Abidor v. Napolitano: Suspicionless Cell Phone and Laptop Searches at the Border Compromise the Fourth and First Amendments

Adam Lamparello, Indiana Tech Law School
Charles MacLean, Indiana Tech Law School
INTRODUCTION

The point is technology matters . . . the 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 the 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.3

Technology has outpaced the law, and the United States Supreme Court needs to do something about it—now. Every day at the border, an individual’s privacy—along with the Fourth’s Amendment’s particularity requirement and the First Amendment’s free speech guarantee—are being infringed. And for reasons having no relation to the outdated “border exception,” or the Government’s interest in security.

To be sure, without even so much as a “hunch,” border security personnel can confiscate an individual’s laptop (sometimes, for days), force the owner to disclose its password, and conduct an unlimited search of (even copy) the contents for later investigation. What the Department of Homeland Security refuses to acknowledge, but which is true nonetheless, is that

1 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). The authors wish to thank Jon Olinger, J.D. candidate 2016, for his research assistance.

2 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).

3 United States v. Cotterman, 709 F.3d 952, (9th Cir. 2013) (en banc) (emphasis added), cert. denied, ___ S. Ct. ___, No. 13-186, 2-14 WL 102985 (Jan. 13, 2014) (the Ninth Circuit, in Cotterman, casting into doubt a long line of cases holding that virtually no showing must be made to render a border search constitutional, held that border agents must have reasonable suspicion before executing a forensic search of electronic devices seized from border crossers); see generally Casenote, Ninth Circuit Holds Forensic Search of Laptop Seized at Border Requires Showing of Reasonable Suspicion – United States v. Cotterman, 127 HARV. L. REV. 1041 (Jan. 2014).
border security officials are not searching for contraband. They are fishing for evidence of any criminal activity—related or unrelated to border security—where there exists not a scintilla of suspicion that any crime has been committed.

This bears no relation to the reasons, e.g., locating dangerous weapons or illicit drugs, that initially justified a “Constitution-free” zone 100 miles inland from the border. And it implicates some of our most cherished freedoms—privacy and free expression. Specifically, such conduct violates the Fourth Amendment’s reasonableness and particularity requirements, and threatens to chill political speech that is neither criminal nor suspicious. Think about it: 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 a video critical of the President or of someone burning the American flag.

Simply stated, the law can no longer keep pace with technological advances. The protection of an individual’s constitutional rights, particularly privacy, can no longer wait for lawsuits to meander their way through the lengthy—and often costly—litigation process. Lest there be any doubt, decades ago, the Court upheld the constitutionality of suspicionless border searches based on doubts that “any other canvassing technique would achieve acceptable results,”\(^4\) and because “there is a relatively limited invasion…of privacy.”\(^5\)

Until a more comprehensive policy is established, one thing should be clear: there is a fundamental difference between the physical and virtual world, between searches of containers and laptops, and between present and future threats. In *Abidor v. Napolitano*,\(^6\) the court failed to


\(^5\) *Id.*

recognize this fact, instead applying an old solution to a new—and unforeseen—problem. The Supreme Court must intervene, as it did recently in Riley v. California, and begin the process of restoring the balance between liberty and security.

I. THE TIDE IS BEGINNING TO SHIFT

As the recent NSA scandal demonstrates, the government has gone to substantial, and unchecked, lengths to compromise private information. The pendulum, however, is beginning to shift. 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 because we can do something doesn't mean we necessarily should.” The President was reacting to the forty-six National Security Agency (“NSA”) surveillance reform recommendations his own five-expert panel had released just eight days before, on December 12, 2013.

Although the NSA programs at issue in the President’s press conference involved global and domestic telephone metadata collection, presumably for later investigation, 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.

