

**UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF NEW YORK**

PASCAL ABIDOR, <i>et al.</i>	)	
	)	
Plaintiffs,	)	Case No.
	)	1:10-cv-04059
v.	)	
	)	(Korman, J.)
JANET NAPOLITANO, <i>et al.</i>	)	(Azrack, M.J.)
	)	
Defendants.	)	
	)	

**MEMORANDUM IN SUPPORT OF PLAINTIFFS’ ALTERNATIVE MOTION FOR  
RELIEF PURSUANT TO FEDERAL RULE OF CRIMINAL PROCEDURE 41(g)  
AND FOR EXPUNGEMENT**

**BACKGROUND**

In the Complaint, Plaintiff Pascal Abidor (“Plaintiff”) requested that the Court “[o]rder defendants to return all information unlawfully obtained from [Plaintiff] and to the extent information cannot be returned, to expunge or otherwise destroy that information, including photographs and fingerprints.” Compl. ¶ F. The Court concluded that an order compelling the return or destruction of Plaintiff’s private information was unnecessary because “the Department of Justice attorney conceded at oral argument that [Plaintiff’s] materials ‘would have been destroyed but for the fact that cases had been filed,’ and that they were being retained as potentially relevant to those cases.” Mem. and Order at 20, ECF No. 36 (quoting Hr’g Tr., 32:4-29, June 8, 2011).

It is now apparent, however, that that is not the case. When Plaintiff followed up to request a certification “that all images of [Plaintiff’s] electronic devices have been destroyed and any documents containing data extracted, or information derived, from the contents of the devices or images have been destroyed,” *see* Declaration of Catherine Crump (“Crump Decl.”),

Exhibit A, defense counsel responded by representing only that “Defendants will destroy all images of [Plaintiff’s] laptop in their possession.” *See id.*, Exhibit B.

It is important to understand precisely what the government’s representation encompasses and what it does not. Plaintiff traveled with a variety of devices, all of which were seized and may well have been copied by the government: his laptop, his external hard drive, two cell phones, and his digital camera. *See* Declaration of Pascal Abidor (“Abidor Decl.”) ¶¶ 2, 12. But defendants say nothing about destroying data taken from any of Plaintiff’s devices other than the laptop. Moreover, they speak only of expunging “images” of the laptop. An “image,” or “mirror image,” is a technical term, meaning “an exact duplicate of the entire hard drive.” *United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 48 (D. Conn. 2002). It does *not* include, for example, a file folder containing only the photographs extracted from Plaintiff’s devices, an individual copy of one of Plaintiff’s Word documents, or even a complete copy of his hard drive where only a single bit of data was altered. It also does not encompass records derived from Plaintiff’s electronic devices, such as investigator’s notes created as a result of the government’s review of Plaintiff’s email correspondence. Because it remains entirely unclear what files or records are even in the government’s possession, the government’s representation leaves open the disturbing possibility that it will continue to possess copies of all of Plaintiff’s digital files, along with copious records analyzing the information contained in those files, long after this litigation has concluded.

Given the government’s near-meaningless representation, Plaintiff filed a motion for partial reconsideration asking the Court to revise its ruling to more accurately reflect the limited scope of the government’s promised expungement and, based on this factual understanding, to find that Plaintiff has standing. Mem. in Supp. of Pls.’ Mot. for Partial Recons. at 1, ECF No. 38-

1. The Court construed Plaintiff's motion for partial reconsideration as, in the alternative, a Federal Rule of Criminal Procedure 41(g) motion for return of property, and ordered briefing on the applicability of Rule 41(g).

### ARGUMENT

Plaintiff relies on two separate avenues of equitable relief to ensure that the government will not retain his private electronic information. First, the equitable principles embodied in Rule 41(g) entitle Plaintiff to the return or destruction of all government copies of his private digital information—i.e., the images made from his electronic devices and the data extracted from those devices or images. Second, although the Second Circuit has construed Rule 41(g) not to cover files created by the government, the Court should exercise its inherent equitable power to order the expungement of all government records derived from Plaintiff's private digital information.

