Testifying by Fingerprint: Why the Government Can't Force You to Unlock Your Phone

by Annemarie Ardy[*]

Cell phones have become ubiquitous in modern life; they are often carried everywhere and used to facilitate nearly every activity. Yet their incredible convenience is a double-edged sword: when searched by law enforcement, the wealth of information contained on a cell phone can paint a more intimate and fine-grained portrait of a person's life than 24/7 surveillance. Passcodes and biometric scanners—mechanisms that permit a user to unlock a device through its recognition of the user's face or fingerprint—stand in the government's way, but only so long as courts do not permit the government to compel people to unlock their phones. Although the compulsion of a passcode clearly violates the Fifth Amendment's Self-Incrimination Clause, courts have split on the question of whether compulsion of biometric scanning receives similar protections. This Contribution argues that courts should treat the use of biometric scanners as categorically testimonial and therefore protected by the Self-Incrimination Clause. Biometric scanners convey information that is classically testimonial, and to hold otherwise would pose unacceptable risks to personal privacy.

On November 3, 2021, Jeremy Travis Payne was pulled over by California Highway Patrol Officers Garcia and Coddington in Death Valley, California, who believed that the windows of his Nissan were unlawfully tinted.[1] Payne informed the officers that he was on parole, and the officers detained Payne and searched him, finding $1,270 in cash on his person.[2] Officer Coddington sought to unlock and search Payne's phone pursuant to his parole conditions, which required Payne to unlock "any digital/electronic

---

[*] Annemarie Ardy is a J.D. Candidate (2027) at New York University School of Law and the 2026–27 Executive Editor of *Proceedings*. This Contribution is a commentary on the competition problem for the 2026 UCLA School of Law Cybercrimes Moot Court Competition. The views expressed herein do not necessarily represent the author's views.

[1] United States v. Payne, 99 F.4th 495, 499 (9th Cir.), *cert. denied,* 145 S. Ct. 605 (2024).

[2] *Id.* at 499–500.

device in [his] vicinity" and "surrender" it "to any law enforcement officer for inspection" upon request, "with or without" reasonable suspicion, a warrant, or probable cause.[3] Payne refused to unlock the phone.[4] At that point, Officer Coddington could have lawfully confiscated the device and arrested Payne pending further investigation, per Payne's parole conditions.[5] Instead, Officer Coddington "forcibly grabbed Payne's thumb and used it to unlock the phone via a built-in biometric unlocking feature."[6] Officer Coddington searched the phone's stored photos and videos as well as its maps application, discovering evidence that ultimately led to Payne's indictment on several drug-related charges.[7]

Both the Central District of California and the Ninth Circuit Court of Appeals found that Officer Coddington did not violate Payne's Fifth Amendment privilege against self-incrimination when he forced Payne to unlock his phone against his will.[8] The Fifth Amendment's Self-Incrimination Clause provides that no person may be "compelled in any criminal case to be a witness against himself."[9] Courts have long held that the word "witness" limits the Fifth Amendment's protections to "testimonial" evidence, such that "pure physical" evidence—blood samples, fingerprints, standing in a lineup, and so on—falls outside of its protection.[10] In particular, the Ninth Circuit found that the forcible application of Payne's finger to the phone did not "intrude on the contents of [Payne's] mind," and therefore unlocking the phone was not a testimonial act.[11] The court acknowledged that

---

[3] *Id.* at 499.
[4] *Id.* at 500.
[5] *Id.*
[6] *Id.*
[7] *Payne*, 99 F.4th at 501.
[8] *Id.* at 501, 512.
[9] U.S. CONST. amend. V, cl. 3.
[10] *See* Schmerber v. California, 384 U.S. 757, 764–65 (1966) (The Self-Incrimination Clause does not protect a suspect against the forcible taking of a blood sample, nor "against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture."); United States v. Wade, 388 U.S. 218, 222–23 (1967) (holding that suspects may be constitutionally compelled to stand in lineups for identification purposes).
[11] *Payne*, 99 F.4th at 511.

that outcome might have been different, however, "had Officer Coddington required Payne to independently select the finger that he placed on the phone."[12] But because Officer Coddington chose to use physical force rather than attempting to compel Payne to unlock the phone another way, Payne could make no objection to the admission of the contents of his phone at trial, nor to the evidence discovered as a result of that search.[13]

