Vol. 108
Northwestern University Law Review

ABIDOR V. NAPOLITANO: SUSPICIONLESS CELL PHONE AND LAPTOP "STRIP" SEARCHES AT THE BORDER COMPROMISE THE FOURTH AND FIRST AMENDMENTS

Charles E. MacLean & Adam Lamparello[*]

INTRODUCTION

> The point is technology matters.
>
> . . .
>
> . . . [T]he exposure of confidential and personal information [effected by a laptop or cell phone forensic search at the border] has permanence. It cannot be undone. Accordingly, the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property.
>
> [In this case, a]fter their initial search at the border, customs agents made copies of the hard drives and performed forensic evaluations of the computers that took days to turn up contraband. It was essentially a computer strip search.[1]

In *United States v. Cotterman*, the Ninth Circuit issued a landmark ruling, holding that border agents must have reasonable suspicion before executing a forensic search of electronic devices seized from individuals crossing the border.[2] Unfortunately, the Ninth Circuit's opinion is the exception, not the rule. The vast majority of cases require virtually no suspicion before border agents can search laptops or other electronic devices. Given that individuals now store highly personal information on these devices, the threat to privacy is substantial.

---

[*] Charles E. MacLean is an Assistant Professor of Law, Indiana Tech Law School; B.A., M.B.A. (University of Minnesota); J.D., cum laude (William Mitchell College of Law). Adam Lamparello is an Assistant Professor of Law, Indiana Tech Law School; B.A., magna cum laude (University of Southern California); J.D., with honors (Ohio State University College of Law); LL.M. (New York University School of Law). The authors wish to thank Jon Olinger, J.D. candidate 2016, for his research assistance, and dedicate this Article to the memory of Judi L. Vaught.

[1] United States v. Cotterman, 709 F.3d 952, 965–66 (9th Cir. 2013) (en banc), *cert. denied*, 134 S. Ct. 899 (2014). *See generally* Recent Cases, *Constitutional Law—Fourth Amendment—Ninth Circuit Holds Forensic Search of Laptop Seized at Border Requires Showing of Reasonable Suspicion.*—United States v. Cotterman, *709 F.3d 952 (9th Cir. 2013) (en banc)*, 127 HARV. L. REV. 1041 (2014).

[2] *Cotterman*, 709 F.3d at 962–68.

Technology has outpaced the law, and the United States Supreme Court needs to do something about it—now. Every day at the border, the privacy rights of individuals are being infringed, and the Fourth Amendment's particularity requirement and the First Amendment's free speech guarantee are being violated.[3] Yet the justification for these infringements bears no relation to the outdated "border exception"[4] or the government's interest in security. Without even so much as a hunch, border security personnel can confiscate an individual's laptop for days, force the owner to disclose its password, and conduct an unlimited search of (or even copy) the contents for later investigation. The Department of Homeland Security has not acknowledged that border security officials may search for contraband well beyond that which poses an immediate threat to border security. They can fish for evidence of any criminal activity—related or unrelated to border security—without a scintilla of suspicion that any crime has been committed.[5]

This bears no relation to the reasons that initially justified a "Constitution-free" zone 100 miles inland from the border,[6] such as locating dangerous weapons or illicit drugs, and it implicates some of our most cherished freedoms—privacy and free expression. These suspicionless searches violate the Fourth Amendment's reasonableness and particularity requirements and threaten to chill political speech that is neither criminal nor suspicious. A laptop is a virtual office with the capacity to store thousands of files, troves of entertainment, and scores of intimate photos. If border officials could look in any "room" they pleased, people might think twice before storing personal documents that would be embarrassing if viewed by an unknown border agent or, perhaps more concretely, storing a video critical of the President or of someone burning the American flag.

The law is often unable to keep pace with the technological advancements law enforcement uses to conduct more intrusive and, often, suspicionless searches. The protection of an individual's constitutional rights, particularly privacy, can no longer wait for lawsuits to meander their

---

[3] *See* Susan Stellin, *Border Agents' Power to Search Devices is Facing Increasing Challenges in Court*, N.Y. TIMES, Dec. 3, 2012, at B1, *available at* http://www.nytimes.com/2012/12/04/business/court-cases-challenge-border-searches-of-laptops-and-phones.html ("[A]bout 36,000 people are referred to secondary screening by United States Customs and Border Protection daily, and roughly a dozen of those travelers are subject to a search of their electronic devices."). Between October 1, 2008 and June 2, 2010, Customs and Border Protection border agents searched the electronic devices of 6671 travelers, nearly half of which were American citizens. *Government Data Regarding Electronic Device Searches*, ACLU (Aug. 19, 2010), https://www.aclu.org/national-security/government-data-regarding-electronic-device-searches.

[4] *See* United States v. Ramsey, 431 U.S. 606 (1977).

[5] *See* Editorial, *Congress Must Act to End Electronic Fishing Expeditions at the Border*, L.A. TIMES (Sept. 13, 2010), http://articles.latimes.com/2010/sep/13/opinion/la-ed-laptops-20100913.