Moreover, because the relief sought by the present motion depends on a precise understanding of what data the government has in its possession and what records it has created as a result of reviewing the contents of Plaintiff's electronic devices, evidence regarding those holdings must be provided. *See* Fed. R. Crim. P. 41(g); *Mora v. United States*, 955 F.2d 156, 158–59 (2d Cir. 1992). The Court should therefore order the government to: (1) provide a full accounting of files in its possession that were either copied or derived from plaintiff's electronic devices; (2) certify that it has destroyed each such file or record in its possession.

#### **I. This Court Should Exercise Its Equitable Jurisdiction to Order the Destruction of Plaintiff's Digital Information and Records Derived From That Information.**

Where, as here, “no criminal proceedings against the movant are pending or have transpired, a motion for the return of property is treated as [a] civil equitable proceeding[] even if styled as being pursuant to Fed. R. Crim. P. 41[(g)].” *Id.* at 158 (first and second alterations in original) (internal quotation marks and citation omitted); *see also United States v.*

*Comprehensive Drug Testing*, 621 F.3d 1162, 1172 (9th Cir. 2010) (en banc) (per curiam); *Diaz v. United States*, 517 F.3d 608, 610 (2d Cir. 2008).<sup>1</sup> Under such circumstances, “[a] Rule 41(g) motion is an equitable remedy.” *De Almeida v. United States*, 459 F.3d 377, 382 (2d Cir. 2006). Similarly, the Court’s authority to order expungement of government records derives from its inherent equitable powers. *United States v. Schnitzer*, 567 F.2d 536, 539 (2d Cir. 1977). The Court may award such equitable relief “when there is no adequate remedy at law and the equities favor the exercise of jurisdiction.” *De Almeida*, 459 F.3d at 382. Those circumstances apply here.

First, Plaintiff has no adequate remedy at law. Unlike the petitioner in *De Almeida*, he has had no opportunity to challenge the legality of the government’s continued seizure of his private information in a civil, criminal, or administrative forfeiture proceeding. *See id.*; *see also* 3A Charles Alan Wright, et al., *Federal Practice & Procedure* § 690 n.12 (4th ed. 2013) (collecting cases where Rule 41(g) proceedings were dismissed due to the existence of alternative forfeiture proceedings where the seizure could be challenged). Plaintiff is aware of no other form of legal relief to effectuate the return or destruction of his private information, and the government has identified none. This Court’s equitable jurisdiction is therefore Plaintiff’s only recourse for relief from the continuing invasion of his privacy.

Second, the equities favor the exercise of this Court’s equitable jurisdiction. Plaintiff has a significant and ongoing interest in preventing the government from retaining and further disseminating his private information. *See Comprehensive Drug Testing*, 621 F.3d at 1173–74 (holding that petitioner for Rule 41(g) relief was “plainly aggrieved” by the government’s continued possession of its members’ drug testing records, particularly because of “the risk to

---

<sup>1</sup> Although these proceedings are technically equitable, they are nevertheless largely governed by the standard set out in Rule 41(g). Plaintiff accordingly refers to his rights under the Rule.

players associated with disclosure” of the records); *Paton v. La Pade*, 524 F.2d 862, 868 (3d Cir. 1975) (“[H]istory of a not too distant era has demonstrated that future misuse of a file labeled ‘Subversive Material’ can prove extremely damaging. As the district court aptly observed, ‘the existence of (the) records may at a later time become a detriment to [the plaintiff].’”). As Plaintiff averred in his Complaint, an examination of his laptop revealed that government agents had access to “highly private and expressive materials that reveal intimate details about [his] life, such as [his] personal photos, a transcript of a chat with [his] then-girlfriend, copies of email correspondence, class notes, journal articles, [his] tax return, his graduate school transcript, and [his] resume.” Declaration of Pascal Abidor (“Abidor Decl.”) ¶ 25. These files and every other file on Plaintiff’s laptop—and possibly files from other electronic devices, as well as information from his online email and social networking accounts—remain in the government’s possession, and constitute a continuous and irreparable invasion of Plaintiff’s privacy. The government’s retention of a potentially massive amount of Plaintiff’s private digital information, and records derived from that information, “results in injuries and dangers that are plain enough.” *Paton*, 524 F.2d at 868 (quoting *Sullivan v. Murphy*, 478 F.2d 938, 970 (D.C. Cir. 1973)) (internal quotation marks omitted).<sup>2</sup>

