UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

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

SUPPLEMENTAL MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL RECONSIDERATION

Plaintiffs respectfully submit this supplemental memorandum supporting reconsideration, because this Court's December 31, 2013, Memorandum and Order—holding that searches of electronic devices at the border are nothing more than routine border searches—conflicts with the Supreme Court's recent decision in *Riley v. California*, Nos. 13-132, 13-212, 2014 WL 2864483 (June 25, 2014), and the Second Circuit's recent decision in *United States v. Ganias*, No. 12-240-cr, 2014 WL 2722618 (2d Cir. June 17, 2014). In these opinions, both courts unanimously recognized that government searches of data stored on personal electronic devices are highly intrusive and merit careful Fourth Amendment scrutiny. In addition, *Ganias* supports Plaintiffs' request for expungement, because it affirms that the Fourth Amendment prohibits the government from retaining an individual's private data for a prolonged period of time in the mere hope that the information will someday prove useful.

Shortly after this Court issued its memorandum opinion and order dismissing Plaintiffs' claims on both justiciability and merits grounds, Plaintiffs submitted a Motion

for Partial Reconsideration, ECF No. 38. In their supporting memorandum, Plaintiffs argued that the Court should reconsider its dismissal of Plaintiff Abidor's claims for lack of standing. Mem. in Supp. of Pls.' Mot. for Partial Recons., ECF No. 38-1. Defendants argued that reconsideration is inappropriate here because revision of this Court's standing decision would not affect the ultimate disposition of the case, given the Court's alternative dismissal of Plaintiffs' claims on the merits. Opp. to Mot. for Recons. at 6–7. The Court subsequently construed Plaintiffs' Motion for Partial Reconsideration as a motion, in the alternative, for relief pursuant to Federal Rule of Criminal Procedure 41(g). Order, Mar. 26, 2014. The *Riley* and *Ganias* decisions, however, now underscore the need for reconsideration in this case. These precedents demonstrate that the Court's initial December 31, 2013, Memorandum and Order critically undervalued the significant privacy intrusion occasioned by Defendants' search of Plaintiff Abidor's private electronic devices. Reconsideration thus provides the Court a valuable opportunity to bring this case into line with intervening appellate jurisprudence regarding the search and seizure of data stored on electronic devices.[1]

[1] Although Plaintiffs' Motion for Partial Reconsideration focused on this Court's standing determination, that fact does not limit the court's ability to address new issues raised while the motion for reconsideration remains pending. "[A] judge may enlarge the issues to be considered in acting on a timely motion under Rule 59." *E.E.O.C. v. United Ass'n of Journeymen and Apprentices of the Plumbing & Pipefitting Industry of the U.S. and Canada, Local No. 120*, 235 F.3d 244, 250 (6th Cir. 2000) (quoting *Charles v. Daley*, 799 F.2d 343, 347 (7th Cir. 1986) (Easterbrook, J.)) (internal quotation marks omitted); *see also, e.g.*, *United States v. Hollis*, 424 F.2d 188, 191 (4th Cir. 1970); 11 Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 2817 n.20 (2014). Alternatively, Plaintiffs ask this Court to construe this memorandum as a request to amend their initial Motion for Partial Reconsideration, *see, e.g.*, *Marsh v. Dep't of Children & Families*, 259 F. App'x 201, 204 (11th Cir. 2007), or as a Rule 60(b) motion for relief from judgment, *see, e.g.*, *Thompson v. Cnty. Of Franklin*, 127 F. Supp. 2d 145, 159–63 (N.D.N.Y. 2000).

1. Riley v. California

First, the Supreme Court's unanimous decision in *Riley v. California* firmly establishes that personal electronic devices, particularly the voluminous amounts of personal data stored on those devices, deserve greater Fourth Amendment protection than other personal possessions. In *Riley*, the Supreme Court held that even though arrestees have a reduced expectation of privacy upon being taken into police custody, the police must as a general matter obtain a warrant to search the data stored on a cell phone; they cannot do so under the search incident to arrest exception. *Riley*, 2014 WL 2864483, at *20. In reaching this conclusion, the Court reasoned that a search of the contents of a cell phone in a pocket is not the same as a search of the contents of a pocket because of the quality and quantity of information carried in electronic devices. *See id.* at *13 ("The United States asserts that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." (citation omitted)).