[6] *See Fact Sheet on U.S. "Constitution Free Zone,"* ACLU (Oct. 22, 2008), https://www.aclu.org/technology-and-liberty/fact-sheet-us-constitution-free-zone.

way through the lengthy—and often costly—litigation process. Lest there be any doubt about the sweeping authority of border agents currently, decades ago, the Court upheld the constitutionality of suspicionless border searches based on doubts that "any other canvassing technique would achieve acceptable results," and because there is a "relatively limited invasion of . . . privacy."[7]

But there is a fundamental difference between the physical and virtual worlds, between searches of containers and laptops, and between present and future threats. In *Abidor v. Napolitano*, the court failed to recognize this fact and instead applied an outdated solution to a new—and unforeseen—problem.[8] The Supreme Court must intervene, as it did recently in *People v. Riley*, and begin the process of restoring the balance between liberty and security. In *Riley*, the defendant was arrested after a traffic stop revealed a suspended license and two guns in the engine compartment.[9] Without a warrant or probable cause, law enforcement searched the contents of the defendant's cell phone and found various incriminating photographs and video clips that were later used at trial on different charges relating to a prior gunfight with rival gang members.[10] The California Court of Appeals held that the officers' conduct was justified by the inventory search doctrine,[11] even though that doctrine is intended to protect the owner's property, protect police from claims of stolen or lost property, or protect police from danger,[12] none of which were served by searching the cell phone's contents. The Supreme Court's decision to grant certiorari may reflect a concern that law enforcement has gone too far and that privacy protections need to be strengthened in light of recent technological advances. We submit that they do.

The solution, we argue, is that border agents ought not to be permitted to search digital devices absent at least reasonable suspicion.[13] Since there

---

[7] Camara v. Mun. Court of S.F., 387 U.S. 523, 537 (1967).

[8] Abidor v. Napolitano, No. 10–CV–04059 (ERK)(JMA), 2013 WL 6912654, at *17 (E.D.N.Y. Dec. 31, 2013) (comparing laptops to other "closed containers," such as luggage, disposable cameras, and 3.5" floppy disks). We note that the storage capability of a typical laptop computer far exceeds that of luggage, a disposable film camera, or floppy disks.

[9] People v. Riley, No. D059840, 2013 WL 475242, at *1–2 (Cal. Ct. App. Feb. 8, 2013) (unpublished table decision), *cert. granted in part*, 134 S. Ct. 999 (2014).

[10] *Id.* at *3, *6.

[11] *Id.* at *5–6.

[12] South Dakota v. Opperman, 428 U.S. 364, 369 (1976).

[13] It should be noted that, although the court in *Abidor* did not rule on whether reasonable suspicion is necessary for a border search of digital devices, the court nonetheless found that even if reasonable suspicion were required, the agents had adequate reasonable suspicion to search Abidor's digital equipment. 2013 WL 6912654, at *18–19. The court found adequate reasonable suspicion where Abidor (1) possessed computer images of designated terror groups, Hamas and Hezbollah, engaged in rallies, although Abidor explained to the agents that he was a Ph.D. student focused on the modern history of Shi'ites in Lebanon, and (2) possessed two passports, United States and French, although that, in itself, is, of course, legal. *Id.*

is, at present, a circuit split on the matter,[14] the time is ripe for the Supreme Court to resolve the dispute, but it missed that opportunity when it denied certiorari in *Cotterman* in early 2014.[15] Importantly, however, *Abidor* presents another opportunity. In *Abidor*, the Eastern District of New York recognized the majority rule that border agents need not have reasonable suspicion before conducting forensic searches of a laptop computer.[16] *Abidor* is significant because the court acknowledged in its holding that, "if suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required."[17] Nevertheless, the Court refused to impose this standard "because the extremely limited resources available to conduct comprehensive forensic searches necessarily limits such searches to situations where some level of suspicion is present."[18] We believe that courts should not wait until it has "become the norm," particularly where, as the court acknowledged in *Abidor*, these searches intruded upon privacy rights.[19] Instead, the courts should act before, not after, the harm is done. If they do not act, Congress should step in to enact legislation requiring reasonable suspicion for border searches of digital devices. The Constitution requires no less.

I. THE TIDE IS BEGINNING TO SHIFT AMIDST A RECOGNITION THAT LAPTOP SEARCHES AT THE BORDER INFRINGE ON FOURTH AMENDMENT RIGHTS

Laptops, like cell phones, are the modern repositories for the "papers" and "effects" traditionally protected by the Fourth Amendment.[20] The information contained in a hard drive therefore carries with it a subjectively and objectively reasonable expectation of privacy.

In the technology era, these rights are under attack. As the recent National Security Agency (NSA) scandal demonstrates, the government has gone to substantial, and insufficiently checked, lengths to compromise private information. The pendulum, however, is beginning to swing back. As President Obama noted in his final press conference of 2013, "[I]n a virtual world, some of these boundaries don't matter anymore. And just

[14] Two circuits have held that border searches of digital devices require no showing of suspicion. United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007); United States v. Ickes, 393 F.3d 501, 506–07 (4th Cir. 2005). The Ninth Circuit has held reasonable suspicion is required. United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (en banc), *cert. denied*, 134 S. Ct. 899 (2014).