This Contribution argues that this outcome is wrong. The use of biometric unlocking mechanisms should be treated as a testimonial act under the Self-Incrimination Clause, such that the government may not constitutionally compel a person to unlock a phone or laptop via those mechanisms. Biometric scanners convey information regarding a person's unique relationship to their device, including knowledge of that particular device's unlocking mechanism and ownership or control of the device's contents.[14] That communication is testimonial under Supreme Court precedent, and its compulsion is the kind of governmental intrusion that the Fifth Amendment was intended to guard against. Although a person may not necessarily exercise "cognitive exertion" in a case like *Payne*, where the choice of how to unlock the device is made by a government agent rather than the suspect themselves,[15] the potential for biometric scanners to become workarounds for Fourth and Fifth Amendment protections provides strong reason to treat biometric scanners as categorically testimonial.

Although courts have long held that the Self-Incrimination Clause protects only testimonial evidence, the line between testimonial and non-testimonial evidence has never been entirely clear. The Supreme Court's foundational decision in 1966, *Schmerber*, indicated that evidence is only protected if it is a "communication," a category which excludes purely physical evidence such as blood samples and height or weight measurements.[16] But even *Schmerber* acknowledged that this line was blurry: a lie detector test, for instance, measures only

[12] *Id.* at 513.
[13] *Id.*
[14] *See* United States v. Brown, 125 F.4th 1186, 1203–04 (D.C. Cir. 2025).
[15] *Payne*, 99 F.4th at 511 (internal quotations omitted).
[16] *See Schmerber*, 384 U.S. at 763–64.

"physiological responses," but it is "actually . . . directed to eliciting responses which are essentially testimonial" and may therefore fall within the scope of the Self-Incrimination Clause.[17] From *Schmerber*, then, courts inferred that evidence of the suspect's pure physical characteristics would typically be non-testimonial, but some gray area could exist where the purpose of gathering evidence of physical characteristics is to acquire non-physical information from the suspect, particularly thoughts or emotions.[18]

The Supreme Court complicated this picture even further in a trio of cases: *United States v. Doe* ("*Doe I*") in 1984, *Doe v. United States* ("*Doe II*") in 1988, and *United States v. Hubbell* in 2000.[19] In *Doe I*, the Court held that the "act of producing" documents in response to a subpoena could itself be testimonial, irrespective of the contents of those documents.[20] The act of production is communicative in that it conveys the existence of the documents requested, their possession or control by the subject of the subpoena, and the subject of the subpoena's belief that the documents are those described by the subpoena.[21] *Doe II* clarified *Doe I* by holding that an act of production may not be testimonial where the subpoena does not require a suspect to "communicate[] any factual assertions," but merely to execute a directive permitting a third party to disclose certain records or documents to the government, without affirming that such records or documents actually exist.[22] Finally, the *Hubbell* Court expanded on the holding of *Doe I*, finding that Hubbell's act of producing over thirteen thousand pages of documents in response to the government's broad subpoena was testimonial because it "unquestionably" required Hubbell to "make extensive use of the contents of his own mind in identifying the hundreds of documents responsive to the requests in the subpoena."[23]

---

[17] *Id.* at 764.
[18] *See, e.g.*, *Payne*, 99 F.4th at 508–09; *Brown*, 125 F.4th at 1202.
[19] 465 U.S. 605 (1984); 487 U.S. 201 (1988); 530 U.S. 27 (2000).
[20] *Doe I*, 465 U.S. at 612.
[21] *Id.* at 612–13.
[22] *Doe II*, 487 U.S. at 215–16.
[23] *Hubbell*, 530 U.S. at 43 (internal quotations omitted).