---

8 The panel members were Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire.
10 The NSA large-scale interception and storage of telephone metadata have been the subjects of varied assessments in the federal district courts that have examined the programs to date. Compare Klayman v. Obama, ___ F. Supp. 2d ___, No. 13-0851, 2013 WL 6571596 (D. D.C. Dec. 16, 2013) (enjoining the NSA from further metadata seizures, stayed pending appeal, finding that the seizures were Fourth Amendment searches), with ACLU v. Clapper, ___ F. Supp. 2d ___, No. 13 Civ. 3994(WHP), 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013) (finding NSA’s telephony metadata collection program constitutional).
11 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, so that is a distinction without a difference.
In Abidor\textsuperscript{12} the Eastern District of New York upheld the constitutionality of these searches. Despite the First and Fourth Amendments, and Ninth Circuit’s decision in Cotterman, the court held that agents need not meet any particular standard before they search any closed container (including within that category, laptops, cell phones, external hard drives, and similar digital devices) possessed by a border crosser.\textsuperscript{13} 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.\textsuperscript{14}

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 precedent 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, 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.”\textsuperscript{15} 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 suspicionless searches based on the mere possession—or presence—of material that does not reliably suggest criminal behavior. In other words, the same

\textsuperscript{13}Id. at *18.
\textsuperscript{14}Id. at **14-17.
\textsuperscript{15}Abidor, No. 10-CV-04059 at *8.
problems that racial or ethnic profiling cause also arise here, and the constitutional cost, including infringement on personal privacy and downright humiliation, is undeniable. It is, of course, no response to say that Abidor failed to offer a convincing explanation regarding the presence of these materials. The damage to his privacy had already been done. The court in Abidor failed to provide a remedy.

Our Constitution is grounded on protecting different, even dangerous, ideas, thus the border agents ought not be permitted to undertake suspicionless searches of digital devices absent, at least, reasonable suspicion. Since there is, at present, a circuit split on the matter, the time is ripe for the Supreme Court to resolve the dispute. Despite that fact, the Court missed that opportunity when it denied certiorari in Cotterman in early 2014. If the Court will not act, perhaps Congress must step in to enact legislation requiring reasonable suspicion for border searches of digital devices. The Constitution requires no less.

A. THE FACTS IN ABIDOR

In Abidor, border agents 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. In doing so,

---

16 It should be noted that, although the court in Abidor held no reasonable suspicion was 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. Id. at ** 18-19. The court found adequate reasonable suspicion where Abidor (1) possessed on the 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. at ** 18-19.


19 Id. at *5.
the agents followed, in broad brush, the guidelines of United States Customs and Border Protection (“CBP”) promulgated in 2008 and 2009, as justified and explained in the 2011 Civil Rights/Civil Liberties Assessment of Border Searches of Electronic Devices. According to the complaint, the agents had searched numerous files on his laptop that contained “highly private and expressive materials that reveal intimate details” about the student’s life. Presiding federal District Court Judge Korman upheld the extended search of the student’s laptop and hard drive because (1) border searches have historically been granted complete 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, thus there was no need to require the agents to meet any standard at all, even mere reasonable suspicion, to justify such a search.

In reaching its decision, the court in Abidor cited many of the leading cases from the largely pre-digital age. After noting the inquiry balances the government’s interest against the intrusion into the subject’s Fourth Amendment rights, the court found, “The Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.” Although the Flores-Montano case arose in the digital era, it did not implicate digital technologies. The court also relied on Camara v. Municipal Court, the leading case from the pre-digital era, on administrative searches, in general. While it briefly touched on the

---

23 Id. at *6.
24 Id. at **14-16, 18.
26 387 U.S. 523 (the case did not involve border searches or searches of digital equipment).
27 See id. (the case did not involve border searches or searches of digital equipment).
“significant invasion of privacy” occasioned by a laptop search, the court quickly foreclosed any more searching inquiry by finding that travelers are on notice their laptop may be searched, so the court suggested, “the sensible advice to all travelers is to ‘think 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?’”

But, it is not really necessary for courts in the digital age to apply old, pre-digital age cases and theories to today’s digital technologies. They are not only factually distinguishable, but also rest on assumptions that, in a digital age, are no longer valid. As such, it would be improvident, even injurious, to rely on cases that did not account for, or even contemplate, technology’s rapid emergence and use by the government as a law enforcement tool. Simply put, a laptop is not analogous to a closed container in any relevant legal sense. The digital age requires a different analytical construct not tied down by precedent that no longer applies.