In explaining why the data on cell phones merit greater constitutional solicitude than other personal possessions, the Court began by pointing out that electronic devices differ from physical objects in terms of their "immense storage capacity," which allows them to store and transport "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* at *14. Moreover, personal electronic devices "collect[] in one place many distinct types of information—an address, a note, a prescription, a bank statement, a

video—that reveal much more in combination than any isolated record." *Id*. And although "people did not typically carry a cache of sensitive personal information with them as they went about their day" in the pre-digital age, cell phones and other personal electronic devices "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at *9, *15.

The Court also identified several qualitative differences between the digital information stored on personal electronic devices and other physical objects people might carry. "A phone not only contains in digital form many sensitive records previously found in the home, it also contains a broad array of private information never found in a home in any form," such as Internet search and browsing history and location information. *Id.* at *16. The Court further explained that the physical container analogy put forth by the government to justify its search of data stored on an electronic device "crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen," a problem exacerbated by the fact that "[c]ell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference." *Id.*[2] In short, "[m]odern cell phones are not just another technological convenience," but "hold for many Americans 'the privacies of life.'" *Id.* at *20 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). The Court accordingly recognized that these privacies demand special Fourth Amendment protection, even in the context of a search incident to arrest. "The fact that technology

[2] In response to the government's contention that it could resolve the knotty Fourth Amendment problems raised by cloud computing through self-governing agency protocols, the Court observed that "the Founders did not fight a revolution to gain the right to government agency protocols." *Id.* at *16.

now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.*

The Supreme Court's rationale for refusing to apply the search incident to arrest exception to data stored on cell phones strongly counsels against reflexive application of the border search doctrine to the search of Plaintiff Abidor's personal electronic devices.[3] As the Second Circuit has held, in deciding whether a border search is "non-routine," and therefore requires reasonable suspicion, "[t]he determining factor is . . . 'the level of intrusion into a person's privacy.'" *Tabbaa v. Chertoff*, 509 F.3d 89, 98 (2d Cir. 2007) (quoting *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006)); *see also United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985) (holding that non-routine border searches require at least reasonable suspicion). Here, Plaintiffs have consistently argued that the search of data stored on an electronic device is highly intrusive and should therefore be classified as non-routine. Pls.' Mem. of Law in Opp. to Defs.' Mot. to Dismiss 19–23, ECF No. 17; *see also United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc) (holding that the forensic border search of the data stored on electronic devices requires reasonable suspicion, because of the highly intrusive nature of such searches).

This Court rejected those arguments in its December 31, 2013, Memorandum and Order. Relying heavily on the district court's opinion in *United States v. Irving*, No. S3 03 CR.0633, 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003), which analogized searches of data stored on personal electronic devices to the paradigmatically routine

[3] Like the plaintiffs in *Riley*, Plaintiff Abidor alleges a Fourth Amendment violation stemming from the government's search of his cell phones. Compl. ¶¶ 44, 130. Moreover, the privacy concerns raised in *Riley* apply with even more force to government searches of laptops, which often contain even more private information than cell phones.

search of luggage or other closed physical container, this Court held that the Fourth Amendment does not require any articulable suspicion for the border search of data stored on electronic devices. Mem. & Order 28–31, ECF No. 36. In so holding, this Court suggested that the intrusiveness of the search was mitigated by the fact that travelers interested in ensuring the privacy of their personal information could limit the information they take with them on their electronic devices. *Id.* at 28.

Riley casts considerable doubt on this rationale. As described above, the Supreme Court has made clear that searches of the data stored on electronic devices cannot be analogized to the search of a piece of luggage or other physical object. Both the amount and nature of personal information stored on laptops, cell phones, and other electronic devices renders them categorically distinct from ordinary physical containers. Moreover, *Riley* recognized that individuals cannot reasonably protect their privacy by limiting the amount of data stored on their personal electronic devices, both because such devices have become so pervasive in modern life that it is effectively impossible to function without them and because individual users are not likely to know how much or what kind of personal information is actually stored on their device or in cloud services accessible from their device. *Riley*, 2014 WL 2864483 at *15–*16. As the Supreme Court observed, the widespread use of personal electronic devices enables (and in many cases, requires) us to take our homes with us wherever we go. *Id.* at *16. It simply cannot be the case that our society's reliance on modern technology gives the government carte blanche to search our digital homes, and more, as a routine matter every time we cross the border. *Riley* thus strongly suggests that the border search of data stored on electronic devices is non-routine and requires at least reasonable suspicion.