---

<sup>2</sup> In determining whether to invoke equitable jurisdiction for Rule 41(g) relief, some courts further consider whether the government displayed a “callous disregard” for the petitioner’s constitutional rights. *See, e.g., United States v. Huggins*, No. 13-CR-00155 (SHS) (SN), 2013 WL 1728269, at \*4 (S.D.N.Y. March 22, 2013). Plaintiff maintains that the suspicionless search and seizure of his electronic devices, together with Defendants’ unwarranted retention of the information obtained from those devices, evinces a callous disregard of his Fourth Amendment rights. The Court need not reach this issue, however, because Rule 41(g) itself makes clear that relief may be awarded to “[a] person aggrieved . . . by the deprivation of property,” as Plaintiff indisputably is here, even where that property was lawfully seized. Fed. R. Crim. P. 41(g) (emphasis added); *see also* Fed. R. Crim. P. 41 (notes of advisory committee on rules – 1989 amendments) (stating that what is now Rule 41(g) was specifically amended to provide that “a person whose property has been lawfully seized may seek return of property when aggrieved by the government’s continued possession of it”). As the Tenth Circuit held in *Floyd v. United*

**II. The Court Should Order the Government to Destroy All Its Copies of Plaintiff's Private Digital Information.**

Federal Rule of Criminal Procedure 41(g) provides as follows:

A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property.<sup>3</sup>

To prevail on a Rule 41(g) motion, the petitioner “must demonstrate that (1) he is entitled to lawful possession of the seized property; (2) the property is not contraband; and (3) either the seizure was illegal or the government's need for the property as evidence has ended.” *In re Application of Madison*, 687 F. Supp. 2d 103, 109 (E.D.N.Y. 2009) (quoting *Ferreira v. United States*, 354 F. Supp. 2d 406, 409 (S.D.N.Y. 2005)) (internal quotation marks omitted). Plaintiff meets these requirements, and therefore has a right to the return or destruction of all copies of his private digital information—including both the images made from his electronic devices and all data copied or extracted from the devices or images—pursuant to Rule 41(g).

---

*States*, “It would be anomalous to impose as a jurisdictional hurdle a requirement more restrictive than the substantive harm specifically sought to be remedied by Rule 41[(g)].” 860 F.2d 999, 1003 (10th Cir. 1988) (refusing to consider the “callous disregard of constitutional” factor, because the then-current version of Rule 41(g) required only a showing of illegality). Even if the Court concludes that the antiquated “callous disregard” factor weighs against Plaintiff in the balance of equities, however, that factor alone does not overcome the other factors supporting the exercise of equitable jurisdiction.

<sup>3</sup> As the Rule's text demonstrates, Rule 41(g) motions must be filed in the district where the property was seized. Here, Plaintiff's electronic devices were seized in Champlain, Clinton County, which is located in the Northern District of New York. However, because this is an ancillary civil equitable proceeding, the Rule's venue requirement does not apply. *See Reyes-Dilone v. United States*, Nos. 12 Civ. 3902(LAP), 08 Crim. 351(LAP), 2013 WL 1204058, at \*2 & n.5 (S.D.N.Y. March 25, 2013) (holding that Rule 41's venue requirement does not apply to civil equitable proceedings, and that the district court where the defendant was tried has ancillary jurisdiction over his or her post-trial motion for return of property) (collecting cases). Similarly, this too is a case where the Court is being asked to exercise its ancillary equitable jurisdiction. If the Court disagrees, Plaintiff respectfully requests that the proceeding be transferred to the Northern District of New York.

