LAW360®

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

DC Circ. Cellphone Ruling Upends Law Enforcement Protocol

By **Sarah Sulkowski** (February 6, 2025, 5:06 PM EST)


Sarah Sulkowski

On Jan. 17, the U.S. Court of Appeals for the District of Columbia Circuit issued a decision that will have significant consequences for law enforcement authorities seeking to access suspects' cellphones.

In U.S. v. Brown, the D.C. Circuit held that, by forcing a defendant in custody to use his fingerprint to unlock his cellphone, the FBI violated his Fifth Amendment privilege against self-incrimination.

The defendant, Peter Schwartz, was convicted at trial of assaulting police officers at the U.S. Capitol on Jan. 6, 2021. He was among the thousands of individuals convicted of Jan. 6-related crimes pardoned by President Donald Trump on Jan. 20, though prosecutors note he has 38 prior convictions spanning over three decades.

A month after the Jan. 6 insurrection, FBI agents arrested Schwartz and executed a search warrant at his home, where they found a cellphone in the bedroom. An FBI agent asked Schwartz for the passcode to the phone, and Schwartz responded with three possible codes, none of which succeeded in unlocking the phone. The FBI agent then used Schwartz's thumbprint to open the phone.

The agent could not remember at trial "precisely how that was done,"[1] but testified that his usual practice was to ask a suspect whether he wished to access any saved numbers in the phone for use at the jail.

Once the phone was unlocked, the FBI photographed information on it, including incriminating text messages, but did not conduct a full forensic search of the phone.

Seven months later, the FBI obtained a warrant to conduct a full search of the phone, pursuant to an affidavit that included the photographs of the phone's contents taken on the day of Schwartz's arrest.

At trial, Schwartz moved to suppress the results of the resulting phone search, arguing that the FBI had violated his Fifth Amendment privilege against self-incrimination by forcing him to unlock the phone.

The U.S. District Court for the District of Columbia disagreed, finding that — although the government conceded that it "had compelled Schwartz to unlock his cellphone," and that the contents were "inculpatory"[2] — Schwartz's doing so was not a testimonial act, but a merely physical one, and thus the Fifth Amendment did not apply.

The district court went on to rule that, in any event, Schwartz's Fifth Amendment claim was subject to the good faith exception, which — in the Fourth Amendment context — protects from suppression evidence seized by law enforcement in good faith reliance on a valid search warrant.

The D.C. Circuit reversed, holding that "the compelled opening of the cellphone was testimonial under the Fifth Amendment."[3]

The court reasoned that using a fingerprint to unlock a cellphone is more akin to a lie-detector test than to providing a blood sample or standing in a lineup, in that it seeks to use a physiological

response as evidence of guilt.[4]

According to the court, Schwartz's "act of unlocking the phone represented the thoughts 'I know how to open the phone,' 'I have control over and access to this phone,' and 'the print of this specific finger is the password to this phone'" — the same ideas he would have communicated if compelled to "verbally disclose the password."[5]

The Brown court explained that "testimonial acts are those physical actions that require no additional information to communicate an incriminatory message," unlike a blood sample, which must be analyzed before it can incriminate, or a handwriting exemplar, which must first be compared to another sample.[6]

According to the court, "[t]here is no additional information that is needed to understand the messages communicated by the act of opening a phone."[7]

And, because the subsequent search warrant for the phone was based at least in part on information extracted from the phone following the compelled unlocking, the inevitable-discovery doctrine — which, the court explained, "allows for the admission of evidence that would have been discovered even without the unconstitutional source"[8] — did not save the contents of the phone from suppression.

The D.C. Circuit went on to reverse the district court's ruling on the good faith exception, as well, holding that there was no evidence that the FBI agent in fact acted in good faith, as he could not remember the circumstances of the unlocking, and the search warrant for Schwartz's home expressly withheld authority to force Schwartz to provide the passcode or biometric key to unlock his phone.

And, because the government had not offered "any developed argument in support of extending the good faith exception to the Fifth Amendment, offering only a cursory footnote," the D.C. Circuit declined to decide whether that exception, developed in the Fourth Amendment context, applies to Fifth Amendment violations.[9]

Notably, the Brown court took pains to distinguish the facts before it from those of U.S. v. Payne, in which the U.S. Court of Appeals for the Ninth Circuit held in April 2024 that a defendant did not commit a testimonial act when police forced his thumb against his cellphone to unlock it.[10]

According to the D.C. Circuit, the salient difference between the two cases is that the officer in Payne did not require the defendant to "independently select the finger that he placed on the phone."[11]

Of course, as noted, the FBI agent in Brown testified that he could not remember how Schwartz came to press his thumb to his phone, so it's far from clear that the facts of Brown meaningfully differ from those of Payne. But even putting this point aside, the D.C. Circuit did not explain how its holding that Schwartz made a testimonial communication that "I have control over and access to this phone" can be distinguished from the circumstances of Payne.

