental faculties to identify responsive documents is testimonial.[35] Finally, the Hubbell majority held that the act of production itself can be testimonial if it requires the defendant to make implicit statements of fact.[36]

Applying these principles to biometric smartphone decryption has led to a significant split among federal and state courts across the United States. Among federal appellate courts, in *United States v. Apple MacPro Computer*,[37] the Third Circuit Court of Appeals ruled in favor of allowing compelled decryption, reasoning that the decryption of devices was not sufficiently testimonial to trigger Fifth Amendment protection.[38] Most recently, in *United States v. Payne*,[39] the Ninth Circuit similarly held that compelled biometric unlocks are not testimonial and evade the Fifth Amendment entirely.[40] The *Payne* court embraced the distinction between biometric and passcode unlocks.[41] Conversely, in *In re Search of a Residence in Oakland, California*,[42] the Northern District of California took a more protective stance, holding that compelled biometric decryption violated the Fifth Amendment as it forced the defendant to provide incriminating testimony about their ability to access the device.[43] The court was convinced by the authentication aspect and the vast scope of private information the phone would reveal.[44]

State court decisions similarly diverge on this issue, further highlighting the lack of consensus. For example, in *State v. Diamond*,[45] the Minnesota Supreme Court held in 2018 that

35. *Id.* at 43.
36. *Id.* at 44–45.
37. 851 F.3d 238 (3d Cir. 2017).
38. *Id.* at 248.
39. 99 F.4th 495 (9th Cir. 2024).
40. *Id.* at 513.
41. *Id.* at 511.
42. 354 F. Supp. 3d 1010 (N.D. Cal. 2019).
43. *Id.* at 1016.
44. *Id.*
45. 905 N.W.2d 870 (Minn. 2018).

compelling a defendant to provide a fingerprint to unlock a phone did not violate the Fifth Amendment, as it was no more testimonial than giving a blood sample without the use of mental exertion.[46] However, in *Commonwealth v. Davis*,[47] three justices of the Pennsylvania Supreme Court reached the opposite conclusion, finding that compelling biometric decryption should be testimonial and therefore protected by the Fifth Amendment.[48]

In 2020, three justices of the New Jersey Supreme Court took a similar stance in *State v. Andrews*, emphasizing the need to protect privacy in the digital age.[49] In *Seo v. State*,[50] the Indiana Supreme Court reaffirmed Fifth Amendment protection by focusing on the phone's contents rather than the act of unlocking it.[51] The court noted that biometric unlocks are functionally equivalent to passcodes and that modern devices contain intimate details beyond physical evidence.[52]

Policy considerations loom as courts continue to rule on compelled decryption using biometrics. The ubiquity of smartphones and the vast amount of personal information they contain raise significant privacy concerns. These devices are repositories for our most intimate thoughts, communications, and activities, all of which deserve robust Fifth Amendment protections. On the other hand, law enforcement critically relies on access to smartphone data to investigate and prosecute crimes in the digital age. Balancing these competing interests will be critical for courts and policymakers moving forward.

46. *Id.* at 878.
47. 220 A.3d 534 (Pa. 2019).
48. *Id.* at 554–55 (Baer, J., dissenting).
49. 234 A.3d 1254, 1278 (2020) (LaVecchia, J., dissenting).
50. 148 N.E.3d 952 (Ind. 2020).
51. *Id.* at 960–61.
52. *Id.* at 957, 959.

III. Policy Concerns

The evolving digital privacy and security landscape presents a complex challenge for courts and policymakers grappling with applying Fifth Amendment protections to compelled biometric decryption. This tension between individual privacy rights and law enforcement requires a nuanced approach considering constitutional principles and modern technology's realities. The Supreme Court's decisions in *Carpenter v. United States*[53] and *Riley v. California*[54] demonstrate a growing recognition of the unique privacy concerns posed by digital devices. In *Carpenter*, the Court acknowledged that the "seismic shifts in digital technology" necessitate a reevaluation of traditional Fourth Amendment doctrines, extending privacy protections to cell-site location information.[55] Similarly, *Riley* recognized the vast amount of personal data contained in modern smartphones, requiring warrants for their search incident to arrest.[56] While these cases concerned Fourth Amendment jurisprudence, they suggest a judicial willingness to adapt constitutional protections to the digital age. This principle extends to Fifth Amendment considerations in compelled decryption cases.