[15] Cotterman v. United States, 134 S. Ct. 899 (2014).

[16] *Abidor*, 2013 WL 6912654 at *18.

[17] *Id.*

[18] *Id.*

[19] *Id.* at *16.

[20] *See* U.S. CONST. amend. IV.

because we can do something doesn't mean we necessarily should . . . ."[21] The President was reacting to the forty-six NSA surveillance reform recommendations his own five-expert panel had released just eight days before, on December 12, 2013.[22]

Although the NSA programs at issue in the President's press conference involved global and domestic telephone metadata collection, presumably for later investigation,[23] it has relevance in the border search context. Pursuant to agency policies, border agents can seize and search the contents of the cell phones, laptops, and other digital devices as their possessors cross into the United States. Although some commentators and courts differentiate between so-called "quick look" and deeper "forensic" digital border searches, the authors maintain that both types violate the First and Fourth Amendments, therefore making it a distinction without a constitutional difference. To be sure, the issue is one of degree, not kind. While a quick look is obviously not as intrusive as a forensic search, it can nonetheless uncover highly personal information that an individual has a right to keep private. One commentator states:

> An officer searching a cell phone can at least initially do so fairly easily, by "just 'thumbing through' the cell phone." As Professor Gershowitz has written, searches of pagers and early generation cell phones "do not require in-depth searching to obtain evidence. Police need to push only a limited number of buttons in order to reach pager numbers and only a few additional buttons to retrieve text messages."[24]

Thus, both quick look and forensic searches "create 'a serious and recurring threat to the privacy of countless individuals.'"[25]

---

[21] *Full Transcript: President Obama's December 20 News Conference*, WASH. POST (Dec. 20, 2013), http://www.washingtonpost.com/politics/running-transcript-president-obamas-december-20-news-conference/2013/12/20/1e4b82e2-69a6-11e3-8b5b-a77187b716a3_story.html.

[22] PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[23] The NSA large-scale interception and storage of telephone metadata has been the subject of varied assessments in the federal district courts that have examined the programs to date. *Compare* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013) (enjoining the NSA from further metadata seizures, stayed pending appeal, and finding that the seizures were Fourth Amendment searches), *with* ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (finding NSA's telephone metadata collection program constitutional).

[24] Margaret M. Lawton, *Warrantless Searches and Smartphones: Privacy in the Palm of Your Hand?*, 16 UDC/DCSL L. REV. 89, 101 (2012) (footnotes omitted) (quoting Ashley B. Snyder, Note, *The Fourth Amendment and Warrantless Cell Phone Searches: When is Your Cell Phone Protected?*, 46 WAKE FOREST L. REV. 155, 163 (2011); Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 41 (2008)).

[25] United States v. Wurie, 728 F.3d 1, 14 (1st Cir. 2013) (quoting Arizona v. Gant, 129 S. Ct. 1710, 1720 (2009)).

A. The Facts in Abidor

In *Abidor*, the United States District Court for the Eastern District of New York upheld the constitutionality of laptop border searches.[26] Despite the First and Fourth Amendments, the court held that border agents need not meet any particular standard before they search any closed container (including laptops, cell phones, external hard drives, and similar digital devices).[27] The court quoted *Cotterman* to acknowledge that an "exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border."[28] It also used *Cotterman* to diminish these interests, stating that "the Ninth Circuit acknowledged that its opinion would not have any practical effect . . . because the extremely limited resources available to conduct comprehensive forensic searches necessarily limits such searches to situations where some level of suspicion is present."[29] The *Abidor* court did recognize, however, that if these searches were to "become the norm," reasonable suspicion would be required.[30] In our view, the court erred by taking a wait-and-see approach, rather than saying now what courts will almost certainly say later: suspicionless searches are unconstitutional. To make matters worse, the court rested its decision on the long history of suspicionless border searches held to be constitutional as necessary to protect the sovereign from dangerous material entering its territory.[31] As discussed below, these decisions do not justify the suspicionless search of a laptop.

The *Abidor* case involved border agents that seized numerous digital devices from a graduate student crossing a United States border and searched the student's cell phones for up to five hours but did not return the student's laptop and external hard drive until eleven days later.[32] In doing so, the agents followed, in broad brush, the guidelines of United States Customs and Border Protection (CBP) promulgated in 2008[33] and 2009,[34] as justified and explained in a 2011 Department of Homeland Security

---

[26] Abidor v. Napolitano, No. 10–CV–04059 (ERK)(JMA), 2013 WL 6912654, at *18 (E.D.N.Y. Dec. 31, 2013).

[27] *Id.*

[28] *Id.* at *17 (quoting United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (en banc), *cert. denied*, 134 S. Ct. 899 (2014)).

[29] *Id.* at *18.

[30] *Id.*

[31] *Id.* at *14–17.

[32] *Id.* at *5.

[33] U.S. CUSTOMS & BORDER PROT., POLICY REGARDING BORDER SEARCH OF INFORMATION. (2008), *available at* http://www.cbp.gov/sites/default/files/documents/search_authority_2.pdf.

