The Epstein Files and the risks of forensic image retention

By William E. Johnston, Esq., Bird, Marella, Rhow, Lincenberg, Drooks & Nessim LLP

MAY 11, 2026

The Department of Justice (DOJ) continues to experience blowback from how it handled the release of voluminous files from the criminal investigations of Jeffrey Epstein. Overlooked in this debate is the Fourth Amendment question raised by the disclosures themselves: what the Constitution requires when the government makes forensic images of electronic devices pursuant to search warrants.

Every search warrant executed on a modern device produces a forensic image, and every forensic image retained by the government carries the same indefinite risk tail.

In July 2019, concurrent with Epstein's arrest on sex trafficking charges, the Federal Bureau of Investigation (FBI) executed search warrants at his private island and New York townhouse. Agents seized 62 computers, phones and hard drives. The files on the forensic images of those devices, containing communications going back to the early 2000s, appear to be a main source of the "Epstein Files." *See* Letter from Todd Blanche, Deputy U.S. Att'y Gen., U.S. Dep't of Justice, Re: Epstein Files Transparency Act – Production of Department Materials (Jan. 30, 2026), available here: https://bit.ly/4u6xHBX.

In the Epstein Files Transparency Act, Congress mandated that the DOJ release all files related to Epstein, not just evidence of the crimes the DOJ was investigating. So the DOJ released tens of thousands of documents that it had no authority to use as substantive evidence — because they fell outside the scope of the original warrants — but which had nevertheless been retained through forensic images. *See* Memorandum, U.S. Dep't of Justice, Search Warrant Responsiveness Review Protocol for Image and Video files, Oct. 19, 2020, EFTA00153170, available here: https://bit.ly/3PznFdt.

Ordinarily, a warrant that authorized seizure of files for which there was no probable cause would violate the Fourth Amendment. But the retention of forensic images, in effect, permits the government to maintain possession over such files indefinitely. Until courts decide what limits to apply to such retention, the burden rests on defense counsel to anticipate the over-seizure risks facing their clients and, where necessary, seek return or destruction of the images.

The forensic image and the Fourth Amendment

The main protection against over-seizure is the Fourth Amendment's particularity and probable cause requirements, which require that the warrant describe the items to be seized with specificity and that probable cause exist for each item to be seized. In the analog setting, these limitations prevent agents from seizing every document in a home or office. In the digital setting, it should have the same effect, but the mechanics complicate that goal.

Agents first must image the device, because examining it directly risks altering data. Imaging permits the government to return the original device, but it also extends the timeline for review, creating two main risks.

First, the government's theory of prosecution may evolve beyond the one articulated in the warrant affidavit, leading to seizure of items not originally contemplated. Second, with effectively unlimited time, the government can seize additional items under the plain-view exception. The 9th U.S. Circuit Court of Appeals warned of this risk in the 2010 case *United States v. Comprehensive Drug Testing*, noting that the doctrine "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant."

Courts have responded with two solutions: a timeline for scoping the warrant (i.e., determining which items fall within the warrant and which ones do not) and requiring a new warrant before the government may search the image for crimes not identified in the original warrant. Ninth Circuit magistrates frequently prescribe scoping timelines in the warrants themselves; elsewhere, courts evaluate them retroactively for reasonableness.

Even with those restrictions, the question of what happens to the forensic image remains. Prosecutors who confine their

use to within-scope files still retain the forensic image to authenticate trial exhibits. Nothing prevents the government from obtaining a new warrant years later to search the image for new crimes, weakening the Fourth Amendment privacy protections and creating a risk tail that stretches indefinitely into the future.

Forensic images in the Epstein investigation

The Epstein case illustrates the risk. On July 6, 2019, Epstein was arrested and his 62 devices were seized; before the FBI could finish imaging them, on August 10, 2019, Epstein committed suicide. Under the prevailing rule that most constitutional rights do not survive death, a deceased person no longer has Fourth Amendment standing to challenge a search of his electronic devices.

The lesson for defense counsel is straightforward. Scrutinize every warrant for particularity, and negotiate destruction or sequestration protocols during the review.

In theory, the government could have searched and seized everything on Epstein's devices without consequence. To their credit, prosecutors in the Southern District of New York reviewed the devices as if Epstein were alive. As revealed in a DOJ memorandum released as part of the Epstein Files themselves, prosecutors obtained a new warrant and segregated within-scope files from those that fell outside.

