AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 115–365

EXAMINING WARRANTLESS SMARTPHONE SEARCHES AT THE BORDER

HEARING

BEFORE THE

SUBCOMMITTEE ON FEDERAL SPENDING OVERSIGHT AND EMERGENCY MANAGEMENT

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 11, 2018

Available via http://www.Govinfo.gov

Printed for the use of the Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE

31–483 PDF WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN McCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana

CLAIRE McCASKILL, Missouri
THOMAS R. CARPER, Delaware
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*
MARGARET E. DAUM, *Minority Staff Director*
LAURA W. KILBRIDE, *Chief Clerk*
BONNI E. DINERSTEIN, *Hearing Clerk*

SUBCOMMITTEE ON FEDERAL SPENDING OVERSIGHT AND EMERGENCY MANAGEMENT

RAND PAUL, Kentucky, *Chairman*

JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, Montana

GARY C. PETERS, Michigan
KAMALA D. HARRIS, California
DOUG JONES, Alabama

GREG MCNEILL, *Staff Director*
ZACHARY SCHRAM, *Minority Staff Director*
KATE KIELCESKI, *Chief Clerk*

CONTENTS

	Page
Opening statement:	
Senator Paul	1
Senator Peters	2
Senator Wyden	12
Senator Jones	13
Prepared statement:	
Senator Paul	21
Senator Peters	23

WITNESSES

WEDNESDAY, JULY 11 2018

Laura K. Donohue, J.D., Ph.D., Professor of Law, Georgetown University Law Center	4
Neema Singh Guliani, Senior Legislative Counsel, Washington Legislative Office, American Civil Liberties Union	6
Matthew Feeney, Director, Project on Emerging Technologies, Cato Institute	8

ALPHABETICAL LIST OF WITNESSES

Donohue, Laura K. J.D., Ph.D.:	
Testimony	4
Prepared statement	26
Feeney, Matthew:	
Testimony	8
Prepared statement	60
Guliani, Neema Singh:	
Testimony	6
Prepared statement	51

APPENDIX

Letters referenced by Senator Peters	68
Statement submitted for the Record from Customs and Border Protection	81

EXAMINING WARRANTLESS SMARTPHONE SEARCHES AT THE BORDER

WEDNESDAY, JULY 11, 2018

U.S. SENATE,
SUBCOMMITTEE ON FEDERAL SPENDING,
OVERSIGHT AND EMERGENCY MANAGEMENT,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:39 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Rand Paul, Chairman of the Subcommittee, presiding.

Present: Senators Paul, Peters, Harris, and Jones.

Also present: Senator Wyden.

OPENING STATEMENT OF SENATOR PAUL

Senator PAUL. I call to order this hearing of the Senate Homeland Security and Governmental Affairs Subcommittee on Federal Spending Oversight and Emergency Management. I have to read it because the title of our Committee is so long, I cannot remember it.

Today we will be discussing the Fourth Amendment's guarantee against unreasonable searches and seizures and its application to 21st Century technology at the U.S. border. Early last year, reports began to surface about travelers having their phones confiscated and searched by U.S. border authorities for no obvious reason and without a warrant or even much of an explanation. These searches have targeted a National Aeronautics and Space Administration (NASA) engineer, a former captain in the U.S. Air Force, a Wall Street Journal reporter, a government security contractor, and numerous other U.S. citizens.

These searches are not just running a phone through an X-ray machine or a metal detector. Customs officials demand that these travelers unlock their phones so that the contents can be searched. If they refused, these travelers were threatened and interrogated. One man was handcuffed while another was physically restrained in a chokehold while government agents picked his phone out of his pocket. Yet another, the NASA engineer, was told that he was not allowed to leave until he gave his password to customs officials.

Two ironies here: (1), the engineer was enrolled in the Border Patrol's Trusted Traveler Program, which strikes me as false advertising; and, (2), the phone in question was a government phone.

Some may be asking, What about the Fourth Amendment protection against warrantless searches? Does this not extend to U.S. citi-

zens at the border? Actually, the courts have held there is something of a gray area at the border, which, by the way, includes international airports and seaports. Customs officials may conduct routine searches of luggage or other containers without a warrant under what some refer to as "the border search exception to the Fourth Amendment." This so-called exception has historically been used to ensure that no weapons, drugs, or other prohibited items, cargo, or persons are entering the country. I think that most Americans could agree that it is reasonable to let customs officials search suitcases for contraband. What is unreasonable is that government lawyers want you to believe that there is no difference between a suitcase and a smartphone.

I disagree, and here again I think most Americans would, too. Physical contraband cannot enter the country unless it is smuggled in. But this is not the case for electronic property. Anything a Border Patrol Agent can find in the contents of your cell phone could enter the country through the Internet without the physical phone ever coming close to the United States. But it is all the more troubling when you consider what the government is gaining access to. Smartphones can reveal virtually everything about a person—their movements, habits, relationships, health, faith, and finances, all in a single, easy-to-use, and archived interface. Indeed, I think for many of us today, searching our smartphone would prove to be much more intrusive than even a search of our homes.

This same sentiment has been echoed in recent Supreme Court decisions regarding the Fourth Amendment and digital data. In a unanimous opinion in a 2014 case involving cell phone searches incidental to arrest, *Riley* v. *California,* Chief Justice Roberts wrote, "Cell phones differ in both a quantitative and qualitative sense from other objects that a person may possess." Searching a person's smartphone or other electronic device is fundamentally different than searching their suitcase or their car, and I believe as legal challenges to these searches reach the Supreme Court, they will agree.

We have an esteemed panel of witnesses here today who will discuss the history of border searches, the appropriateness of using this authority to search smartphones, and what actions Congress should take to address this issue.

At this time I would like to recognize Ranking Member Peters for his opening remarks. Senator Peters.

OPENING STATEMENT OF SENATOR PETERS[1]

Senator PETERS. Thank you, Mr. Chairman, for calling this hearing today. I appreciate your continued willingness to work in a bipartisan way to take on tough questions about our core values as Americans, our rights and responsibilities as citizens, and our role in the centuries long fight to ensure equal protection under the laws.

The problem we are exploring today requires us to examine detailed policy directives and puzzle over how 18th Century words fit to a 21st Century technology. The details are important undoubtedly, but at its core this hearing is about the liberties guaranteed

[1] The prepared statement of Senator Peters appears in the Appendix on page 21.

to us by the Constitution. It is about our freedom to travel, our right to be secure against unreasonable search and seizure. It is about our right to be treated equally under the law without regard to race, national origin, or religion.

The Fourth Amendment states clearly, and I quote from the amendment, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

U.S. Customs and Border Protection (CBP) asserts that the Fourth Amendment does not require a CBP officer to obtain a warrant or even have individualized suspicion before searching a smartphone or directing travelers to unlock their devices for official inspection. Today's witnesses, like most of the courts that have considered this question, disagree.

This issue is of particular significance to those of us who live in Michigan. Michigan shares hundreds of miles of international border with Ontario, Canada, including the Ambassador Bridge, one of North America's busiest border crossings. Most importantly, Michigan is home to a large and extremely vibrant and patriotic Arab and Muslim American community, and community leaders tell me that they feel unfairly targeted by CBP.

I have heard countless stories of my constituents returning from family vacations, medical conferences, work trips, you name it, and being singled out for additional screening, being required to turn over phones and computers, provide their passwords, and wait for hours while their devices are searched. Some constituents have reported being asked about their views on politics or foreign affairs.