First, Plaintiff is entitled to lawful possession of the images of his electronic devices, as well as all data extracted or copied from the devices or images. A petitioner retains a property interest in copies made from files, documents, recordings, and other media that were once in his possession. *See Sovereign News Co. v. United States*, 690 F.2d 569, 577 (6th Cir. 1982) (holding that the petitioner had a property interest in copies made by the government from its lawfully seized business records, because petitioner had possessed the records before they were copied); *accord United States v. Cvijanovich*, 359 F. App'x 675, 676 (8th Cir. 2010); *Stancil v. United States*, 978 F.2d 716, at \*2 n.2 (9th Cir. 1992) (table). This property interest does not automatically entitle the petitioner to destruction of all copies of his private media in the government's possession, where, for example, the records or documents at issue "are relevant to ongoing or contemplated investigations and prosecutions." Fed. R. Crim. P. 41 (notes of advisory committee on rules – 1989 amendments). "In some circumstances, however, equitable considerations might justify an order requiring the government to return or destroy all copies of records that it has seized." *Id.*; *see also Comprehensive Drug Testing*, 621 F.3d at 1174 (affirming the district court judge's decision to order the return of all copies of petitioner's drug test records, pursuant to Rule 41(g)).<sup>4</sup>

Those circumstances are demonstrably present here, where the government retains a potentially massive amount of Plaintiff's private digital information and has given no indication that it *ever* intends to destroy its copies of that information. Electronic devices of the sort at

---

<sup>4</sup> To be sure, the Second Circuit has not recognized a Rule 41(g) property interest in the government's own records. *See Bova v. United States*, 460 F.2d 404, 407 (2d Cir. 1972) (holding that the predecessor to Rule 41(g) did not apply to government tapes of intercepted conversations); *see also Ferreira*, 354 F. Supp. 2d at 410 ("Under Rule 41(g), the property Ferreira can recover is that over which he can establish a sufficient ownership or possessory interest; he cannot recover property of another or property that was never in his possession."). As Plaintiff argues in the next section, however, the Court can and should exercise its inherent equitable power to order the expungement of these government records.

issue here “contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails.” *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc ). And, with the advent of “cloud computing,” an electronic device may also routinely allow access to all manner of files stored by the device’s owner on remote servers rather than on the device itself. *Id.* at 965.<sup>5</sup> Here, Plaintiff stored a large amount of his personal and private information on his laptop and other electronic devices, including: “academic research and reading materials, class notes, emails and chat records with [his] then-girlfriend and friends, photos of friends and family, movies, music, journal articles of interest to [him], documents detailing [his] academic credentials, tax records, and images downloaded from the Internet.” Abidor Decl. ¶ 2. And, at the time the devices were seized, Plaintiff states that he “had saved a variety of passwords on [his] computer, raising the possibility that the government could have used the password to log into [his] remote accounts,” and that his “laptop was configured to automatically allow access to [his] online email and social networking accounts, such that government agents could also have searched through [his] remotely stored correspondence and communications by accessing them through [his] computer.” *Id.* ¶ 26. The government accordingly had access to all manner of Plaintiff’s digital information—akin to his office filing cabinet, personal diary, full mailing correspondence, accounting materials, photo album, magazine collection, and record collection. For all Plaintiff knows, the government intends to keep the lion’s share of that information indefinitely. That is an egregious invasion of Plaintiff’s personal privacy, and it tilts the scales sharply in favor of requiring the government to destroy all copies of Plaintiff’s private digital information.

---

<sup>5</sup> Moreover, the devices often “retain sensitive and confidential information far beyond the perceived point of erasure, notably in the form of browsing histories and records of deleted files.” *Id.*



The remaining two requirements for prevailing on a Rule 41(g) motion are easily demonstrated. “When a Rule 41(g) motion is made before an indictment is filed, but a criminal investigation is pending, the burden of proof is on the movant to establish that the seizure was illegal and that the movant is entitled to lawful possession of the property.” *In re Application of Madison*, 687 F. Supp. 2d at 117. However, where “the property in question is no longer needed for evidentiary purposes, the burden of proof changes.” *Id.* The petitioner is then “presumed to have a right to the return of the property,” even if the initial seizure was legal, “and the government has the burden of establishing that it has a legitimate reason for the continued retention of the property, *i.e.*, that it is contraband or subject to forfeiture.” *Id.* (citing *In re Grand Jury Subpoena Duces Tecum*, 49 F. Supp. 2d 451, 453 (D. Md. 1999)); *see also United States v. Martinson*, 809 F.2d 1364, 1369 (9th Cir. 1987).