[34] Memorandum from U.S. Customs & Border Prot. outlining CBP Directive No. 3340–049 (Aug. 20, 2009), *available at* http://www.cbp.gov/sites/default/files/documents/elec_mbsa_3.pdf.

report.[35] The report states that "overall authority to conduct border searches without suspicion or warrant is clear and long-standing, and courts have not treated searches of electronic devices any differently than searches of other objects."[36]

Abidor's complaint alleged that the agents searched numerous files on Abidor's laptop that contained "highly private and expressive materials [revealing] intimate details" about the student's life.[37] The district court upheld this extended search of the student's laptop and hard drive because (1) border searches have historically been granted considerable leeway for sovereign protection, and (2) cost and manpower concerns make it impossible for federal border agents to conduct suspicionless searches of all cellphones and laptops, so there was no need to set a specific standard, including that of reasonable suspicion, for agents to meet to justify such a search.[38] Most importantly, the court's decisions devalued Abidor's privacy interest, even while recognizing later in its opinion that, should these searches become more widespread, they would require reasonable suspicion. For example, quoting Professor Wayne LaFave, the court stated that because "the individual crossing a border is on notice that certain types of searches are likely to be made, his privacy is less invaded by those searches."[39] As a result, "[t]he individual traveler determines the time and place of the search by his own actions, and he thus has ample opportunity to diminish the impact of that search by limiting the nature and character of the effects which he brings with him."[40]

In reaching its decision, the court cited many of the leading cases from the largely pre-digital age.[41] After noting that the inquiry balances the government's interest against the intrusion into the subject's Fourth Amendment rights, the court found, "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the

---

[35] U.S. DEP'T OF HOMELAND SEC., CIVIL RIGHTS/CIVIL LIBERTIES IMPACT ASSESSMENT: BORDER SEARCHES OF ELECTRONIC DEVICES (2011), *available at* https://www.dhs.gov/sites/default/files/publications/Redacted%20Report.pdf. Most of the report's Fourth and First Amendment analysis was redacted upon publication. *Id*. at 10–18.

[36] *Id.* at 15.

[37] Abidor v. Napolitano, 2013 WL 6912654, at *6 (quoting Complaint at ¶ 51, *Abidor*, 2013 WL 6912654 (No. 10–CV–04059 (ERK)(JMA))).

[38] *Id.* at *14–16, *18–19.

[39] *Id.* at *16 (quoting WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE OF THE FOURTH AMENDMENT § 10.5(a) (4th ed. 2011–12)).

[40] *Id.* at *16 (alteration in original) (quoting LAFAVE, *supra* note 39, § 10.5(a)).

[41] *See id.* at *15 (quoting Carroll v. United States, 267 U.S. 132, 154 (1925) ("Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in and his belongings as effects which may be lawfully brought in."); Camara v. Municipal Court, 387 U.S. 523, 537 (1967) (discussing administrative searches generally, the Supreme Court held that "because the inspections are neither personal in nature nor aimed at the discovery of evidence of crime, they involve a relatively limited invasion of . . . privacy").

international border."[42] In *Flores-Montano*, border agents discovered illegal drugs after removing and disassembling the defendant's gas tank.[43] The Court's decision was based on the long-standing recognition "that automobiles seeking entry into this country may be searched."[44]

Indeed, as the Court correctly held, "[i]t is difficult to imagine how the search of a gas tank, which should be solely a repository for fuel, could be more of an invasion of privacy than the search of the automobile's passenger compartment."[45]The same cannot be said for the search of a laptop, which, like modern-day cell phones, "can also contain address books, calendars, voice and text messages, email, video and pictures."[46] Also, unlike a gas tank, the intrusion upon privacy in the context of laptop searches is far-reaching and potentially unlimited.

The *Abidor* court declined to highlight these differences. While it briefly touched on the "significant invasion of privacy" occasioned by a forensic laptop search, the court suggested that "the sensible advice to all travelers is to '[t]hink twice about the information you carry on your laptop,' and to ask themselves: 'Is it really necessary to have so much information accessible to you on your computer?'"[47] This advice just front-loads each border-crosser's loss of constitutional protection; rather than being subjected to a laptop search at the border, the court recommends that it is somehow preferable for the traveler's speech to be chilled by leaving the laptop at home. Constitutional rights should not be so flimsy, particularly in the context of laptop border searches, where the traditional justifications for border searches—safety and discovery of contraband—do not apply. As discussed below, laptops cannot hide or be used as weapons, and they cannot store physical objects.

Ironically, the *Abidor* court recognized this fact, by holding that, "if suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required."[48] The Fourth Amendment does not, however, require a set number of harms before it springs into action. One violation is too many. Constitutional rights are intended to chill the arbitrary exercise of government power, not the individual's right to privacy—or free speech.

---

[42] *Abidor*, 2013 WL 6912654, at *14 (quoting United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004)).

[43] 541 U.S. at 151.

[44] *Id.* at 154.

[45] *Id.*

[46] United States v. Park, No. CR 05–375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007).

[47] *Abidor*, 2013 WL 6912654, at *16 (quoting PONEMON INST. LLC, AIRPORT INSECURITY: THE CASE OF MISSING & LOST LAPTOPS 8 (2008), *available at* http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf.