Doe I, *Doe II*, and *Hubbell* leave us with a muddied "act of production" doctrine, wherein a physical act is typically non-testimonial but may be communicative "wholly aside from the contents" of any information produced,[24] so long as the action "impl[ies] assertions of fact."[25] Hence the Ninth Circuit's confusion: fingerprints have long been treated as a prototypical form of physical evidence which falls outside of the scope of the Self-Incrimination Clause,[26] but the use of a fingerprint to unlock a phone "*produc[es]* the contents" of that phone[27] and communicates information about a person's relationship to the phone.[28]

Fundamentally, a testimonial act is one that communicates information contained in a person's mind.[29] The physical nature of a fingerprint distinguishes biometric scanners from passwords, wherein a person's decision of which numbers and letters to press clearly requires the use of thoughts and mental recall.[30] As a result, some courts have suggested that the application of a fingerprint to a biometric scanner is categorically non-testimonial.[31] However, what these courts failed to recognize is that unlocking a phone generally does "disclose [a person's] knowledge . . . that [their] thumb would unlock the device," which reveals "ownership or control over the phone and the messages it contained."[32] Unlocking a phone is "tantamount to answering a

---

[24] Fisher v. United States, 425 U.S. 391, 410 (1976).
[25] *Doe II*, 487 U.S. at 209.
[26] *See, e.g.*, *Schmerber*, 384 U.S. at 764 (noting that the Fifth Amendment does not protect against compelled fingerprinting).
[27] In re Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (emphasis in original).
[28] *Brown*, 125 F.4th at 1203–04.
[29] *See Hubbell*, 530 U.S. at 43.
[30] *Id.*
[31] *See, e.g.*, In re Search Warrant No. 5165, 470 F. Supp. 3d 715, 720, 730–32 (E.D. Ky. 2020) (finding that Self-Incrimination Clause did not prohibit authorization of a search warrant which would "permit[] law enforcement to compel all individuals present at" the premises to be searched "to unlock any [electronic devices] requiring biometric access"); Matter of Search Warrant Application for cellular telephone in United States v. Barrera, 415 F. Supp. 3d 832, 841–42 (N.D. Ill. 2019) (finding that unlocking a phone using its biometric scanner does not implicitly communicate any knowledge, and therefore the act is not testimonial).
[32] *Brown*, 125 F.4th at 1203–04.

series of questions about ownership or control over the phone, including how it [can] be opened and by whom."[33] Such disclosures are essentially communicative in nature and therefore testimonial.

The Ninth Circuit's struggle over the fingerprint stemmed primarily from the fact that Payne's finger was forcibly pressed to the biometric scanner.[34] The lack of conscious decision-making on Payne's part undermined the argument that Payne had communicated any thoughts or beliefs to Officer Coddington; Payne may as well have been asleep.[35] However, unlocking a phone unavoidably amounts to "testifying that [the person] has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents."[36] In other words, the testimonial communications do not necessarily hinge on a person's voluntary choice of how to unlock the phone. Officer Coddington's choice of which of Payne's fingers to press to the phone may have eliminated one testimonial communication from the list of possible communications, but Payne was still forced to testify that he understood how biometric scanners function, had chosen to set up a biometric unlocking mechanism on this particular device, and possessed some control over that device and could access its contents.

Even if one believes that Payne's act of unlocking the phone was not testimonial, there are good reasons to treat biometric scanners as categorically testimonial rather than taking a case-by-case approach. Without Fifth Amendment limitations on the forcible unlocking of phones, it would be all too easy for law enforcement to invade the privacy not only of those suspected of crimes, but of anyone with whom a criminal suspect has communicated.

---

[33] *Id.* at 1204.
[34] *See Payne*, 99 F.4th at 513.
[35] *See Barrera*, 415 F. Supp. 3d at 839 ("[T]he application of a finger to the home button on a iPhone can be done while the individual sleeps or is unconscious, and thus does not require any revelation of information stored in a person's mind." (internal quotations omitted)).
[36] *In re Application for a Search Warrant*, 236 F. Supp. 3d at 1073.

Searches of phones and laptops pose significant threats to privacy. As the Supreme Court recognized in *Riley v. California*, a modern smartphone essentially contains the entirety of a person's life in portable form.[37] The Fourth Amendment, which places a reasonableness limitation upon searches and seizures, generally requires the government to obtain a warrant based upon probable cause before searching a phone or laptop.[38] A warrant would typically limit the scope of the subsequent search of that cell phone or laptop.[39] However, in practice, the reasonableness limitation may not provide meaningful protection from privacy intrusions.