CBP says that travelers can file complaints if they feel that they have been mistreated, but my constituents fear that complaining will cause them further targeting. And who among us, tired from travel and eager to return home to family, would not feel very vulnerable in this situation?

One of my constituents described his perceived targeting as a "backdoor travel ban." The fear of unfair treatment and the profound inconvenience of repeated and prolonged searches creates an immense disincentive to travel. It hurts families. It impacts commerce. We can do better, and we have to do better.

Under the Constitution, Arab and Muslim American citizens are entitled to the same liberty, the same privacy, and the same freedom of movement that I am entitled to. CBP plays a central role in securing our future and protecting our national security. It is critical that they have the tools that they need to succeed, but it is no less critical that those tools adhere to the Constitution in their design and application and that no law-abiding American is unfairly singled out.

Just over the last few days, I have received several heartfelt letters describing unfair and unconstitutional treatment and asking for congressional intervention. Mr. Chairman, I ask that letters from the Arab American Institute, the Arab American Civil Rights League, the Arab American Anti-Discrimination Committee, and

the Electronic Privacy Information Center be entered into the record.[1]

Senator PAUL. Without objection.

Senator PETERS. Congress should weigh in and establish clear constitutional rules and a means for ensuring that they are applied equitably. I am grateful that Senator Paul with Senators Wyden, Leahy, and Daines have taken the lead in identifying a path forward, and I hope this hearing goes a long way in making that path available.

Senator PAUL. Thank you, Senator Peters.

First, I would like to begin by noting that we may have some Senators who are not on this Committee here today, and I would like to ask unanimous consent to allow them to fully participate in the hearing, provided Members of the Subcommittee be given deference in order of recognition.

Next, I would like to remind the witnesses that the written testimony they have submitted will be included in the record and to keep your opening remarks to around 5 minutes. Let us begin.

Laura Donohue is a professor of law at Georgetown Law and the director of Georgetown's Center on National Security and the Law, as well as the director of the Center on Privacy and Technology. She has written extensively on privacy, surveillance, national security, and emerging technologies, and enjoys the distinction of having been appointed as one of the five Friends of the Court to the U.S. Federal Intelligence Surveillance Court, positions which were newly created by the 2015 USA Freedom Act.

I would also note that she serves as a reporter for the American Bar Association's Criminal Justice Section Task Force on border searches of electronic devices, so she is extraordinarily well versed on the topic of the hearing today. Welcome, Professor Donohue.

TESTIMONY OF LAURA K. DONOHUE, J.D., PH.D.,[2] PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER

Ms. DONOHUE. Thank you very much. Chairman Paul, Ranking Member Peters, and Members of the Subcommittee, thank you for the opportunity to testify at today's hearing.

The border search of electronic devices is rapidly increasing. In 2015 CBP examined 8,500 devices. The number more than doubled the following year before soaring in 2017 to more than 30,000 searches. U.S. Immigration and Customs Enforcement (ICE) in turn searched just over 4,400 cell phones in 2015. In 2016 it searched 23,000 devices.

As Chairman Paul noted, the Supreme Court in *Riley* v. *California* recognized that these devices "implicate privacy concerns far beyond those implicated by the search of a wallet or a purse." Even the term "cell phone" is misleading. The Court noted many of these devices are, in fact, mini computers that happen to be used as a telephone. They have an immense storage capacity and can hold millions of pages of text, thousands of pictures, or hundreds of videos.

[1] The letters referenced by Senator Peters appear in the Appendix on page 66.
[2] The prepared statement of Ms. Donohue appears in the Appendix on page 24.

In contrast, most people do not lug around every piece of mail they have received for the past several months, every picture they have taken, and every article or book that they have read.

The type of information is different than that uncovered in a luggage search: medical records, location information, political beliefs, religious convictions, and relationship details for decades, in fact, more information than can be ascertained from the search of your home.

The Executive Branch is divided on how it addresses border searches. As Ranking Member Peters pointed out, CBP's January 2018 guidelines allow for searches without any suspicion whatsoever. This means that the Executive Branch could seize the phones, iPads, and laptops of every Member of this Committee, those of your staff, your spouses, and your children whenever entering or leaving the United States without any suspicion of wrongdoing. There are no statutory limits on who can see this information, how long it can be kept, or how it can be used. And there is no special protection provided for sensitive materials, political materials, client-attorney privilege, trade secrets, medical information, or materials otherwise privileged under the law.

For advanced forensic searches, officers must merely meet a standard of reasonable suspicion of illegal activities or national security concerns. No probable cause is required. The equivalent immigration directive has not been updated since 2012. Like its counterpart, it pertains to any item containing electronic or digital information. But unlike its counterpart, ICE authorizes agents to search, detain, seize, retain, and share aliens' electronic devices and information with or without individualized suspicion. At any point during a border search, electronic devices or copies may be detained for further review, either on or offsite. They can be kept for 30 days and extended at 15-day intervals thereafter.

CBP claims the plenary authority to conduct searches and inspections of persons and merchandise crossing our Nation's borders. The government is right that this border search power derives from U.S. sovereignty. As I note in my written remarks, courts have for decades recognized that this power resides in Article I and Article II. But the Founders did not end the Constitution there. The Constitution also protects rights. And as Chairman Paul recognized when he introduced the Protecting Data at the Border Act, innovation does not render the Fourth Amendment obsolete.

Three Supreme Court cases now recognize the heightened privacy interest at stake. Riley dealt specifically with mobile telephones. In the 2012 case of *United States* v. *Jones,* five Justices, the so-called shadow majority, adopted the view that individuals have a reasonable expectation of privacy in the whole of their physical movements. This past month, the Carpenter Court built on Jones. Chief Justice Roberts writing for the majority looked at just one type of information that is located on mobile telephones, noting six elements that make it different from other kinds of records, namely, that it is specific; it is retroactive; it is extensive, going back multiple years; it is precise; it is deeply revealing; and it is easy, cheap, and efficient to access.

Mobile phone data is different in kind than other kinds of records, and it is different in kind than what we pack for a trip

to, say, Australia. Lower courts, unclear about how to think about electronic border search post-Riley, Jones, and now Carpenter are reaching disparate and deeply concerning conclusions. I would be happy to discuss these further during the session.

In addition to the Fourth Amendment issues, as I note in my written remarks, there are important First Amendment issues of freedom of speech and religion and association; there are Fifth Amendment self-incrimination and due process concerns; and there are Sixth Amendment right to counsel issues on the table.

I look forward to the discussion. Thank you.

Senator PAUL. Thank you.

Our next witness will be Neema Singh Guliani, who is senior legislative counsel with the American Civil Liberties Union's (ACLU) Washington Legislative Office, specializing in surveillance, privacy, and national security issues. She was previously on staff at the Department of Homeland Security (DHS) and Department of Agriculture and I think is very familiar with the type of oversight work we are doing here today from her time as investigative counsel with the House Oversight and Government Reform Committee.

Welcome, Ms. Guliani.

TESTIMONY OF NEEMA SINGH GULIANI,[1] SENIOR LEGISLATIVE COUNSEL, WASHINGTON LEGISLATIVE OFFICE, AMERICAN CIVIL LIBERTIES UNION

Ms. GULIANI. Thank you. Chairman Paul, Ranking Member Peters, and Members of the Subcommittee, thank you for the opportunity to testify today and thank you for your leadership on this important issue.