Many rulings, including *Seo v. State*, acknowledge that the contents of smartphones are vast and qualitatively different from traditional physical evidence.[57] However, current jurisprudence creates an arbitrary distinction between biometric and passcode protections, potentially undermining the Fifth Amendment's core purpose. Indeed, some view passcode and biometric lock mechanisms as implicating the Fifth Amendment's protections.[58] Thus, the amount of Fifth Amendment protection a

53. 585 U.S. 296 (2018).
54. 573 U.S. 373 (2014).
55. *Carpenter*, 585 U.S. at 313.
56. *Riley*, 573 U.S. at 403.
57. *Seo*, 148 N.E.3d at 960–61.
58. *See, e.g.*, Commonwealth v. Davis, 220 A.3d 534, 550 (Pa. 2019).

defendant receives should not turn on the type of lock they choose to use. In the digital context, this arbitrary distinction fails to account for the functional equivalence of these security measures. It unwisely incentivizes individuals to use less secure decryption methods—passcodes—to gain stronger constitutional protections.

The irony that biometrics—often considered the most secure form of device protection—may receive less Fifth Amendment protection than simple passcodes underscores the need for a more coherent legal framework. As argued by Professor Laurent Sacharoff, the act of unlocking a device, regardless of the method, should be considered testimonial because it implies assertions of fact about the defendant's knowledge, control, and possession of the device's contents, consistent with the *Fisher*, *Doe*, and *Hubbell* line of cases.[59] This perspective aligns with the broader interpretation of the Fifth Amendment advocated by some scholars and jurists, which would provide consistent constitutional protection regardless of the unlocking mechanism.

Moreover, the rapid pace of technological advancement suggests that any distinction based on contemporary unlocking methods may quickly become obsolete. As biometric technologies evolve and integrate more deeply with our digital lives, the line between physical characteristics and "contents of the mind" may blur.[60] This gradual advancement of technology, recognized in Carpenter, calls for a forward-looking approach to Fifth Amendment protections that can adapt to future innovations while maintaining consistent constitutional safeguards.

59. Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEXAS L. REV. ONLINE 63, 68–70 (2019).

60. Fisher v. United States, 425 U.S. 391, 420 (1976).

IV. Options and Counterarguments

The argument that compelled biometric unlocks are non-testimonial is strong based on the physical evidence doctrine (*Schmerber*), lack of mental exertion (*Hubbell*), and foregone conclusion that a device belongs to a particular defendant (*Fisher*). Yet, the Supreme Court has several viable paths forward beyond adopting Justice Thomas's broader reading of the Fifth Amendment privilege against self-incrimination. One compelling alternative involves expanding the act-of-production doctrine to encompass compelled biometric decryption, effectively prioritizing this analytical framework over the physical-characteristics precedent established in *Schmerber*. The act-of-production doctrine recognizes that the very act of producing documents or information may communicate facts about existence, possession, and authenticity that could be incriminating.[61]

This doctrinal approach would acknowledge that using biometrics to unlock a device inherently communicates the defendant's ability to access its contents, regardless of whether that access occurs through physical characteristics or knowledge-based authentication. Such an expansion would provide consistent constitutional protection across authenticating methods while respecting existing Fifth Amendment jurisprudence. The Court could achieve this outcome without abandoning the framework of physical characteristics. Instead, the Court would recognize that biometric decryption represents a unique hybrid that merits distinct constitutional analysis.

Additionally, the foregone conclusion doctrine, first articulated in *Fisher*, presents a potential but limited avenue for resolution. As discussed, this doctrine permits the government to compel the production of incriminating information when it can demonstrate with reasonable particularity that it already knows the existence, location, and authenticity of the evidence sought.

61. *See* United States v. Hubbell, 530 U.S. 27, 36–37 (2000).