Even where the government only seeks content related to a specific investigation, longstanding Fourth Amendment doctrine permits law enforcement to seize any incriminating evidence which is in "plain view."[40] Once law enforcement agents lawfully access a phone or device, they will be permitted to seize any evidence they happened to come across, regardless of whether that evidence was the original object of the search.[41] And typically, authorization to search for a particular piece of evidence permits law enforcement to search any place or object where that evidence might reasonably be found.[42] In a phone or laptop, an incriminating piece of evidence could potentially be found in any of a person's photos, videos, files, maps applications, Google search history, social media and messaging applications, email applications, or call history. Searches of phones or laptops may thus involve a wide-ranging intrusion into a variety of files and applications, burdening not only the device owner's privacy, but also the privacy of any third parties with whom the device owner

---

[37] 573 U.S. 373, 393–97 (2014).
[38] *See id.* at 401.
[39] *See generally In Re* Search of Info. Associated with Facebook Acct. Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc. ("*Aaron.Alexis*"), 21 F. Supp. 3d 1, 10 (D.D.C. 2013).
[40] *See id*. at 10.
[41] *See id*.
[42] *See* United States v. Giberson, 527 F.3d 882, 886 (9th Cir. 2008) ("We have long held that a search warrant authorizing the seizure of materials also authorizes the search of objects that could contain those materials.").

has communicated via messaging platforms accessible through the device.[43]

Thus, significant privacy interests are at stake even when the government is on its best behavior in carrying out searches. And the government is not always on its best behavior. One consequence of the fallout from Edward Snowden's exposure of extensive surveillance by the National Security Agency ("NSA") was the revelation of a practice called "parallel construction," which involves covering up an unlawful investigative practice by "going through the motions of re-discovering evidence in some other way."[44] For example, the NSA might pass on a "tip" to a federal agent who was "trained to 'sanitize' the information and cover up its origin[.]"[45] The federal agent might be told "to look for a specific car at a certain place" and "find his or her own reason to stop and search the car."[46] One former DEA agent described this process as "just like laundering money—you work it backwards to make it clean."[47] Agents would be instructed never to reveal the original tip, thereby maintaining the secrecy of the underlying surveillance practices.[48] Parallel construction thus offers a workaround for constitutional limitations on intrusive surveillance practices, such as the requirement that law enforcement obtain a warrant before searching location data acquired from a person's cell phone.[49]

---

[43] *See Aaron.Alexis*, 21 F. Supp. 3d at 7 (discussing third-party privacy interests implicated by search of suspect's Facebook account).

[44] *Dark Side: Secret Origins of Evidence in US Criminal Cases*, HUMAN RIGHTS WATCH (Jan. 9, 2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

[45] Amanda Claire Grayson, Note, *Parallel Construction: Constructing the NSA Out of Prosecutorial Records*, 9 HARV. L. & POL'Y REV. S25, S33 (2015) (quoting *DEA Secretly Uses NSA to Prosecute Crime*, DEUTSCHE WELLE (Sept. 4, 2013), http://perma.cc/J983-5DHS).

[46] John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), https://www.reuters.com/article/world/uk/exclusive-us-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409S/.

[47] *Id.*

[48] *Id.*

[49] *See* Carpenter v. United States, 585 U.S. 296, 315–16 (2018) (finding that government acquisition of cell-site location information is a Fourth Amendment search requiring a warrant); Chatrie v. United States, No. 25-112, 2026 WL 1855568, at *4 (U.S. June 29, 2026) (finding that government

Parallel construction is a pressing concern with unlocked devices in law enforcement possession. Although the Constitution requires law enforcement officers to obtain a warrant before searching the contents of the device, there are few available means to compel them to actually do so,[50] especially where officers could retroactively construct an alternate narrative for their discovery of any evidence obtained. In *Brown*, the FBI held the unlocked cell phone for seven months before obtaining a warrant to search it.[51] This scenario raises clear dangers of parallel construction, undermining the efficacy of imposing Fourth Amendment limits on the scope of the search and threatening the privacy interests protected by those limitations.

The Fifth Amendment, of course, is not a catch-all protection of privacy in the way that the Fourth Amendment is. While the Fourth Amendment's limitations on searches and seizures are based on society's reasonable expectations of privacy, the Fifth Amendment targets a narrower harm: the dignity and autonomy interests violated by coerced confessions.[52] However, interpreters of the Fifth Amendment should not shut their eyes to privacy interests, nor blithely ignore the practical problems which Fifth Amendment jurisprudence may raise for the enforcement of Fourth Amendment jurisprudence. In an era of increasingly complex and technical—yet relatively cheap and easy[53]—forms of surveillance, courts must be attentive to the interplay of their

---

acquisition of Google Location History data is a Fourth Amendment search requiring a warrant).