Each year, tens of thousands of individuals are subject to invasive and often humiliating searches of their electronic devices at the border without a warrant based on probable cause. One of these individuals is Diane Maye, a former Air Force captain and current professor of homeland security and global conflict issues. She is also a plaintiff in an ongoing case brought by the ACLU and the Electronic Frontier Foundation.

In June 2017 Professor Maye was traveling to Miami when she was detained by CBP officers upon arrival. She was escorted into a small room, where CBP officers seized her smartphone and her laptop. Because she had no meaningful choice, Professor Maye unlocked both devices and watched as officers searched her laptop and later as they confiscated her unlocked phone for approximately 2 hours.

In describing her experience, Professor Maye has said, "I felt humiliated and violated. This was my life, and a border officer held it in the palm of his hand."

In yet another case, Ghassan and Nadia Alasaad, who are also plaintiffs in the same case, were returning from a family vacation when their entire family was detained by CBP, including their ill 11-year-old daughter. Upon arrival, they were directed to secondary inspection where CBP officers questioned Mr. Alasaad and searched through his unlocked phone. The CBP officers later requested that Ms. Alasaad turn over her cell phone password.

[1] The prepared statement of Ms. Guliani appears in the Appendix on page 49.

The couple refused, in particular because Ms. Alasaad wears a headscarf in accordance with her religious beliefs and her cell phone contained pictures of her without her headscarf, which she did not want CBP officers, particularly male officers, to view. The CBP officers explained that failure to turn over the password and comply would result in Ms. Alasaad's phone being confiscated. Because they had no meaningful choice, the Alasaads provided the password.

There are countless other examples, many which raise the additional concern that individuals are being improperly targeted based on their religion, political beliefs, or other impermissible factors. As Professor Donohue noted in her earlier remarks, the number of these searches has soared to over 30,000 in 2017, representing a 3½ time increase from 2015.

DHS violates the Constitution by engaging in these warrantless device searches, wrongly arguing that they fall under the border search exception to the Fourth Amendment's warrant requirement. These searches do not comport with the Fourth Amendment, as recent Supreme Court jurisprudence makes clear.

The Supreme Court's unanimous Riley decision made clear that traditional exceptions to the Fourth Amendment's warrant requirement do not automatically extend to searches of digital devices. In its decision, the Court highlighted the volume and sensitivity of information stored on these devices, noting that it would allow someone to reconstruct the sum of an individual's private life. This term, in Carpenter, a case argued by the ACLU, the Supreme Court also ruled that historical cell phone location information was subject to the Fourth Amendment's warrant requirement. Similar information can often be gleaned from a device search.

Indeed, several courts have rejected the government's claim that the border search exception places no limit on device searches at the border. The Fourth Circuit has recognized that a forensic search of an electronic device at the border requires some level of individualized suspicion, though it declined to address whether a warrant or probable cause is required.

As this issue is litigated, however, thousands continue to have their rights violated. That is why it is important that Congress swiftly pass legislation, including the Protecting Data at the Border Act, sponsored by Senator Paul, Senator Wyden, and others. Congress should make clear that a warrant is required for all searches of the content of electronic devices, that travelers are not under an obligation to unlock or provide device passwords, and that individuals cannot be unreasonably detained for failing to consent to a search or unlock their device.

Until such legislation is passed, Congress should press CBP to release new guidance that contains the following four improvements:

One, the guidance should require a warrant in any case where the government seeks to search the content of a device. Current policy requires no suspicion for so-called basic searches and only reasonable suspicion for advanced searches.

Two, the guidance should narrow the permissible purposes of the search. CBP should be prohibited from conducting searches at the request of or to assist other agencies. The guidance should also not

allow suspicionless searches when there is vague so-called national security concerns. Such language is vague, could be interpreted as applying in cases where an individual poses no imminent threat, and increases the likelihood of discriminatory and arbitrary application.

Three, the guidance should be amended to make crystal clear that travelers are not obligated to turn over their device passwords, and it should prohibit unreasonably detaining individuals for failure to take such action.

And, finally, the CBP guidance should apply to all DHS components, including ICE, which maintains its 2009 policy which has even fewer protections.

Again, thank you for your leadership on this issue, and I look forward to answering any questions you may have.

Senator PAUL. Thank you. Thank you for your testimony.

Our next witness is Matthew Feeney. He is the director of Cato Institute's Project on Emerging Technologies where he focuses on the intersection of new technologies and civil liberties. He was previously an assistant editor at Reason.com and a writer at The American Conservative and the Institute of Economic Affairs.

Welcome, Mr. Feeney.

TESTIMONY OF MATTHEW FEENEY,[1] DIRECTOR, PROJECT ON EMERGING TECHNOLOGIES, CATO INSTITUTE

Mr. FEENEY. Thank you, Chairman Paul, Ranking Member Peters, and Members of the Subcommittee. Thank you for the opportunity to speak with you today about an important topic that I think should concern every American.

In *Riley* v. *California* the U.S. Supreme Court recognized that searches of cell phones implicate privacy concerns beyond those associated with searches of wallets, cigarette packs, and other everyday items. Writing the Riley majority opinion, Chief Justice Roberts stated that the government's claim that the search of a cell phone and the search of a wallet are "materially indistinguishable" is "like saying a ride on horseback is materially indistinguishable from a flight to the moon."

Roberts was correct. Our cell phones contain troves of revealing information about our personal relationships, careers, religious affiliations, and hobbies. It is no exaggeration to say that unfettered access to a cell phone allows investigators to uncover details about almost every intimate communication and relationship associated with the owner of that cell phone. Officials with access to cell phones can easily view photos, calendars, email accounts, social media postings, and other revealing data. Riley's holding that police need a warrant to search phones belonging to arrested persons recognizes the privacy interests American adults have in the content of cell phones.

Despite Riley, as we have already discussed, cell phones and other electronic devices enjoy reduced protections at the border, thanks to the Fourth Amendment's border exception. The Supreme Court has yet to consider constitutionality of warrantless searches

[1] The prepared statement of Mr. Feeney appears in the Appendix on page 58.

of electronic devices at the border; however, Congress can extend the Riley standard to the border via legislation.

Although the warrantless search of electronic devices affect a minority of travelers, the number of these searches has been increasing, almost 60 percent between fiscal year (FY) 2016 and fiscal year 2017.

A 2009 CBP directive on electronic device searches stated, "In the course of a border search, with or without individualized suspicion, an officer may examine electronic devices and may review and analyze the information encountered at the border."

A 2018 directive improved the 2009 directive, but not enough. The latest directive distinguishes between "Basic" and "Advanced" searches. Under current DHS policy, a search of an electronic device that does not involve an officer connecting the device to external investigatory equipment is a Basic search. Basic searches do not require suspicion, which is required for so-called Advanced searches. The new directive includes a worrying provision that allows officers to examine a phone with external equipment if there is a "national security concern." This is especially worrying because the directive notes that "the presence of an individual on a government-operated and government-vetted terrorist watch list" creates reasonable suspicion. Government watch lists, however, do not only include terrorists. Officials have placed law-abiding Americans on watch lists designed to prevent dangerous people from flying.

The 2018 directive also requires travelers to unlock their phones. CBP officers have compelled American citizens to unlock and hand over their phones, even after being told that the phone contained sensitive data, such as those belonging to NASA's Jet Propulsion Laboratory.