However, the doctrine's application to modern digital devices presents significant challenges that suggest its limitations in this context. The Eleventh Circuit's decision in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011* highlighted these difficulties, noting that the government must know with "reasonable particularity" which specific files it seeks on a device before compelling decryption.[62]

Unfortunately, this standard proves very difficult to meet in most digital device cases, where law enforcement often cannot know precisely (or with any level of particularity) which files, if any, exist on a locked device. The practical constraints of applying the foregone conclusion doctrine to smartphone decryption have contributed to its declining relevance in American jurisprudence, particularly in the digital context. In these cases, this doctrine's increasing obsolescence suggests the need for new analytical frameworks better suited to modern technological realities.

Critics of enhanced Fifth Amendment protection for biometric decryption often cite law enforcement's understandable need to access digital evidence in cases involving child exploitation, terrorist organizations, and drug trafficking. Yet, this argument overlooks several crucial considerations. Law enforcement agencies already employ various legal methods to access encrypted devices, including developing sophisticated decryption technologies and partnering with private sector security firms.[63] Moreover, maintaining the current dichotomy between biometric and passcode protection creates a perverse incentive structure: sophisticated criminals would simply opt for passcode

62. 670 F.3d 1335, 1349 (11th Cir. 2012).

63. Johana Bhuiyan, *How Can US Law Enforcement Agencies Access Your Data? Let's Count the Ways*, GUARDIAN (Apr. 4, 2022, 10:05 AM), https://www.theguardian.com/technology/2022/apr/04/us-law-enforcement-agencies-access-your-data-apple-meta [https://perma.cc/X9XV-UQHK].

protection to obtain stronger constitutional safeguards, while less sophisticated individuals using biometric security for greater device security would face greater vulnerability to compelled decryption.

This reality undermines both law enforcement objectives and constitutional principles. It also draws an arbitrary distinction between greater and lesser constitutional protection based on an individual's preference for the decryption method. A consistent approach to Fifth Amendment protection across authentication methods would eliminate these artificial distinctions. It would also preserve law enforcement's ability to pursue alternative investigative strategies.

Recent developments in Fourth Amendment jurisprudence, particularly the Supreme Court's decision in *Carpenter*, suggest a growing judicial recognition of privacy interests in digital data that could inform Fifth Amendment analysis.[64] The *Carpenter* Court's acknowledgment that digital technology requires new approaches to constitutional protection provides a compelling parallel for reconsidering Fifth Amendment applications to biometric decryption. Just as *Carpenter* recognized that traditional Fourth Amendment doctrines inadequately addressed modern privacy concerns, current Fifth Amendment frameworks may require similar evolution to meet contemporary challenges. This doctrinal cross-pollination could help courts develop more nuanced approaches to constitutional protection in the digital age. Thus, the interplay between Fourth and Fifth Amendment jurisprudence offers valuable insights for crafting solutions to the biometric decryption dilemma.

The strongest counterargument to extending broader Fifth Amendment protection to biometric decryption emphasizes the value of clear, easily applicable rules based on physical characteristics. Proponents of this view argue that maintaining the

64. *See* Carpenter v. United States, 585 U.S. 296, 313 (2018).

distinction between physical traits and knowledge-based authentication provides bright-line guidance for law enforcement and citizens. Yet, this argument fails to acknowledge how technological advancement has blurred this once-clear distinction. Modern biometric authentication systems transform physical characteristics into complex mathematical representations that function identically to password-based security. Thus, the simplicity of the physical-characteristics rule comes at the heavy cost of constitutional coherence and technological reality. Legislative solutions could potentially address these concerns while maintaining clear guidelines for law enforcement, but the fundamental constitutional questions require judicial resolution.

Conclusion

The compelled decryption of smartphones through biometric data presents a constitutional paradox that demands resolution as these devices become increasingly central to daily life. While contemporary Supreme Court precedent suggests that compelling physical characteristics for device access remain constitutionally permissible, this framework fails to account for the functional equivalence of biometric and passcode authentication and the intimate nature of smartphone contents. Whether through Justice Thomas's broader reading of the Fifth Amendment privilege, an expansion of the act-of-production doctrine, or a novel analytical framework, the Court must adapt constitutional protections to modern technological realities. The stakes of this resolution extend beyond immediate law enforcement concerns to fundamental questions about privacy, security, and individual rights in an increasingly digital world.