Thus far, the government has never suggested that the images of Plaintiff’s electronic devices and the copies of his files are or will be needed for evidentiary purposes once this proceeding has terminated. It therefore bears the burden of demonstrating that Plaintiff’s materials in its possession are contraband, subject to forfeiture, or necessary to effectuate some other significant government interest. But it asserts no such interest. Instead, it merely asserts a tautological interest in keeping records for the purpose of documentation. *See* Defs.’ Opp. to Pls.’ Mot. for Recons. at 6. That interest is insufficient to justify the continued retention of Plaintiff’s files. “The government may not keep the copies purely for the sake of keeping them or because it is ‘hopeful’ they may be relevant to some future investigation. This amounts to harassment.” *Sovereign News Co.*, 690 F.2d at 578 (citation omitted). To the extent the government asserts an interest in retaining Plaintiff’s files for the purpose of supervising agency

action, Defs.' Opp. to Pls.' Mot. for Recons. at 6, it has yet to explain why Plaintiff's private information is necessary to effectuate that interest.

The government alternatively maintains that destroying its copies of Plaintiff's electronic data will somehow interfere with its records maintenance and retention policies. *See id.* Those concerns are unfounded. In *House v. Napolitano*, a case like this one in several significant respects, the government agreed to certify the destruction of documents "contain[ing] data extracted, or information derived, from the contents of [Mr. House's] devices or images [made of those devices]." Settlement Agreement at 3, No. 11-10852-DJC (D. Mass. May 23, 2013).<sup>6</sup> Presumably, the government can achieve similar results in this case. Moreover, even if the government's records maintenance policies do require the retention of Plaintiff's private digital information, this Court nevertheless has the equitable power to override those policies in order to protect Plaintiff's significant privacy interests. *See Schnitzer*, 567 F.2d at 539 ("The government's [legal] need to maintain arrest records must be balanced against the harm that the maintenance of arrest records can cause citizens.").

### **III. The Court Should Order the Government to Expunge All Records Derived From Plaintiff's Private Digital Information.**

Although Rule 41(g) does not provide a vehicle for the expungement of government records derived from Plaintiff's digital files, the Court may nevertheless order such expungement pursuant to its inherent equitable powers. *See id.* (explaining, in the context of government arrest records, that "expungement lies within the equitable discretion of the court"). "Any particular request for expungement must be examined individually on its merits to determine the proper balancing of the equities." *Id.* at 540; *see also, e.g., Paton*, 524 F.2d at 868 ("Determination of the propriety of an order directing expungement involves a balancing of interests; the harm

---

<sup>6</sup> Available at [https://www.aclu.org/files/assets/house\\_settlement.pdf](https://www.aclu.org/files/assets/house_settlement.pdf).

caused to an individual by the existence of any records must be weighed against the utility to the Government of their maintenance.”). This balancing test resembles the Rule 41(g) balancing test applied to determine whether the government must destroy its copies of Plaintiff’s private digital information. *See* Fed. R. Crim. P. 41 (notes of advisory committee on rules – 1989 amendments) (citing *Paton*, 524 F.2d at 867–69). The Court must, however, “be cognizant that the power to expunge is a narrow one, and should not be routinely used whenever a criminal prosecution ends in an acquittal, but should be reserved for the unusual or extreme case.” *Schnitzer*, 567 F.2d at 539 (internal quotation marks omitted).

This is just such a case. The privacy interests implicated by Defendants’ continued possession of Plaintiff’s personal information almost four years after the search occurred strongly support expungement. Whereas most requests for expungement pertain to the petitioner’s arrest records—which serve an “important function,” involve relatively few items of identifying information, and “help to meet the compelling public need for an effective and workable criminal identification procedure”, *id.* (internal quotation marks omitted)—the government here retains a veritable picture of Plaintiff’s life up to the moment his electronic devices were seized and copied. The government’s retention of records derived from Plaintiff’s private digital information long after any apparent need for the information has dissipated qualifies as a significant and unjustified invasion of Plaintiff’s privacy. *See Lake v. Ehrlichman*, 723 F. Supp. 833, 834–35 (D.D.C. 1989) (exercising the court’s inherent equitable authority to order the expungement of wiretap logs, as well as FBI memoranda and summaries based the logs, because petitioners’ privacy interests in their recorded conversation “clearly outweigh[ed] the interests of the government in preserving records of dubious interest and questionable accuracy”); *Smith v. Nixon*, 664 F. Supp. 601, 604–605 (D.D.C. 1987) (the “sense of violation