According to the latest directive, officers conducting a search must either have the travelers disable network connectivity or disable the connection themselves by, for example, putting the phone into airplane mode. But these policies are of little reassurance to travelers. Even in airplane mode, cell phones contain revealing information. Text messages, emails, photos, browsing histories, videos, and calendars are still available to officers examining a cell phone in airplane mode. In addition, cell phones in airplane mode do not conceal apps that the cell phone owners may use. You hardly need to have a phone connected to a network to uncover information about someone who has downloaded the Muslim Pro, Coinbase, or Tinder apps.

Current DHS policy does not do enough to protect travelers' civil liberties. However, bills proposed by the Chairman as well as Senator Leahy do improve the CBP 2018 directive. A welcome provision of the Senator Wyden and Senator Paul bill is the warrant requirement for cell phone searches. The Leahy bill would also improve the status quo by requiring increased transparency. DHS has not published figures showing how many of these warrantless searches have contributed to terrorism or child pornography-related convictions. Such data would be welcome, as it would allow the public to better assess the efficiency of warrantless searches that endanger their privacy.

As has been discussed, some of the U.S. courts of appeals have considered questions concerning the standard of suspicion that

should be necessary; however, as things stand, there is no consensus. Until the Supreme Court addresses this issue, lawmakers can provide CBP with requirements that go beyond the unsatisfying directive issued by the Department of Homeland Security.

Again, thank you for your attention to this important matter and for the opportunity to testify before you. I look forward to answering any questions you may have.

Senator PAUL. Thank you very much. I thank all of you for your testimony.

When I first heard about this and I heard that it would be possible that an American citizen could leave the country and come back and be denied entry into their own country unless they give their password up, I was horrified by this. I very quickly called my colleague Ron Wyden and said, "We have to do something about this." There are an array of people on both sides of the aisle who I think want to fix this.

The first question I have is a little more tricky and goes to the fine point of things and may not bring us all into an agreement. But there is sometimes a debate over who the Constitution applies to. I think most people who read the Constitution realize it applies to everybody in the United States, all persons, Fifth Amendment, Sixth Amendment, you get a trial whether you are here legally, illegally, whatever your status is, you get a lawyer, a jury trial.

It is a little bit different maybe at the border, and I think I could allow for a little bit of difference between citizens and U.S. persons and maybe those who are visiting. That is the question I throw out to you. For example, one of the gentlemen who had his phone taken was in the Trusted Traveler Program. Frankly, once you get in that program, if it is worth what it is supposed to be worth, you probably should be going through security much more easily than other people. Maybe somebody who is not in the Trusted Traveler Program might get searched more often, randomly or otherwise, and there might be different thresholds for people based a little bit maybe on citizenship and U.S. personhood versus someone who bought his or her ticket yesterday and is coming from an area where there is a lot of terrorism. Could we ask more questions at a lower level or would we have a warrant requirement for everybody?

And so I would throw that question out to the panel on citizenship, whether the rules have to be exactly the same or at the border we might have a gradation based on citizenship versus non-citizenship.

Ms. DONOHUE. Yes, thank you. I would distinguish here between law and policy. So as a matter of constitutional law, the Fourth Amendment—in 1990 Chief Justice Rehnquist ruled in a case called Verdugo-Urquidez that the Fourth Amendment does not apply to non-citizens who lack a substantial connection to the United States. And the reasoning that he had in that case, as well as Kennedy's concurrence in that case, which is slightly different from Chief Justice Rehnquist, but his reasoning was that the right of the people to be secure in their persons, houses, papers, and effects, as Ranking Member Peters quoted us the Fourth Amendment, it is the same people that are the people in the Constitution;

therefore, the Fourth Amendment does not apply. And this might explain the difference between CBP's provisions, which come from a customs background applied as to U.S. persons, as opposed to immigration provisions in Title 19, which apply then to aliens and non-U.S. persons.

With that said, in the last hearing that you had on this in 2017, there was a really interesting discussion, and at that point Senator McCaskill noted that if she were visiting another country and was asked at that point to turn over your social media password, your mobile phones, all of your records, that this could cause significant foreign affairs and national security concerns. So she said, "If my family was traveling to the United Kingdom and they told me we would have to answer questions about my beliefs, we would not go." This will have a profound impact on our standing in the world, a profound impact on the nature of our alliances around the world, and a profound impact on our national security.

So while as a matter of law many of these—there might be a line to be drawn, and that I am happy to speak to as a constitutional law person, but as a matter of policy, that is something that Congress would have to take on board.

Senator PAUL. Right, and I think the one response I would have to that is that while you have to have scrutiny and you want protection, you also want to find ways that make the United States a friendly place to visit. That is why I am actually a big believer in some of the Trusted Traveler Programs, the frequent flyer programs. Let us try to do background scrutiny on people so they can go through the airports much easier and they do not feel oppressed. You could be from any country in the world. If you have gone through the process and we have screened you, I think we could get that. I really think we need to extend the Trusted Traveler Program to the whole world, and even the countries where we are so-called banning people now. Let people go through who are legitimate businessmen and businesswomen or academics or physicians or whatever that have legitimate reasons. I think we could probably obviate some of the problems we have, because you are right, who would want to go to a country where they are going to take your cell phone from you? But, on the other hand, we do have to worry about people coming here who might attack us.

I think without question American citizens and U.S. persons should be protected by the Fourth Amendment when they come back home.

Did either of you want to——

Ms. GULIANI. I think there are strong arguments in favor of applying a warrant standard to U.S. persons and non-U.S. persons. In addition to the reciprocity issue, how we treat non-U.S. persons when they arrive here is how we may be treated abroad. We have to recognize that the searches of these devices implicate not just the privacy of the person who owns that phone, but potentially thousands of others, their family members, their associates. When you are talking about, let us say, business travelers, they may have emails and other content that implicates the privacy of individuals inside the United States.

So we are talking about an enormous privacy violation, and we are talking about searches that at the outset are really quite at-

tenuated from searching for contraband, like you might do in luggage, or admissibility. For that reason, I think the right policy outcome is a strong standard that applies to both U.S. citizens as well as travelers.

Mr. FEENEY. I suppose it is difficult for me to give an unbiased opinion on this given I became an American citizen deliberately and happily after, well, retaining my British citizenship. I would note that I think the proposed legislation proposed by Senator Wyden, the Chairman, and Senator Leahy are all improvements on the status quo. But I think that what Neema and Laura mentioned is right, that maybe purely in the foreign policy realm, that it is good for our foreign policy to extend protections because we should be wary of how American citizens will be treated when they travel abroad.

Senator PAUL. Thank you for those responses. I have a family urgency I have to get to, so Senator Peters has agreed to take over. Before I leave, though, I want to thank Senator Wyden for coming. It is not very often that a Senator comes to a Committee they are not on, and I appreciate his support on this issue and actually coming to a Committee that he is not even obligated to come to.

With that, I am going to turn the gavel over to Senator Peters.

Senator PETERS [presiding]. Thank you, Mr. Chairman, and I will actually recognize Senator Wyden. I know you have a busy schedule, and the last thing you needed was another Committee to come to, but we appreciate that you are here because I know this is an issue you are passionate about, and you have the floor.

OPENING STATEMENT OF SENATOR WYDEN

Senator WYDEN. Well, Senator Peters, thank you for your thoughtfulness. Thank you, Senator Jones, for giving me the opportunity, and also to the majority that arranged for me to come. I know this is unorthodox, and being unorthodox has characterized my life. [Laughter.]

I thank you all for it.