[48] *Id.* at *18.

As *Abidor* revealed, these threats are real. The other plaintiffs in Abidor were the National Association of Criminal Defense Lawyers (NACDL) and the National Press Photographers Association (NPPA). These associations argued that their members were likely to be adversely affected by suspicionless digital border searches. The NACDL, for example, "allege[d] that many of its members—criminal defense attorneys resident throughout the country—routinely travel abroad for professional purposes and bring with them electronic devices containing personal, confidential, or privileged information."[49] Thus, the suspicionless search of their laptops "interfere[s] with its members' ability to represent clients because they must 'take seriously the risk that the content of their electronic devices could be reviewed, copied, and detained.'"[50] These allegations suggest that the *Abidor* court's "sensible advice" to "[t]hink twice about the information you carry on your laptop," is neither sensible nor realistic.[51] The pre-digital case law is inapplicable and harmful.

B. Fourth Amendment Implications Highlighted By Abidor

Unfortunately, *Abidor* is symptomatic of the difficulties courts face when trying to force-fit today's digital age realities into old, longstanding, and virtually unchallenged doctrine from the pre-digital era. Those border search precedents permitted suspicionless searches to allow the border agents to search for and seize dangerous things, such as guns and illegal drugs. When the court in *Abidor* permitted the extended search of the student's laptop and other digital equipment without setting a standard of reasonable suspicion, it expanded border agents' authority to search for any evidence of current or potential criminal activity, even if expressed as an idea, belief, or opinion. For example, in *Abidor* the court noted that the border agents' search of Abidor's computer uncovered pictures of Hamas and Hezbollah, "both of which were designated by the State Department as terrorist organizations."[52] Absent any other indicator that Abidor actually had ties to these organizations, the obvious response to that statement should be: so what?

To begin with, the mere possession of images depicting a terrorist organization, be it Hezbollah or Al Capone, is not unlawful. Additionally, the government treads on dangerous ground when it attempts to justify searches based on the mere possession—or presence—of material that does not reliably suggest criminal behavior. In other words, the same problems that racial or ethnic profiling cause also arise here, and the constitutional cost, including infringement on personal privacy and downright

[49] *Id.* at *6.

[50] *Id.* (quoting Complaint at ¶ 77, *Abidor*, 2013 WL 6912654 (No. 10–CV–04059 (ERK)(JMA))).

[51] *Id.* at *16 (internal citations and quotation marks omitted) (quoting PONEMON INST. LLC, *supra* note 47, at 8).

[52] *Id.* at *5.

humiliation, is undeniable. They are problems of interpretation and inference, all of which risk the arbitrary exercise of power. For example, images of an anti-American rally, or a video documenting the bombing of Pan Am Flight 103, do not suggest criminal or even hostile behavior. These items may be part of a research project, a course assignment, or a curious mind. But if discovered during a laptop search at the border, law enforcement has the discretion to interpret them any way they want. And they use other factors, such as the individual's race and ethnicity, to create suspicion and thereby justify a more extensive—and intrusive—search.

Moreover, it makes little sense to argue that Abidor failed to offer a convincing explanation regarding the presence of these materials. He should not have to. The burden is on law enforcement, not individual citizens, to explain their reasons for conducting a search of protected information. Otherwise, it creates a situation where the victim of an invasive search is blamed for the failure to explain innocent conduct in a suspicionless context. Despite these realities, and the damage to Abidor's privacy, the court failed to provide a remedy.

The court's decision highlighted another problem—applying old, pre-digital age case law and theories to today's digital technologies. These older cases are not only factually distinguishable but also rest on now-invalid assumptions. For example, unlike traditional closed containers, laptops cannot hold tangible objects, much less dangerous ones.[53] Also, unlike gas tanks, passenger compartments, or suitcases, laptops cannot hide illegal drugs or other contraband. What they can hold, however, is limitless amounts of personal information that constitute the electronic version of the "papers" and "effects" that the Fourth Amendment protects.[54] And people do, in fact, store this type of information on laptops (and other electronic devices).[55] That is why the reasoning in pre-digital era case law cannot address this problem. Laptops are fundamentally different objects, as to both the contraband they cannot contain (dangerous weapons or illegal drugs), and the scope of information they can contain (private and confidential documents).

Thus, the risk of relying on outdated case law is substantial. Travelers and organizations of all stripes are at risk of extensive border searches of their digital equipment if they travel internationally. Private emails to family members and loved ones may be searched. An individual's Facebook page, Google search history, and record of recent purchases may

---

[53] *See, e.g.*, State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009) (distinguishing cell phones from closed containers, which "have traditionally been physical objects capable of holding other physical objects").

[54] *See* U.S. CONST., amend. IV.

[55] *See* United States v. Park, No. CR 05–375 SI, 2007 WL 1521573, at *9 (N.D. Cal. May 23, 2007) (emphasizing "the quantity and quality of information that can be stored on a cellular phone" as a basis for affording Fourth Amendment protection).

also be subject to examination. Additionally, defense counsels, for example, who bear the extreme burdens of privilege and confidentiality on behalf of their clients, cannot confidently carry their confidential material across a border for fear of interception and search. A reporter cannot really promise confidentiality to a source whose identity, when stored on a laptop or cell phone, can be seized without suspicion upon the reporter's re-entry into the United States. This begs the question—what reason can the government offer to justify these searches? As *Abidor* demonstrates, the government has offered several, but none are convincing.