B. OTHER “VICTIMS” OF SUSPICIONLESS BORDER SEARCHES OF DIGITAL DEVICES

In addition to graduate student Abidor, the other plaintiffs in the Abidor case were the National Association of Criminal Defense Lawyers (“NACDL”) and the National Press Photographers Association (“NPPA”). Those association plaintiffs argued that their members were likely in the future to be adversely affected by suspicionless digital border searches since they often travel internationally with confidential and sometimes privileged materials that are stored digitally. Travelers of all stripes are at risk of extensive border searches of their digital equipment if they travel internationally, but defense counsel, perhaps members of the NACDL, bearing 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.

28 Abidor, ___ F. Supp. 2d. at ___, 2-13 WL 6912654 at *16 (quoting Airport Insecurity: The Case of the Lost & Missing Laptops, Ponemon Inst. LLC, at 8 (July 29, 2008)).
29 Abidor, ___ F. Supp. 2d. at ___, 2-13 WL 6912654 at *6.
And a reporter, perhaps a member of the NPPA, cannot really promise confidentiality to an informant if the informant’s identity, when stored on a laptop or cell phone, can be seized without suspicion upon the reporter’s re-entry into the United States.

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

The First Amendment provides: Congress shall make no law . . . abridging the freedom of speech.”  

And that protection has been repeatedly extended to unpopular or offensive speech or other expressive conduct, including profane speech, Nazi speech, obscenity so long as consistent with community standards, and a substantial portion of what some would consider of ‘hate’ speech. Given the realities of border searches, imagine how much of the contents of one’s laptop or cell phone might be offensive to one person or group or another, 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 indicative of criminal intent. American citizens 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.

This demonstrates the inextricable link between privacy and expression. The infringement, while not occasioned by disclosure itself, arises from the resulting “chill” on political speech that makes people think twice before exercising their constitutional rights. In Abidor, the seized depictions were gatherings of terroristic groups – gatherings one can see

---

30 U.S. Const. amend. I.
32 See Collin v. Smith, 578 F.2d 1197 (7th Cir. 1978).
depicted on television and internet news programming. The government’s search of this 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—justified these suspicionless border searches.

They are tantamount to a search for ideas, and conducted in a manner that is far more intrusive than the “border exception” contemplates. The border agents are not searching for drugs or guns, or other physical evidence that threatens safety or, in and of itself, is unlawful. 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 letters to a loved one, or opinions criticizing the government, are searchable in the interests of border safety, then the viability of a “constitution-free” zone must be questioned.

In the absence of some standard—reasonable suspicion—these border agents are just fishing in what is nothing other than a digital dragnet. Neither the border control exemption, nor the interest in national security, justifies such sweeping governmental power, particularly where the invasion upon privacy is so substantial and enduring. Furthermore, the possibility of uncovering present criminal activity, e.g., images of child pornography, does not justify intrusions that are based on mere hunches, and that serve to create, not independently demonstrate, probable cause. In most cases, such as Abidor, the ‘evidence’ of wrongdoing is suggestive of future criminal activity, and based on the unreliable assumptions that drove racial and ethnic profiling.

Ultimately, therefore, a sovereign’s interests in self-protection and protection of its residents does not justify nor require suspicionless border searches of digital devices. Indeed, a

reasonable suspicion threshold before permitting a border search of digital devices would adequately protect the sovereign.

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

Reasonable suspicion is a threshold far lower than probable cause, but far higher than no threshold at all. As the court noted in Abidor, “[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’.”36 A relatively modest threshold, to be sure, and as such, a threshold within which the sovereign’s interests can still be protected without permitting fishing expeditions, digital dragnet searches, of electronic devices at our borders.

If a person appears at the border, intending to enter the United States, and the border agent’s screen indicates the person has prior convictions for child pornography, that would yield sufficient reasonable suspicion to permit the border agents to search the person’s electronic devices.37 If a person seeks to enter the United States and border agents discover the person is on a terror watchlist, border agents would have sufficient reasonable suspicion to search the person’s electronic devices.38 And where the agents know that an entering person was suspected

36 Abidor, ___ F. Supp. 2d at ___, 2013 WL 6912654 at *18 (quoting United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006) (in turn quoting United States v. Asbury, 586 F.2d 973, 975-76 (2d Cir. 1978)).