The investigation continued into his former partner, Ghislaine Maxwell, and prosecutors presumably wanted to insulate themselves from any later Fourth Amendment claim Maxwell might assert. But the DOJ never discarded the forensic images.

That retention was not contrary to 2nd Circuit law though the circuit briefly appeared headed that way. In the 2014 case *United States v. Ganias*, a panel held that a new warrant search of out-of-scope materials on a hard drive 18 months after the initial warrant was unreasonable.

On rehearing en banc, however, the 2nd Circuit reversed on good-faith grounds and expressly declined to reach the constitutional question. It remains an open question in every circuit whether the government may retain forensic images and for how long.

So when Congress commanded that the DOJ release all files related to Epstein, the forensic images were the inevitable source of many disclosed files that were not themselves evidence of the crimes under investigation. While few subjects of criminal investigations will have their files legislated into the public domain, the retention of forensic images still has privacy implications for ordinary people whose electronic devices are seized.

The Rule 41(g) motion

Defense counsel who want to minimize the risks of over-seizure should address the forensic image directly. The mechanism is a motion under Federal Rule of Criminal Procedure 41(g), which permits a person aggrieved by an unlawful search or by the deprivation of property to move for the property's return. Although designed for physical property, the rule has increasingly been applied to digital evidence.

The relief commonly sought is destruction or return of the forensic image, or at minimum segregation of out-of-scope materials. Such a motion should establish that the government has had ample time to complete its scoping review, identify the categories of out-of-scope materials with specificity and propose a concrete remedy.

Defense counsel should also try to negotiate voluntary restrictions with the DOJ, such as filter team protocols, defined review timelines and destruction obligations. Building those terms into the record by stipulation, court order or warrant addendum creates a stronger basis for later enforcement.

The Richman case

The most notable recent development came in November 2025, when Columbia Law Professor Daniel Richman, a friend and attorney to former FBI Director James Comey, filed a Rule 41(g) motion in the U.S. District Court for the District of Columbia.

Richman's personal computer was first imaged in 2017 for limited searches with his consent. Between 2017 and 2020, the FBI searched his email accounts, iCloud account and the 2017 computer image as part of an investigation into Comey's alleged disclosure of classified information. The FBI retained complete copies.

Years later, amid the renewed DOJ investigation of Comey that culminated in his September 2025 indictment on charges of false statements to Congress, agents searched those copies again without a new warrant. In December 2025, the court, in *Richman v. United States*, ruled that the Fourth Amendment does not categorically prevent the government from retaining forensic images, but requires the government to obtain a new warrant before returning to the data in a subsequent investigation.

The government's failure to obtain a new warrant rendered the later search unconstitutional, and the court ordered the government to return all its copies to Richman. Although the Comey false statements indictment was dismissed before the *Richman* order issued, the order makes the seized materials unusable in any future prosecution absent a new warrant.

The victory for Richman (and Comey) was incomplete. The government insisted it intended to re-prosecute Comey,

and the court deferred in part to the government's interest in pursuing future investigations. The court ordered the government to deposit a copy of Richman's materials with the U.S. District Court for the Eastern District of Virginia.

The lesson from *Richman* is that convincing judges to order destruction of forensic images is an uphill battle. But its reasoning suggests litigants are more likely to obtain such an order when the government's investigation has closed, or when no files derived from those images will be used in a pending criminal case.

Looking ahead

The Epstein Files are an unusual vehicle for a Fourth Amendment lesson, but the underlying problem is commonplace. Every search warrant executed on a modern device produces a forensic image, and every forensic image retained by the government carries the same indefinite risk tail.

The lesson for defense counsel is straightforward. Scrutinize every warrant for particularity, and negotiate destruction or sequestration protocols during the review. If negotiation proves fruitless, file the Rule 41(g) motion when the investigation closes without charges or after a case ends; *Richman* shows that courts may grant meaningful relief in the right posture.

The debate in the coming years will be whether continued possession of a forensic image, even when tied to an active investigative need, is itself a Fourth Amendment violation that demands a remedy.

About the author

William E. Johnston is a partner at **Bird, Marella, Rhow, Lincenberg, Drooks & Nessim LLP** in Los Angeles, where he focuses on white collar criminal defense and complex civil litigation. He previously served as an assistant chief in the fraud section, criminal division, U.S. Department of Justice in Washington, D.C. He can be reached at wjohnston@birdmarella.com.

This article was first published on Reuters Legal News and Westlaw Today on May 11, 2026.