[50] Magistrate Judge John Facciola of the District Court for the District of Columbia candidly acknowledged the possibility of law enforcement officers exceeding constitutional limitations when searching devices in *Aaron.Alexis*: "While there has never been anything stopping the government from exceeding the scope of an otherwise valid warrant when searching a physical place, it is clearly easier to do so when the government has an identical copy of an entire hard drive or database." 21 F. Supp. 3d at 10.

[51] *Brown*, 125 F.4th at 1200.

[52] *See Fisher*, 425 U.S. at 401; *see generally* Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857 (2005).

[53] *See, e.g.*, Carpenter v. United States, 585 U.S. 296, 311 (2018) (noting that "cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools").

precedents, or risk constitutional protections becoming an "empty promise."[54]

Treating biometric scanners as categorically testimonial would impose a general prohibition on their compulsion, unlike the Fourth Amendment's reasonableness-based restrictions.[55] Some may worry that such a rule would unduly restrict law enforcement, since not even a warrant or court order would be able to force someone to unlock their phone.[56] Law enforcement might then be cut off from the wealth of valuable evidence contained in cell phones and laptops, hampering their ability to solve serious crimes.[57] However, two key tools will permit the government to unlock devices on a more limited and case-by-case basis. First, law enforcement officers can negotiate access to a device by offering the device owner immunity against admission of the information discovered on the device in a future criminal prosecution.[58] Second, the foregone conclusion exception to the act of production doctrine would continue to apply to biometric scanners.

The foregone conclusion exception stems from *Fisher*, a case in which the Supreme Court held that a suspect in a criminal case could not exercise his Fifth Amendment privilege to prevent the government from subpoenaing tax documents held by his

---

[54] Mapp v. Ohio, 367 U.S. 643, 660 (1960).
[55] *Fisher*, 425 U.S. at 400.
[56] *See id.* at 400–01 (explaining that, unlike the Fourth Amendment, the Fifth Amendment cannot be satisfied by a warrant or showing of reasonableness).
[57] *See Riley*, 573 U.S. at 393–94 (discussing incredible storage capacity of cell phones). One example of cell phones' utility in solving crimes is the prosecution of Alex Murdaugh for the murder of his wife and son. In the absence of any witnesses, investigators were able to put together a timeline of events using Murdaugh's and others' cell phones' "call logs, text messages, GPS location data, information about the number of steps individuals took, whether a cell phone was locked or unlocked, when it was connected to Wi-Fi and Bluetooth, whether the phone backlights were on, and how the phones were orientated (landscape or portrait mode) at various times." Jonathan Kerr, *Riding on Horseback to the Moon: Consent Searches in the Age of Smartphones and Digital Tracking*, 82 WASH. & LEE L. REV. 491, 505 (2025).
[58] *See* Kastigar v. United States, 406 U.S. 441, 453 (1972) (holding that the government may compel testimony if it offers immunity against use of the evidence compelled, or evidence derived from the initial compulsion, in a future criminal prosecution).

attorney.[59] Although the Court focused on the fact that the government compulsion was exercised against the attorney, not the suspect who sought to exercise the privilege, the Court suggested in dicta that production of the documents would not be considered testimonial because the existence and location of the documents were a "foregone conclusion" to the government.[60] That reasoning has been fleshed out in the lower courts, which have found that otherwise testimonial evidence may no longer be protected where the essential information to be gained from that evidence was already known to the government.[61] Since the evidence "adds little or nothing to the sum total of the Government's information," the Fifth Amendment is not meaningfully served by protecting that evidence from compulsion.[62]

In a case concerning a cell phone or laptop, the government would need to "independently confirm" the information revealed when the device is unlocked: that a particular person is capable of unlocking the device using the biometric scanner.[63] Essentially, this would require the government to have evidence that the device belongs to that person and that the person is capable of accessing it, tasks which the government has been able to accomplish in more than one case.[64] The government will be able to compel a person to unlock a device so long as it conducts additional investigation before doing so.