This apparent circuit split is one worth watching, as it may convince the U.S. Supreme Court to weigh in on the issue sooner than it otherwise might.[12]

Moreover, the Brown decision has immediate and significant implications for law enforcement. Cellphones, of course, "contain 'vast trove[s]' of personal information such as diary entries, personal photographs, medical data, and banking information" — in short, they "are mobile hard drives" containing data of great interest to authorities, as the U.S. District Court for the District of Connecticut aptly noted in its July 2024 decision in U.S. v. Salaman.[13]

Accordingly, police officers and federal agents routinely seek search warrants authorizing them to forcibly press a suspect's fingers against the suspect's phone to unlock it, and lower courts have regularly ruled that such warrants do not violate the Fifth Amendment.[14]

If deprived of this method of access, law enforcement may have to resort to "brute force" attempts to override cellphone security, which courts have noted can take years or even decades to yield results.[15]

Members of the criminal defense bar should be alert for opportunities to use the Brown decision as a ground for the suppression of electronic evidence seized from clients' cellphones.

Further, with the widespread use of facial recognition largely replacing fingerprints as a mechanism for unlocking electronic devices, Brown can provide a jumping-off point for an argument that forcibly holding a cellphone to a suspect's face likewise raises Fifth Amendment concerns, as several federal district courts have concluded.[16]

And, of course, clients should always be advised not to voluntarily provide passcodes or biometrically unlock cellphones for law enforcement.

Given the novel nature of the Brown ruling and the momentous interests at stake on both sides of the issue, we can expect to see Fifth Amendment arguments crop up frequently in the cellphone context in the wake of Brown. Defense lawyers should be sure to keep this significant decision close at hand.

Sarah A. Sulkowski is a partner at Gelber & Santillo PLLC. She previously served as an assistant U.S. attorney in the Criminal Division of the U.S. Attorney's Office for the District of New Jersey.

[1] United States v. Brown , — F.4th —, 2025 WL 223881, at *8 (D.C. Cir. Jan. 17, 2025).

[2] Id. at *9-10.

[3] Id. at *9.

[4] Id. at *10-11.

[5] Id. at *11.

[6] Id.

[7] Id.

[8] Utah v. Strieff , 579 U.S. 232, 238 (2016).

[9] Brown, 2025 WL 223881, at *14.

[10] 99 F.4th 495 (9th Cir. 2024).

[11] Brown, 2025 WL 223881, at *12 n.2.

[12] See United States v. Thomas , 939 F.3d 1121, 1132 (10th Cir. 2019) ("[A] core responsibility of the Supreme Court is to resolve circuit splits . . . .").

[13] United States v. Salaman , — F. Supp. 3d —, 2024 WL 3565248, at *7 (D. Ct. July 29, 2024) (quotation marks omitted).

[14] See, e.g., Matter of Search Warrant Application v. Barrera , 415 F. Supp. 3d 832, 837-38 (N.D. Ill. 2019) (collecting cases and noting, pre-Payne, that "neither the Supreme Court, the Seventh Circuit, nor any other court of appeals has weighed in").

[15] See, e.g., United States v. Raymond , No. 21-380 (CKK), 2023 WL 7005341, at *4 (D.D.C. Oct. 24, 2023) (noting that, as of 2020, "it could take . . . up to twenty-five years to 'brute force' entry into the phones, i.e., trying random codes until one works"); United States v. Kopankov , 672 F. Supp. 3d 862, 865 (N.D. Cal. 2023) ("The government represents it is not uncommon for entire

racks of phones to be undergoing brute force attacks for years.") (quotation marks omitted); United States v. Morgan , 443 F. Supp. 3d 405, 407 (W.D.N.Y. 2020) (noting that, after nearly two years, the government's "brute force" attempts had "apparently progressed from its initial one-in-a-million odds of breaking the passcode" to a point where" a mere 960,526 possible passcodes remained").

[16] See United States v. Wright , 431 F. Supp. 3d 1175, 1187-88 (D. Nev. 2020) ("The Court therefore finds that WCSO detectives' unlocking of Defendant's phone with his face infringes the Fifth Amendment's privilege against self-incrimination, was an abuse of power and is unconstitutional.") (quotation marks and brackets omitted); Matter of Residence in Oakland, California, 354 F. Supp. 3d 1010, 1014-15 (N.D. Cal. 2019) ("[I]f a person cannot be compelled to provide a passcode because it is a testimonial communication, a person cannot be compelled to provide one's finger, thumb, iris, face, or other biometric feature to unlock that same device."), rev. denied as moot sub nom. In re Search of a Residence in Oakland, California , No. 19MJ70053KAW1JD, 2019 WL 6716356 (N.D. Cal. Dec. 10, 2019).