II. FIRST AMENDMENT IMPLICATIONS OF SUSPICIONLESS DIGITAL SEARCHES AT THE BORDER

Abidor is not just about the Fourth Amendment. Intrusive searches of laptops at the border also threaten to chill constitutionally protected speech. If individuals know that their laptops can be subject to suspicionless searches, then they may hesitate before sending an email, downloading a video, or storing a confidential document. The chilling effect that will likely occur cannot be tolerated in a society that prides itself on a "marketplace of ideas."[56]

Indeed, using outdated case law also implicates First Amendment issues. The First Amendment provides: "Congress shall make no law . . . abridging the freedom of speech . . . ."[57] The Amendment's protections have repeatedly extended to unpopular or offensive speech or other expressive conduct, including profane speech,[58] Nazi speech,[59] obscenity consistent with community standards,[60] and a substantial portion of what some would consider "hate" speech.[61] Much of the contents of one's laptop or cell phone might be offensive to a person or group, be considered profane or obscene to a degree, or give rise to a subjective belief that the mere possession of such material suggests criminal conduct. Some of the contents may be unpopular, "unpatriotic," and even revolting, but they are protected, and not necessarily indicative of criminal intent. Of course, there will be some items, which are traditionally characterized as hate speech, that may suggest criminal activity and therefore justify a laptop

[56] Joseph Blocher, *Institutions in the Marketplace of Ideas*, 57 DUKE L.J. 821, 851 (2008).

[57] U.S. CONST. amend. I.

[58] *See, e.g.*, Cohen v. California, 403 U.S. 15 (1971).

[59] *See, e.g.*, Collin v. Smith, 578 F.2d 1197 (7th Cir. 1978).

[60] *See, e.g.*, Miller v. California, 413 U.S. 15 (1973).

[61] *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377 (1992). "[I]f there is any principle of the Constitution that more imperatively calls for attachment than any other it is the principle of free thought—not free thought for those who agree with us but freedom for the thought that we hate." United States v. Schwimmer, 279 U.S. 644, 654–55 (1929) (Holmes, J., dissenting).

search.[62] But the courts are not justifying these laptop border searches based on speech that is suggestive of criminal activity; they are relying on the rationale of pre-digital case law. As stated above, however, this rationale does not apply in the context of laptop searches.

Ultimately, American citizens—and noncitizens—should not have to fear that they will arouse suspicion when crossing the border simply because their laptop contains a YouTube video depicting an anti-American rally. Indeed, permitting unlimited laptop searches at the border might result in a significant chilling effect on the exercise of First Amendment rights. To be sure, a laptop is not similar to a briefcase, even though both can contain confidential documents. A laptop can store an infinitely larger amount of information, including electronic and social media, and numerous forums through which individuals communicate.[63] Furthermore, unlike briefcases, laptops cannot store weapons. That is why suspicionless laptop border searches present a unique—and acute—threat to First Amendment freedoms.

This possibility also demonstrates the inextricable link between privacy and expression. Though the infringement is not occasioned by disclosure itself, it arises from the resulting chill on political speech that makes people think twice before exercising their constitutional rights, or, as the *Abidor* court said, "[t]hink twice about the information [people] carry on [their] laptop."[64] In *Abidor*, the seized depictions were gatherings of terroristic groups—gatherings one can see depicted on television and Internet news programming, yet the government's search of the laptop, and the court's reliance on images of Hezbollah to support its decision, shows how far we have come from the days when physical safety and the presence of contraband, rather than protected speech, justified these suspicionless border searches.

Searches like the ones in *Abidor* are tantamount to a search for unpopular ideas,[65] and are conducted in a manner that is far more intrusive than the pre-digital creators of the border exception could have contemplated. The border agents are not searching for drugs or guns, or other implements that threaten safety. Instead, they are searching for evidence of lawful activities that might give rise to a suspicion that a further

---

[62] *See, e.g.*, Richard Delgado, *What if* Brown v. Board of Education *was a Hate-Speech Case?*, 1 STAN. J. C.R. & C.L. 271, 281 (2005) (internal footnotes omitted) ("Recent scholarship has cast doubt on the idea that hate speech is essentially innocuous. Books such as Alexander Tsesis's *Destructive Messages* show how a climate of hate speech contributed to practically every mass hate movement in history.").

[63] *See* Jacqueline Kotyk, *What Is a Reasonable Expectation of Privacy in the Information Contained on a Workplace Computer?*, 22 EDUC. & L.J. 223, 226 (2013).

[64] Abidor v. Napolitano, No. 10–CV–04059 (ERK)(JMA), 2013 WL 6912654, at *16 (E.D.N.Y. Dec. 31, 2013) (quoting PONEMON INST. LLC, *supra* note 47, at 8).