Just one question so I do not impose too much on my colleagues. From the very beginning, what we tried to tap into was the zeitgeist of the times, and the zeitgeist of the times seems to be picking up, for example, that digital is truly different. That is how John Roberts puts it. The Carpenter case was certainly a step in the right direction, really looking to some of the privacy issues surrounding geolocation questions, and I remember from my Intelligence Committee days, we established that you had privacy rights overseas, if you were a soldier, and certainly constitutional rights should not stop automatically. They should not just disappear at the border.

So for my one question, Ms. Guliani, let me ask you about the government waiting until a person gets to the border zone. When you think about this concept, the question is whether it could be used as an end run around the warrant process. And all our bills, metadata, the bill as it relates to border searches, we have always had this, I think, very generous emergency exception so that if the government really thinks the security and safety of the American people is at stake, you can move quickly, then come back and settle up later on the warrant process. But to actually have an end run

around the warrant process is something completely different, and what you would have is just the opposite of my saying you ought to have an emergency process when something looks serious, the government does not have much to go on, probably does not have enough to get a warrant, so the government waits until the person gets in the border zone, then asks another agency, maybe CBP, to grab the devices for searches.

Now, in our bill we require reporting on instances like this in addition to requiring a warrant. Does anybody know how often these kinds of searches take place by agencies, like ICE would be an example?

Ms. GULIANI. We have reporting by CBP which has put out numbers that shows a dramatic increase in border searches. But I think what your remarks sort of touch on is a bigger problem: one, the weaknesses in the guidance in allowing these warrantless searches; the fact that the guidance does not prohibit them from being used for general law enforcement purposes as an end run around the Constitution. For example, the guidance does not prohibit searches performed at the request or to assist other law enforcement agencies, which is a major problem. And there is also, I think, a question about oversight and compliance even with the limited protections in that guidance. How do we know that a lot of the restrictions in that guidance are really being followed by the agency? The fact is that there is not a lot of comfort that that is happening.

Senator WYDEN. I appreciate the way in which you have tackled this over the years, keeping the focus on the substance, and we have talked to Mr. McAleenan about exactly some of those kinds of concerns, and some of those may be possible to address administratively as well as by statute.

Senator Peters, Senator Jones, I thank you both for your courtesy, and I look forward to working with you both on this and many other matters in the days ahead.

Senator PETERS. Thank you, Senator Wyden, and thank you for your leadership on this issue and other issues related to privacy and constitutional protections. We appreciate it.

Senator Jones, you are recognized.

OPENING STATEMENT OF SENATOR JONES

Senator JONES. Thank you, Senator Peters.

This is always a tough issue for someone who has been both a prosecutor and a defense lawyer, because I have been on both sides of the aisle, I recognize that. Of course, I think that also made me a better lawyer to understand when I could see both sides of this.

I am curious, Ms. Donohue. There are people who say the counter to the argument is that given the nature of a border crossing—and I mean at a port of entry (POE)—that you could really never get probable cause to go to a magistrate, to select—absent an extraordinary—somebody coming in with a sign hanging around their neck saying, "I am a dangerous person," you could really never get enough information to get a warrant to search a phone. What is your response to that for folks that are coming in? They are just travelers, they are coming in. What would it take to get past that probable cause standard?

Ms. DONOHUE. Yes, thank you for the question. There are a number of cases where the courts have actually said they had probable cause in order to examine the phone. So even post-Riley we see cases that have come forward. There is one that came out of the Fourth Circuit, for instance, *United States* v. *Kolsuz*, and in that the court said that the forensic border search of a mobile device was non-routine; it required individualized suspicion. But it did not reach what level of individualized suspicion was required, whether it was regular individualized suspicion or some sort of probable cause, because they said in that case probable cause was present.

Similarly, in the Fifth Circuit there is a case, *United States* v. *Molina-Isidoro.* The court said once again some level of individualized suspicion is necessary, but in this case they had probable cause in order to search the device. And there are many cases like that where the courts have come forward and said, "Well, they actually had probable cause." It tends to be where there is some—one of two things has happened. Either they have found criminal items in the suitcase, for instance. In one case it was firearms parts that were illegally being exported out of the country. That was probable cause to search the phone. In other cases it might be a text hit on the Treasury system or some other hit when they run a name through a database. Then that satisfies probable cause depending on the information that comes up. I think that there is an empirical counter to that.

The one thing I would mention, however, is the history of this is this was actually to raise revenue for the United States, and that was the history from England, and I wrote about this—they are in the written remarks, the history of this. This has never been used as a general law enforcement power, and that is partly to prevent it from becoming an end run around the Fourth Amendment. This is specifically for customs issues and post-World War II, certain other items that might be carried in the mails like child pornography and the like.

So there are limits on the types of things that they can search for at the border, and that is probably why the border exception.

Senator JONES. Let me follow up on that with you and probably Ms. Guliani. You mentioned contraband. That is what people normally think. You go through customs. They look at your suitcase to see if you are bringing in Cuban cigars, those kinds of things. Can't you bring in contraband on your cell phone?

Ms. DONOHUE. Child pornography has been the way that this is presented most readily at the border, and the way that they have actually found that is just by searching the cell phone when they have reasonable suspicion, usually from some sort of a hit, a lower level hit on one of the systems that they can check when somebody comes across the border. That seems to be the level. There are some plans that have been used. There was a computer facility that was going to be built in Iran, and they found some plans that were actually on the cell phone. I guess one could consider that a form of contraband of a sort, but it tends to be really in the child pornography area that we have seen cell phones used, which raises the difficult issue as a prosecutor. Should you be able to just upload it to the cloud and pull it down on the other side? And what do we do for those types of cases?

Senator JONES. Sure.

Ms. DONOHUE. And there I would suggest the Foreign Intelligence Surveillance Act (FISA). When the law came down, the Foreign Intelligence Surveillance Act can be used when the primary aim is criminal in nature, and we have surveillance provisions that are addressing those types of criminal activity.

Senator JONES. Do any of you have an issue with a border agent being able, I say an agent, a customs agent, for whatever reason just kind of randomly saying, OK, you are number 14 in line, sorry, we are going to go look through your suitcases? Is anybody going to have a problem with that? That happens. Nobody has a problem with that? All right. I am getting silence, so I am going to assume that nobody has a problem.

I have a question. I hate to dumb this down a little bit, but this is a tough topic. I mean, it really is. So if in that suitcase there is a three-ring binder like the one I have here, is it OK for the agents to look through that binder?

Ms. GULIANI. I think the distinction when we are talking about electronic devices is sort of twofold. One is just the quantity and the types of information we are talking about.

Senator JONES. Why does that make a difference? I am not challenging you. I am just asking you for the record. Why does that make a difference because of the quantity as opposed to the thickness of the binder?

Ms. GULIANI. As the Supreme Court has recognized, the types of information on an electronic device are different. We are talking about medical information, information about your religious beliefs, your political affiliation. You are talking about quantity and types of information that are extraordinary sensitive. It would be the equivalent of somebody arriving at the border not just with a suitcase, but maybe an entire house full of papers. That just does not happen. I think that we are really in a different realm when we are talking about digital searches of data.

And then when we look at sort of the purposes underlying border searches, looking for contraband, determining admissibility, these types of searches are quite attenuated. Even in the child pornography context, there is not particular evidence that suggests that the border is an area where there is increased risk of that. Child pornography certainly is a problem, but it is something that individuals use the Internet for. If you have that exception, what you are essentially saying is, because of this one issue that there is no evidence is more prevalent at the border, we are going to open up every single individual to a search that is incredibly invasive, often humiliating, often scary and frightening for the people who are put in that position. That seems to me to swallow the Fourth Amendment.