2. United States v. Ganias

The Second Circuit's recent decision in *United States v. Ganias*, 2014 WL 2722618, also supports reconsideration and, in the alternative, expungement. In *Ganias*, a Second Circuit panel unanimously held that the government's prolonged retention of non-responsive files obtained from a defendant's personal computer pursuant to a search warrant violates the Fourth Amendment.[4] The government first obtained the information at issue in *Ganias* in 2003, when government investigators obtained a search warrant to search the offices of Ganias's accounting business for evidence relating to an ongoing fraud investigation. *Id.* at *1. Instead of seizing Ganias's computers, government computer specialists made forensic mirror images of the devices' hard drives. *Id.* A little over a year later, government investigators isolated and extracted the computer files relevant to the search warrant, but decided to keep the full images made of Ganias's computers, because they believed the information was government property. *Id.* at *2. When government agents later realized that Ganias's computer files might also contain evidence of tax evasion, they obtained a second warrant and searched the DVDs in 2006—more than two years after the files were initially obtained. *Id.* at *2–*3. The district court denied Ganias's motion to suppress this evidence at his criminal trial. *Id.* at *3.

Reversing, the Second Circuit held that the government's prolonged retention of Ganias's unresponsive computer files was an unreasonable seizure under the Fourth Amendment. *Id.* at *12. Like the Supreme Court in *Riley*, the court of appeals observed

[4] Judge Hall concurred with the Court's Fourth Amendment ruling, but disagreed that the government acted in bad faith. *Id.* at *13–*14 (Hall, J., concurring in part and dissenting in part).

that "computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle," and should therefore be accorded at least as much—if not more—constitutional protection as 18th century "papers." *Id.* at *7. Applying this observation to the case at hand, the court reasoned that although the government had authority under the initial warrant to create the mirror image of Ganias's devices for off-site review and segregation of relevant material, extending that authority to all government retention of "all the data on Ganias's computers on the off-chance the information would become relevant to a subsequent criminal investigation . . . would be the equivalent of a general warrant." *Id.* at *10. Because the government had already identified and segregated the relevant material by December 2004, the court held, its continued retention of non-responsive material for another year-and-a-half, "[w]ithout some independent basis for its retention of those documents in the interim . . . clearly violated Ganias's Fourth Amendment rights," by unreasonably interfering with his possessory interest in his private information. *Id*.

Similarly here, the government's indefinite retention of Plaintiff Abidor's private information, long after the initial border-search justification for obtaining that information has evaporated, renders the seizure of his private information unreasonable under the Fourth Amendment. Indeed, in this case, the government has already retained Plaintiff's information for more than three years and proposes to continue holding onto it indefinitely, despite disclaiming any specific law enforcement or border security interest in the information at issue.[5] Moreover, the initial seizure of Plaintiff's private information

[5] Although Defendants contend in their most recent filing that Plaintiff's private information is not broadly available on government databases, *see* Defs.' Reply to Pls.' Supplemental Mem. Supp. Expungement of Government Records 5, ECF No. 61, they

was conducted without the ordinary Fourth Amendment safeguards—a finding of probable cause by a neutral and detached magistrate—that were present in *Ganias*. To be sure, the information now at issue here is contained in derivative government records, rather than exact copies of Plaintiff's files; however, that formal distinction does not alter the significant intrusion on Plaintiff's privacy interest in his personal information or his interest in excluding others from accessing that information. Thus, even if this Court concludes that Defendants' initial search and seizure of the data stored on Plaintiff's personal electronic devices passes constitutional muster, their continued retention of that information years after the fact—and in the absence of any articulable border security or law enforcement interest—violates the Fourth Amendment.

---

have yet to provide any significant description of the number and kind of agency personnel who have or may obtain access to the records at issue here.

CONCLUSION

For the foregoing reasons, and for the reasons detailed in Plaintiffs' initial Memorandum Supporting Partial Reconsideration, ECF No. 38, this Court should reconsider its December 31, 2013, opinion dismissing Plaintiff Abidor's claims on both justiciability and merits grounds.

Respectfully submitted,

/s/ Brian M. Hauss
Brian M. Hauss
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

Catherine Crump
University of California, Berkeley
433 Boalt Hall, North Addition
Berkeley, CA 94270
Phone: (510) 292-6860
Email: ccrump@law.berkeley.edu

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

cc: Counsel of Record (via ECF)