[65] *See generally* Erick Lucadamo, Note, *Reading Your Mind at the Border: Searching Memorialized Thoughts and Memories on Your Laptop and* United States v. Arnold, 54 VILL. L. REV. 541 (2009).

and even more intrusive search is necessary. They are searching tax returns, personal correspondence, locational data, browsing history, photographs, and information that has been deleted, though retained in the deep recesses of the device. If the border exception currently makes it permissible for a border agent to retroactively manufacture reasonable suspicion only by first having unlimited authority to search these otherwise legally possessed types of documents and information, then we must seriously rethink the border exception.

In the absence of some standard to first justify the search, such as reasonable suspicion, border agents are conducting nothing other than a digital dragnet. Furthermore, the traditional justifications underlying the border exemption—"national self-protection"[66] and "unwanted . . . effects,"[67]—are outweighed by the substantial and enduring threats to privacy and speech. Also, the possibility of uncovering present criminal activity, e.g., images of child pornography, does not justify intrusions that are based on no suspicion whatsoever. Instead of requiring suspicion to precede the search, border agents now have an unchecked power to search and thereby create suspicion. In many cases, such as *Abidor*, that suspicion or evidence of wrongdoing is at most suggestive of future criminal activity, and that suggestion is itself often based on unreliable assumptions. Videos of anti-American or anti-government demonstrators, for example, are suggestive only insofar as the border agent thinks they are. And that degree of subjectivity does not—and should not—permit either a quick look or forensic search of a laptop.

III. A REASONABLE SUSPICION THRESHOLD STRIKES THE RIGHT BALANCE BETWEEN NATIONAL SECURITY AND INDIVIDUAL PRIVACY

Given the significant infringement on First and Fourth Amendment rights, the government's interests in self-protection and protection of its residents neither justify nor require suspicionless border searches of digital devices. Rather, a reasonable suspicion threshold before permitting a border search of digital devices would adequately protect the sovereign. Reasonable suspicion is a threshold far lower than probable cause, but is vastly superior to no threshold at all. "A reasonable suspicion inquiry simply considers, after taking into account all the facts of a particular case, whether the border official ha[d] a reasonable basis on which to conduct the search."[68] Though this is a relatively modest threshold, it provides an extra layer of protection for travelers' rights by banning digital dragnet searches

[66] *Abidor*, 2013 WL 6912654, at *15 (quoting Carroll v. United States, 267 U.S. 132, 154 (1925)).

[67] *Id.* at *14 (quoting United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004)).

[68] *Id.* at *18 (alteration in original) (quoting United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006)) (internal quotation marks omitted).

at our borders while at the same time protecting legitimate government interests.

Of course, the alternative would be to require probable cause, which would afford those crossing the border the full protection of the Fourth Amendment. This could, however, hinder the government's legitimate interest in interdicting criminal material in laptop memories from entering the country. If border agents, for example, had reasonable suspicion to believe that an individual possessed a computer file depicting a particular plan to attack the White House, but could not conduct a search absent additional proof, it would almost certainly guarantee that these criminal digital materials would, at some point, cross the border. In this way, a probable cause standard would undermine the initial justifications that gave rise to the border exception. A reasonable suspicion standard therefore strikes a better—and more constitutional—balance.

Thus, if a person appears at the border intending to enter the United States and the border agent's screen indicates the person has an ongoing pattern of prior convictions for child pornography, those convictions may, depending on circumstances such as the number, severity, and recentness of prior convictions, permit the border agents to search the person's electronic devices.[69] If a person seeks to enter the United States and border agents discover the person is on a terror watchlist, border agents might also, depending on the circumstances, have sufficient reasonable suspicion to search the person's electronic devices. And where the agents know that an entering person was suspected of ongoing immigration fraud involving the creation of immigration documents on his computer, the agents would certainly have at least reasonable suspicion sufficient to justify the agents' search of the person's computer equipment.[70]

It is not enough, however, to say that the unchecked searches of laptops are acceptable because the border search exception is "as old as the Fourth Amendment itself."[71] Times change, and new circumstances can present threats to constitutional protections that did not exist or were not foreseen. That is precisely the case in the digital age. Border searches of digital devices are not searches for the particular types of illegal objects that

[69] *See, e.g.*, *Irving*, 452 F.3d 110 (ruling that border agents had reasonable suspicion to search computer diskettes in Irving's luggage upon his arrival to the United States from Mexico after the agents were informed Irving had a prior conviction for attempted sexual abuse of a child, and was a target in a federal investigation into persons traveling to Mexico to engage in sexual acts with children); United States v. Bunty, 617 F. Supp. 2d 359 (E.D. Pa. 2008) (noting that upon Bunty's return to the United States from London, border agents had reasonable suspicion to search the computer equipment in Bunty's possession after the agents were informed he had a prior arrest for sexual abuse of a child and a prior guilty plea for corrupting morals of a minor).

[70] *See, e.g.*, United States v. Singh, 295 F. App'x 190 (9th Cir. 2008).

[71] United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005) (quoting United States v. Ramsey, 431 U.S. 606, 619 (1977)).

also are as old as the Fourth Amendment itself. Instead, they are searching for anything at all and that is the problem.