Senator JONES. All right. Thank you. I think I am about out of time. Let me say I think this is a really tough issue, and I agree with all of you, because the one thing that troubles me more than anything about this issue is the potential for profiling and targeting in a bad way. With all due respect to you all, the issue of the invasive search is an issue for me but not as much for me as it is targeting people with last names that raise an eyebrow. I think that is a real issue. As a prosecutor you can take anything

anybody says and say, "Oh, here it is," whether they answer fast, whether they answer slow, whether they hesitate, whether they do not. There are just so many ways you can read into it the way you want to read into it, and so the profiling is an issue that I am really kind of focusing on, Mr. Chairman. Thank you very much, Senator.

Senator PETERS. Thank you, Senator Jones.

Actually, I will pick up on the profiling comment. In my opening comments I mentioned the fact that we have a vibrant Arab American/Muslim American community in Detroit, and it is exactly that concern that I hear regularly from the community, that folks can pretty much plan on spending more time at the airport coming and going based on the fact that they are part of that community. What are you hearing out there? Is this real? And how do we deal with it?

Ms. GULIANI. I think we have heard a series of disturbing complaints. In a complaint that was received by the Knight Institute through a FOIA request, there was a report of an individual who in the same encounter they had their device searched, they were asked about their political affiliation, their religious beliefs, and who they gave charitable contributions to. I think these types of complaints raise the concern that individuals are being inappropriately targeted because of their religion or how they look, and that, frankly, is one of the reasons a warrant requirement is so important. Whether your device is searched and whether you are held should not be the result of a whim by a particular officer. It should be subject to strict judicial oversight. The fact that there is no warrant really allows and enables that type of discriminatory targeting in a way that raises significant constitutional concerns.

Senator PETERS. Mr. Feeney, the CBP's current rules include instructions for any data that is collected to be destroyed if the data does not provide probable cause. For anyone whose smartphone or laptop has been seized, searched, or returned by the CBP, how sure can we be that the data collected is truly deleted and is no longer accessible either to those authorities or any other government agency?

Mr. FEENEY. Well, I think that there is a certain point at which you trust that CBP are adhering to their own policies. There are, of course, audits that will oversee that kind of thing.

The worry, of course, though, is that some U.S. citizens might not take that policy as reassurance enough. One of the cases that was mentioned was of this NASA engineer who had his travel interrupted and his phone searched, and afterwards he did make changes to the phone and his social media profiles. And I do not think that is much of a surprise.

The guarantee that non-relevant data is destroyed is really important, but, frankly, even with CBP saying that they will do it, I imagine it will still change the behavior of American citizens who are stopped at the border because I think knowing that your phone has gone to a back room and has been examined by officers will prompt some change of behavior, and we should not be that surprised by that.

Senator PETERS. Yes, Ms. Donohue?

Ms. DONOHUE. Yes, I just wanted to note that leaving it to CBP and ICE to police themselves, to come up with their own regulations, is quite dangerous. This was actually exactly the proposal that was put forward in Riley. The government argued to the Court that we should be able to come up with our own regulations for how to deal with cloud technologies and mobile phones. The Court replied, saying, "The Founders did not fight a revolution to gain the right to government agency protocols." It was a really profound point that the Court had, which is this is about rights, and those rights should be statutorily guaranteed, and they are constitutionally guaranteed. They should not be left up to the whim of an organization or an agency in terms of their regulations.

Ms. GULIANI. Right, and this is absolutely an area where there needs to be more oversight. We do not know to what extent CBP complies with its own limited protections that are in its policy. When it comes to data retention, I think there does need to be independent auditing, compliance reviews done by independence entities to make sure that even what is in those policies is being followed.

Senator PETERS. You mentioned the cloud. I just want to be sure that I understand what we are dealing with here. If you access the device, what was being stored on the device, that does not mean—or does it—that once you get into the phone, then you access cloud storage that an individual may have, which, of course, opens up more than a house. That is a whole building full of materials. Is there a limit to this? What are we talking about?

Ms. DONOHUE. For ICE there is not. For CBP it is in their regulations. As of January of this year, they now say that you have to put the phone in airplane mode while you are examining it. But that has been as a regulatory matter, not as a statutory one.

Senator PETERS. That is back to your point, that we are counting on them to do that, and it would be better for us to look at that legislatively to prevent that from happening. ICE does not have to do that, though.

Ms. DONOHUE. Right, ICE has no limits in their regulation on that.

Ms. GULIANI. I think that is part of the problem. We have a CBP policy. It does not extend to all of DHS. So ICE is still bound by its 2009 policy, which has even less protections. Again, I think the cloud issue raises another area where there needs to be more oversight. I am sure you have heard stories, as we have heard, of individuals who say, look, information in the cloud was accessed during these searches, whether that was before the change or after the change, and it certainly is an area where there needs to be more rigorous oversight to ensure that policy is being followed.

Senator PETERS. Mr. Feeney.

Mr. FEENEY. I would only mention, as I mentioned in my remarks, putting a phone into airplane mode is actually not as big a privacy protection as I think a lot of people believe it is. Most of the intimate details on someone's phone are still accessible to a phone in airplane mode, including emails, text messages, browsing histories, and photos.

Senator PETERS. Right. Now, we have been discussing searches right at the port of entry or right at the border, but the Border Pa-

trol is also authorized to set up checkpoints and patrols within 100 miles of international borders and coasts. Being from the State of Michigan, we have a lot of international border, as I mentioned. If you go 100 miles from that border, it is a pretty good chunk of the State. In fact, I think the ACLU says the entire State. I am not sure the geography works for that, but, nevertheless, it is a significant part.

Talk to me a little bit about those authorizations and things that we should be concerned about.

Ms. GULIANI. When it comes to device searches, it has primarily been done at ports of entry. Were CBP to do it in the interior, I think it would be unconstitutional. But I share your concern. I think that we have long been concerned about this 100-mile zone where CBP asserts its authority to conduct stops and to conduct searches without a probable cause warrant.

We have heard stories from individuals who live in that 100-mile zone who report being stopped by officers, undergoing often humiliating experiences, really expressing consternation that they are Americans living in America and they are being subject to this kind of treatment by their own government.

Senator PETERS. Ms. Donohue.

Ms. DONOHUE. Thank you. I would add a couple of things. First is the fleeing felon exception. We all know this is an exception to the warrant requirement for the home, and it goes back centuries, into English law.

Similarly, the way that we have thought about customs border authorities historically through the United States' history has been that as somebody crosses the border, it is almost like the fleeing felon, like you have this extended border as they extend into the interior. The reason for this is because illegal goods put on vehicles or vessels could be transported somewhere else. There is this exception idea that when that item is on that car and it is being shipped somewhere else, that illegal item that is undutied or illegally brought into the United States, then you can chase it. That is a very different determination than whether you can go through somebody's home. I would really distinguish between those two.

In addition, there are special home protections even away from the border. Within those 100 miles, ICE cannot just go onto anybody's farm; they cannot go onto open agriculture land. They need a warrant in order to do so because of the privacies of life, because of what individuals living there would be exposing to the government unwillingly or unwittingly perhaps.

I think on both counts, both in terms of comparing it to the fleeing felon and the reason why we have this customs border exception as well as looking at the protections afforded the home, I think it would be an invalid exercise of the border search authority within that 100 miles.

Senator PETERS. All right. Thank you.