37 See United States v. Irving, 452 F.3d 110 (2d Cir. 2006) (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) (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); United States v. Furukawa, No. 06-145 (DSD/AJB), 2006 WL 3330726 (D. Minn. Nov. 16, 2006) (upon Furukawa’s return to the United States from Japan, border agents had reasonable suspicion to search Furukawa’s laptop and external hard drive where the agents had been informed of evidence that Furukawa had purchased accessed to a website that contained child pornography).

38 Indeed, the Abidor case, where the agents only had evidence that a Ph.D. student, whose area of study was Shi’ites, had a few photographs of Hamas and Hezbollah activities and two passports, would have left a very different mark had the border agents obtained evidence, prior to the search, that Abidor was on a terror watch list,
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. \(^{39}\)

It is not enough, as some have noted, that the border search exception is “as old as the Fourth Amendment itself.” \(^{40}\) In the digital age, with border searches of digital devices, the agents are not searching for guns, drugs, or illegal persons. They are searching for anything, and that is the problem. Thus, where laptop computers, cell phones, and data storage devices hold mountains of data that travelers could not have carried had it all been in paper format, and where computers and cell phones retain copies of data and website visits in shadow files even after the user has deleted and purged them, the legal system—and doctrinal paradigm—must react. Outdated precedent has, as a practical matter, already been overruled.

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

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

Congress—or the courts—must recognize that antiquated notions of privacy have no place in an era where technology has outpaced legal doctrine, and undermined the value of \textit{stare}

---

39 E.g., United States v. Singh, 295 Fed. App’x 190 (9th Cir. 2008).
decisis. While, the court in Abidor dismissed the association plaintiffs’ complaints on standing grounds after exhaustively exploring, in eight pages of the nineteen-page opinion, the law of standing, it made clear that, had it reached the merits, it would have ruled that the search was perfectly valid.\footnote{Id. 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.\footnote{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 A.L.B. L.J. SCI. & TECH. ___, (forthcoming 2014).} This suggests that courts are both unable—and unwilling—to meet the new challenges of the digital age.

First, a plaintiff must have a particular and personal injury – that had already 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 – by definition, a case or controversy that had already occurred in the past – before a court will take the case. Thus, purported plaintiffs, such as the NACDL and the NSSA, have no recourse in court to try to head off future disaster at the pass. Third, a court cannot, with precedential value, extend the impact of an opinion beyond the facts of the case before it, because that would be considered mere dicta.\footnote{Query why a court cannot extend the precedential power of its own case opinion beyond the facts of that particular case, but later courts are apparently free to apply that prior opinion as precedent in cases unimaginably far afield from the facts of that original “precedent.” The authors refer to that as the Dicta-Precedent Anomaly.} Fourth, courts – particularly courts of last resort – have a limited docket. Given these doctrinal constraints, coupled with the fact that the United States Supreme Court hears a fraction (often less than one percent), of the cases petitioned to it for certiorari,\footnote{See 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 files between June 30, 2011, and July 2, 2012). The Court issued formal opinions in fewer than 85 cases per year for each year from 2007-2011. http://www.uscourts.gov/uscourts/Statistics/JudicialBusiness/2012/appendices/A01Sep12.pdf.} the courts are not in a position to answer the questions that will arise as
technological advances become more common—and complex. Simply put, courts are not an
effective forum for resolving basic digital age privacy disputes in a timely fashion. Courts, in the
digital age, are doomed to provide too little, too late.

Congress and state legislatures, however, 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), 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, Congress and state legislatures are the proper guardians of privacy in the digital
age. For example, if Congress could muster the votes, it could enact legislation requiring all
future digital searches at the border to be conducted only upon a showing of at least reasonable
suspicion. Now that the Supreme Court has declined certiorari in *Cotterman*, 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. As demonstrated by the Court’s recent grant of certiorari in
*Riley v. California*, 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

---

45 Perhaps the Congress could focus its efforts by amending the statute authorizing such border searches, 19 U.S.C.
§ 1467, and passing enabling legislation to compel the agency to revise the rule on point, 19 C.F.R. § 162.6.
46 See *supra* note 13 and accompanying text.
expand, and citizens will be without recourse. Eventually, the right balance will be struck, but there is no reason, as the Court’s future ruling in *Riley* might show, why we cannot do it now.