and trauma” experienced by the wiretap subjects when they learned about the recordings far outweighed the government’s interest in preserving the records as a matter of historical interest); *cf. Skinner v. Ry. Labor Execs. Ass’n*, 489 U.S. 602, 616 (1989) (observing that government *analysis* of the plaintiffs’ urine samples qualified as a “further invasion of the tested employee’s privacy interests”); *Chastain v. Kelley*, 510 F.2d 1232, 1236 (D.C. Cir. 1975) (recognizing that an individual may have a right to expungement of information that is “prejudicial without serving any proper purpose” of the government’s, “as may be the case with information about his private and personal relationships”).

To remedy this significant privacy invasion, it is essential that the Court require the government to destroy *all* of Plaintiff’s private digital information, regardless of whether that information is located in copies of Plaintiffs’ data or government records analyzing that data. Were the rule otherwise, the government would simply have an incentive to include as much private information as possible in government records exempt from Rule 41. The Court should not countenance such an anomalous result. Plaintiff’s significant interest in securing his private digital information thus counsels strongly in favor of expungement.

On the other hand, the information at issue here is of dubious value to the government. The government relied on its border control interests to justify its initial search and seizure of Plaintiff’s electronic devices, but that interest evaporated a long time ago. Moreover, precisely because there are so few *ex ante* restrictions on the government’s search authority at the border, the Court should closely regulate the government’s *ex post* retention of information obtained through the government’s border searches—otherwise, there is a significant risk that the government will abuse its border search authority to gather information on private individuals, without the traditional constraints imposed by the Fourth Amendment, and then store that

information indefinitely. The government has thus far not identified any interest in retaining Plaintiff's information in its files, beyond its own bureaucratic interest in records maintenance. As discussed above, *supra* Section II, that interest is insufficient to justify the serious and ongoing invasion of Plaintiff's privacy. *See Sovereign News Co.*, 690 F.2d at 578; *Schnitzer*, 567 F.2d at 539; *Lake*, 723 F. Supp. at 834–35. The equities thus tilt sharply in favor of expungement of all government records derived from Plaintiff's electronic devices.<sup>7</sup>

---

<sup>7</sup> Plaintiff also argues, for purposes of preservation, that his information should be expunged because it was collected in violation of his First and Fourth Amendment rights. *See Tabbaa v. Chertoff*, 509 F.3d 89, 96 n.2 (2d Cir. 2007) (plaintiffs had Article III standing to seek expungement of information obtained pursuant to an allegedly illegal search and detention); *Doe v. U.S. Air Force*, 812 F.2d 738, 740–41 (D.C. Cir. 1987) (holding that a plaintiff may be entitled to expungement of government records derived from an unconstitutional search).

## CONCLUSION

For the foregoing reasons, the Court should order the government to: (1) provide a full accounting of files in its possession that were either copied or derived from plaintiff's electronic devices; and (2) certify that it has destroyed each such file or record in its possession.

Respectfully submitted,

/s/ Brian M. Hauss

Brian M. Hauss  
Catherine Crump  
Hina Shamsi  
American Civil Liberties Union  
Foundation  
125 Broad St., 18th Floor  
New York, NY 10004  
Phone: (212) 549-2500  
Fax: (212) 549-2583  
Email: bhauss@aclu.org

Mason C. Clutter  
National Association of Criminal  
Defense Lawyers  
1660 L Street, N.W., 12th Floor  
Washington, D.C. 20036  
(202) 465-7658

Christopher Dunn  
Arthur Eisenberg  
New York Civil Liberties Union  
Foundation  
125 Broad St., 19th Floor  
New York, NY 10004  
(212) 607-3300