One of the proposals before us includes requirements that the government collect specific statistics about the people whose electronic devices they are searching or seizing, noting age, sex, country of origin, citizenship, or immigration status, ethnicity and race of any traveler subjected to electronic device searches or seizures, as well as the number of travelers whose devices were searched

and seized. I have heard some conflicting opinions about this from folks in Michigan and people representing communities that feel particularly targeted by these practices, with some arguing that knowing these statistics would help identify discrimination, but others arguing that this information could be potentially misused.

My question is: Where do you fall in that debate? Mr. Feeney, from your perspective as a researcher on these issues, what kinds of data should be useful for the government to collect about people stopped, searched, or detained by the Border Patrol? In what instances should that data be collected by the government, if at all?

Mr. FEENEY. I think that DHS should publish not only the number of these searches but also the suspicion they had for the searches. I do not object to the age, citizenship, or—I suppose citizenship status, of course, there is a whole host of data demographics that I do not object to being revealed. I take the point that there is a worry about this data being misused. But the most important data that I would like to see more transparency with is the number of times this authority has actually led to or been involved with cases that have convictions. It is not clear how efficient this authority is. I think it is interesting that when DHS spokespeople have been before committees such as this, they have not been particularly forthcoming about the number of times that this authority—actually, at least convictions, that is the most interesting data point. I would welcome there being more data associated with the citizenship, age, sex of the people affected by these searches, as long as, of course, their names are withheld.

Senator PETERS. Right. Ms. Guliani.

Ms. GULIANI. Similarly, we share your concern that these searches may be used to target people inappropriately. I think data could help to get at that point and reveal the extent to which particular travelers are targeted. But bottom line, the reason we have these concerns, the reason there is this problem is because CBP's policy allows searches either with no suspicion for a basic search or with only reasonable suspicion for advanced searches. What really needs to happen is a warrant requirement so that there is judicial oversight to protect against that type of discriminatory application.

Ms. DONOHUE. I agree with my colleagues, but I would have First Amendment concerns about collecting that kind of information from individual travelers.

I would also like to add on a point that Senator Wyden raised, my concern about a lot of this is it is becoming an end run around the Fourth Amendment, and we actually do have cases on the record where agents have come forward and said, "Yes, I could have actually done something while this person was in the country, but I knew that when they crossed the border, I would have just had much broader powers." They wait for people to travel in order to conduct these searches. I would be interested in the type of information that would reveal that kind of activity, which I think is particularly pernicious and concerning.

In addition, I guess one other thing that I want to mention is the circuits are split right now. We have not had even application of Riley to the border search exception, and so the Eleventh Circuit just issued an opinion where it said that there is no individualized

suspicion required whatsoever at the border. This is not at all a settled issue, and I think it is particularly important for Congress to step forward and weigh in.

Senator PETERS. Right. Well, thank you. I would like to thank our witnesses for your testimony today as well as your work in this very important issue. I think you will find there is quite a bit of interest to Members of this Committee to continue to work with you and to continue to work on this issue.

Seeing no one else here to ask any questions, I am going to close the hearing, and I am going to remind everyone that the record will remain open until July 25 at the close of business for Members to submit additional questions or comments to our witnesses. With that, this hearing is adjourned.

[Whereupon, at 3:36 p.m., the Subcommittee was adjourned.]

APPENDIX

Opening Statement of Chairman Rand Paul, M.D.
Federal Spending Oversight Subcommittee

Examining Warrantless Smartphone Searches at the Border
7/11/2018

I now call to order this hearing of the Senate Homeland Security and Governmental Affairs' Subcommittee on Federal Spending Oversight and Emergency Management.

Today, we'll be discussing the Fourth Amendment's guarantee against unreasonable searches and seizures, and its application to 21st century technology at the U.S. border.

Early last year, reports began to surface about travelers having their phones confiscated and searched by U.S. border authorities, for no obvious reason and without a warrant or even much of an explanation.

These searches have targeted a NASA engineer, a former captain in the U.S. Air Force, a Wall Street Journal reporter, a government security contractor, and numerous other U.S. citizens.

These searches are not just running a phone through an x-ray machine or a metal detector. Customs officials demanded that these travelers unlock their phones so that the contents could be searched. If they refused, these travelers were threatened and interrogated.

One man was handcuffed, while another was physically restrained in a chokehold while government agents picked his phone out of his pocket. Yet another—the NASA engineer—was told that he was "not allowed to leave" until he gave his password to customs officials. Two ironies here: one, the engineer was enrolled in CBP's Trusted Traveler program, which strikes me as false advertising, and two, the phone in question was a government phone.

Some may be asking, what about the 4th Amendment protection against warrantless searches? Does this not extend to U.S. citizens at the border?

Actually, the Courts have held there is something of gray area at the border, which by the way includes international airports and seaports. Customs officials may conduct routine searches of luggage or other containers without a warrant under what some refer to as the "border search exception" to the Fourth Amendment. This so-called exception has historically been used to ensure that no weapons, drugs, or other prohibited items, cargo or persons are entering the country.

I think that most Americans could agree that it's reasonable to let customs officials search suitcases for contraband.

What's unreasonable is that government lawyers want you to believe that there's no difference between a suitcase and a smartphone.

I disagree, and here again, I think most Americans would, too. Physical contraband cannot enter the country unless it is smuggled in, but this is not the case for electronic property.

Anything a border patrol agent could find in the contents of your cell phone could enter the country through the Internet, without the physical phone ever coming close to the U.S.

But it is all the more troubling when you consider what the government is gaining access to. Smartphones can reveal virtually everything about a person—their movements, habits, relationships, health, faith, finances—all in a single, easy-to-search and archive interface. Indeed, I think for many of us today, searching our smartphone would prove to be much more intrusive than even a search of our homes.

This same sentiment has been echoed in recent Supreme Court decisions regarding the Fourth Amendment and digital data. In a unanimous opinion on a 2014 case involving cell phone searches incidental to an arrest, *Riley v. California*, Chief Justice John Roberts writes that "[c]ell phones differ in both a quantitative and qualitative sense" from other objects that a person may possess.

Searching a person's smart phone or other electronic device is fundamentally different than searching their suitcase or their car. And I believe as legal challenges to these searches reach the Supreme Court, they will agree.

We have an esteemed panel of witnesses here today who will discuss the history of border searches, the appropriateness of using this authority to search smartphones, and what actions the Congress should take to address this issue.

At this time, I'd like to recognize Ranking Member Peters for his opening remarks. Senator Peters?

U.S. Senate Homeland Security and Governmental Affairs Committee

Subcommittee on Federal Spending Oversight and Emergency Management

"Examining Warrantless Smartphone Searches at the Border"

July 11, 2018

Senator Gary C. Peters, Ranking Member

Opening Statement

Thank you, Mr. Chairman, for calling today's hearing. I appreciate your continued willingness to work in a bipartisan way to take on tough questions about our core values as Americans, our rights and responsibilities as citizens, and our role in the centuries long fight to ensure equal protection under the law.

The problem we are exploring today requires us to examine detailed policy directives and puzzle over how to apply 18th Century words to 21st Century technology. The details are important, undoubtedly. But at its core, this hearing is about the liberties guaranteed to us by the Constitution. It is about our freedom to travel, our right to be secure against unreasonable search and seizure. It is about our right to be treated equally under the law, without regard to race, national origin, or religion.

The Fourth Amendment states clearly, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

U.S. Customs and Border Protection (CBP) asserts that the Fourth Amendment does not require a CBP officer to obtain a warrant, or even

have individualized suspicion, before searching a smartphone or directing travelers to unlock their devices for official inspection. Today's witnesses, like most of the courts that have considered the question, disagree.