---

[59] *Fisher*, 425 U.S. at 397.

[60] *Id.* at 411.

[61] *See, e.g.*, United States v. Doe, 670 F.3d 1335, 1347–49 (11th Cir. 2012) (discussing application of foregone conclusion doctrine); State v. Andrews, 234 A.3d 1254, 1273–74 (N.J. 2020) (same); Commonwealth v. Davis, 220 A.3d 534, 548–49 (Pa. 2019) (same).

[62] *Fisher*, 425 U.S. at 397.

[63] *Hubbell*, 530 U.S. at 44–45 (discussing facts of *Fisher*).

[64] *See, e.g.*, *Andrews*, 234 A.3d at 1274–75 (finding that the foregone conclusion applied to defendant's cellphone passcodes because "[t]he State established that the passcodes exist, [. . .] [and] the trial court record reveals that the cellphones were in [defendant's] possession when seized and that he owned and operated the cellphones, establishing his knowledge of the passcodes and that the passcodes enable access to the cellphones' contents"); State v. Johnson, 576 S.W.3d 205, 226 (Mo. Ct. App. 2019) (holding that the foregone conclusion exception applied because "the existence of the passcode, its possession or control by [the defendant], and the passcode's authenticity . . . were already known to the State").

That barrier will limit the scope of potential privacy intrusions by pushing the government to prioritize and allocate resources towards the cases it considers to be the most serious, rather than "compensat[ing] for its lack of evidence" by going on a "fishing expedition" through a person's phone or laptop.[65] Any remaining hindrances to investigations are the intended benefits of constitutional design, not its defects.[66]

The rapid growth and development of technology have forced the judiciary to answer new and pressing questions about the constitutional scope of police investigations. Warrant applications have become increasingly complex, requiring a more sophisticated technical understanding to parse than ever before.[67] And the increased ease of surveillance enables unprecedented intrusions into personal privacy.[68] Judges, recognizing these challenges, have sought creative methods to impose limits on government surveillance and data retention.[69] These efforts are

---

[65] *In re* Grand Jury Empanelled March 19, 1980, 680 F.2d 327, 335 (3d Cir. 1982); *Hubbell*, 530 U.S. at 32 (quoting United States v. Hubbell, 11 F.Supp.2d 25, 37 (D.D.C. 1998)).

[66] United States v. Smith, 110 F.4th 817, 841 (5th Cir. 2024) (Ho, J., concurring) ("[H]amstringing the government is the whole point of our Constitution.").

[67] *See, e.g.*, *Chatrie*, No. 25-112, 2026 WL 1855568, at *4 (finding that law enforcement conducted a search when they requested that Google draw a virtual "geofence" around a given physical perimeter and provide information about the location history of Google users within that perimeter).

[68] For example, the New York City Police Department's "Domain Awareness System" is capable of tracking any individual through their daily activities in the five boroughs by aggregating information from "(1) video cameras, including body-worn, handheld, dashboard, stationary, and aerial; (2) tracking tools, such as automated license plate readers ("ALPRs"), location trackers, and gunshot detectors; (3) biometric data, including from DNA collection, and fingerprint and iris scanners; (4) electronic monitoring devices, such as phone taps, X-ray imaging, digital record aggregation, and cryptocurrency analysis; and (5) social media surveillance, obtained by monitoring individuals' internet activity, scraping and storing online posts, and using social network analysis to map out a person's relationships, religious beliefs, and political affiliations, among other things," according to a lawsuit filed by the Surveillance Technology Oversight Project. Complaint at 5–6, Wridt v. City of New York, No. 1:25-CV-08903 (S.D.N.Y. Oct. 27, 2025).

[69] *See, e.g.*, *Aaron.Alexis*, 21 F.Supp.3d at *11–12 (listing various "minimization procedures" courts have put in place in order to restrict the government's

laudable, and they should be accompanied by increased sensitivity to the interplay of various doctrines and their consequences for personal privacy. Otherwise, Fourth and Fifth Amendment doctrine risks falling short of the Founders' promises. Courts should accordingly recognize the great dangers inherent in allowing the government to access the full contents of a device and apply Fifth Amendment protections to biometric scanners.

collection and retention of data pursuant to the search of digital information contained in a device or database).