But all is not lost. As the vignettes and actual cases above demonstrate, the sovereign can still protect its interests if it only meets the relatively meager reasonable suspicion threshold. This proposal does not leave sovereigns without border protections, and better honors the Fourth Amendment, the First Amendment, and the people. The proposal leaves in place the traditional border search exception for items other than the contents of digital devices.

IV. IF COURTS CANNOT EFFECTIVELY SERVE AS ARBITERS OF PRIVACY'S CONTOURS IN THE DIGITAL AGE, CONGRESS MUST STEP INTO THAT BREACH

The courts should strengthen privacy protections by providing a fairer—and more just—framework to govern border searches. But courts can only do so much. Legal doctrines such as standing, stare decisis principles, and the slow rate at which litigation progresses impose internal constraints on the Court's power to ensure timely and comprehensive reform.

Indeed, many courts are still wedded to the past. For example, while the court in *Abidor* dismissed the association plaintiffs' complaints on standing grounds, it made clear that, had it reached the merits, it would have ruled that the search was perfectly valid.[72] This suggests that at least some courts are unwilling to meet the new challenges of the digital age.

Standing is also a significant barrier. A plaintiff must have a particular and personal injury—that occurred in the past—to be deemed to have standing sufficient to support a cause of action in court. Second, under the declaratory judgment banner, a plaintiff must be able to proffer a particular case or controversy before a court will take the case. Thus, organizations such as the NACDL and the NSSA will not likely have recourse in court to try to head off future disaster at the pass.

A lack of time and resources also make the courts ill-suited to answer these questions. In fact, the United States Supreme Court hears a fraction (often less than one percent) of the cases petitioned to it for certiorari.[73]

---

[72] *Abidor*, 2013 WL 6912654, at *7–14. Although a discussion of standing is beyond the scope of this Article, it is worth noting that, as standing is applied to exclude more litigants from constitutional discourse, so too will the courts be excluded from efficiently protecting privacy in the digital age. *See generally* Charles E. MacLean, *Katz on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age, Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L.J. SCI. & TECH. (forthcoming 2014).

[73] *See* Kedar S. Bhatia, *Likelihood of a Petition Being Granted*, DAILYWRIT (Jan. 10, 2013), http://dailywrit.com/2013/01/likelihood-of-a-petition-being-granted/ (using Supreme Court data to estimate the certiorari petition granted rate at 0.862% for petitions filed between June 30, 2011, and July 2, 2012). The Court issued formal opinions in fewer than 85 cases per year for each year from 2007-

Also, a case may take years before appellate review occurs, which means that lawyers traveling abroad will continue to face doubt and uncertainty regarding the confidentiality of information stored on laptops. Moreover, courts simply do not have the time or the resources to engage in an extensive policy analysis, or to reflect upon the many issues that are presented in this and other digital contexts. They cannot hold hearings, appoint a task force, or study the substantial amount of empirical research that exists. In other words, courts cannot provide timely—or comprehensive—answers to the complex questions that arise as technology advances at a far more rapid pace.

The solution must come from Congress. Congress and state legislatures need not await particular cases or controversies or be constrained by stare decisis, to create meaningful—and politically viable—solutions (indeed, legislative acts are prospective and contemplate practical solutions to past, current, and future problems). These bodies are not limited to one issue or set of facts at a time, can broadly legislate across whole spheres of activity and, at least when acting functionally, can enact a great deal of legislation during every session.

Thus, it will be Congress's responsibility to carefully consider, reflect upon, and weigh the competing interests in privacy and crime prevention. The outcome should, in our view, result in a modern conception of privacy to match modern technology. Thus, Congress and state legislatures may well be the proper guardians of privacy in the digital age. For example, given the recent fallout from the NSA scandal, Congress can likely muster the votes to enact legislation requiring all future digital searches at the border to be conducted only upon a showing of reasonable suspicion.[74] And the authors call upon Congress to do just that. President Obama's recent measures to curtail NSA spying will hopefully begin a trend that requires the government to answer a few questions before it searches an individual's private text messages or Google search history.

CONCLUSION

National security is an interest of the highest order, but privacy is a constitutional right worthy of unwavering protection. The government's infringements upon privacy extend far beyond the border, to cell phones, for example, where an individual's location can be tracked. Until Congress enacts legislation, or the Supreme Court draws a line, the threats to individual liberty will continue to expand, and citizens will be without

2011. U.S. COURTS, SUPREME COURT OF THE UNITED STATES—CASES ON DOCKET, DISPOSED OF, AND REMAINING ON DOCKET AT CONCLUSION OF OCTOBER TERMS, 2007 THROUGH 2011 (2012), *available at* http://www.uscourts.gov/uscourts/Statistics/JudicialBusiness/2012/appendices/A01Sep12.pdf.

[74] Perhaps Congress could focus its efforts on amending the statute authorizing such border searches, 19 U.S.C. § 1467 (2012), and passing enabling legislation to compel the agency to revise the rule on point, 19 C.F.R. § 162.6 (1972).

recourse. Eventually, the right balance will be struck, but there is no reason why it cannot—and should not—be done now.