This issue is of particular significance to Michigan. Michigan shares hundreds of miles of international border with Ontario, Canada, including the Ambassador Bridge, one of North America's busiest border crossings. Most importantly, Michigan is home to a large and extraordinarily vibrant and patriotic community of Arab and Muslim-Americans. Community leaders tell me that they feel unfairly targeted by CBP. I have heard countless stories of my constituents, returning from family vacations, medical conferences, work trips—you name it—being singled out for additional screening, being required to turn over phones and computers, provide their passwords, and wait for hours while their devices are searched. Some constituents have reported being asked about their views on politics or foreign affairs.

CBP says that travelers can file complaints if they feel that they have been mistreated. But my constituents fear that complaining will cause further targeting. And who among us—tired from travel and eager to return home to family—wouldn't feel vulnerable in that situation?

One of my constituents described this perceived targeting as a "backdoor travel ban." The fear of unfair treatment and the profound inconvenience of repeated and prolonged searches creates an immense disincentive to travel. It hurts families. It impacts commerce. We have to do better. Under the Constitution, my Arab and Muslim-American constituents are entitled to the same liberty, the same privacy, and the same freedom of movement that I am entitled to.

CBP plays an essential role in securing our border and protecting our national security. It is critical that they have the tools they need to succeed. But it is no less critical that those tools adhere to the Constitution in their design and application, and that no law-abiding American is unfairly singled out.

Just over the last few days, I have received several heartfelt letters describing unfair and unconstitutional treatment and asking for Congressional intervention. Mr. Chairman, I ask that the letters from the Arab American Institute, the Arab-American Civil Rights League, the American-Arab Anti-Discrimination Committee, and the Electronic Privacy Information Center be entered into the record.

Congress should weigh in and establish clear, constitutional rules and a means for ensuring that they are applied equitably. I am grateful that Senator Paul, with Senators Wyden, Leahy, and Daines have taken the lead in identifying a path forward. I hope that this hearing goes a long way in advancing that effort.

I yield back.

SEARCH AND SEIZURE OF ELECTRONIC DEVICES AT THE BORDER*

Laura K. Donohue**

I. INTRODUCTION 1

II. BORDER SEARCH AUTHORITIES RELATED TO CUSTOMS 4
A. Commercial Regulation versus Revenue Generation 5
B. Contraband in the Early American Republic 6
C. Contemporary Search Authorities at Border Crossings 8
D. Mail Search 10
E. Special Protections Afforded the Home 11
F. Extended Border Search and the Functional Equivalent 13
G. Restrictions on Customs Searches: Who and Why 14

III. BORDER SEARCH AUTHORITIES RELATED TO IMMIGRATION 15

IV. BORDER SEARCH OF ELECTRONIC DEVICES 17
A. Not Subject to Reasonable Suspicion 18
B. Supported by Reasonable Suspicion 19
C. Special Protections Extended to Forensic Investigations 19
D. *Riley v. California*: Stronger Constitutional Protections for Mobile Devices 21
E. Impact of *Carpenter v. United States* 23
F. The Problem of Digitization 23

V. CONCLUDING REMARKS 24

I. INTRODUCTION

Border searches of electronic devices are on the rise. In 2015, U.S. Customs and Border Protection (CBP) examined 8,503 devices. The number more than doubled the following year before soaring in 2017 to more than 30,000 searches.[1] U.S. Immigration and Customs Enforcement (ICE), in turn, reported the search of 4,444 cellphone and 320 other electronic devices in 2015.[2] In 2016, ICE eclipsed these numbers, searching 23,000 electronic devices.[3]

Three legal arguments support the examination of travelers' digital data. First, conducted with an eye towards national security, border searches are a concomitant of

---

* This statement is adapted from a draft of an essay that is forthcoming in the *Yale Law Journal Forum*. Preferred Citation: Laura K. Donohue, *Electronic Search and Seizure at the Border*, 128 YALE L.J.F. (forthcoming).

** Agnes N. Williams Research Professor; Director, Center on National Security and the Law; and Director, Center on Privacy & Technology, Georgetown Law.

[1] U.S. Customs & Border Prot., *CBP Releases Statistics on Electronic Device Searches*, CBP (April 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0; *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, CBP (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and; U.S. CUSTOMS & BORDER PROT., BORDER SEARCH OF ELECTRONIC DEVICES, CBP Directive No. 3340-049A (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf [hereinafter CBP DIRECTIVE].

[2] Daniel Victor, *What Are Your Rights if Border Agents Want to Search Your Phone?*, N.Y. TIMES (Feb. 14, 2017), https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html

[3] *Id.*

sovereignty and firmly within Article I and Article II powers.[4] Second, case law and statutory provisions recognize an exception to the warrant requirement and broad powers of search at the border. Further, Congress's power to set the contours stems from the Commerce Clause.[5] Third, as an empirical matter, the actual number of searches taking place is a drop in the sea of international travelers: in 2017, CBP searched fewer than 1/100th of 1% of all travelers (0.007 percent).[6] Weighed against the significant governmental interests at stake (e.g., stopping terrorism, catching individuals involved in human trafficking and child pornography, and preventing individuals involved in international crime from entering the United States), a balancing test favors broad authorities.

Arguments mounted against the government center on the nature of the information that can be obtained. While the law focuses on material goods, such as containers or suitcases,[7] electronic devices contain enormous amounts of information about individuals' private lives. It includes not just data related to the actual crossing, but details that stretch years into the past and generate insight into individuals' relationships, thoughts, and beliefs. As Chief Justice Roberts recognized in *Riley v. California*, mobile devices contain "the privacies of life."[8] In an increasingly globalized world, allowing broad collection powers at the borders allows for an end-run around important Fourth Amendment protections. Beyond this, there are significant implications for citizens' First Amendment rights of association and religion; 5th Amendment due process rights and privilege against self-incrimination; and 6th Amendment right to counsel.

The issue of electronic border search is complicated by parallel incursions by agencies into cloud data, which occurs in one of two ways: by using the device to access information held on the cloud, or by requiring travelers to provide identifiers or handles, or account login credentials (such as usernames and passwords) to access social media. This issue appears to have first presented in December 2016 when CBP started asking

---

[4] *See, e.g.*, CBP Jan. Directive, *supra* note 1, at para. 4 ("The plenary authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty," citing United States v. Flores-Montano, 541 U.S. 149, 153 (2004) in support: "[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting its territorial integrity.") *See also* United States v. Ramsey, 431 U.S. 606, 620 (1977) (stating, "[t]he border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."); *id.* at 616 ("That searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration."); United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."); Torres v. Puerto Rico, 442 U.S. 465, 472–73 (1979) ("The authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity. By reason of that authority, it is entitled to require that whoever seeks entry must establish the right to enter and to bring into the country whatever he may carry.").

[5] *See, e.g.*, United States v. 12 200-Ft. Reels of Film, 413 U.S. 123, 125 (1973) (observing, "searches of persons and packages at the national borders rest on different considerations…from domestic regulations. The Constitution gives Congress broad, comprehensive powers' [t]o regulate commerce with foreign Nations.' Art. I, Sec. 8, cl. 3. Historically, such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry.")

[6] U.S. Customs & Border Prot., *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, CBP (Jan. 5, 2018), www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

[7] Daniel Victor, *Forced Searches of Phones and Laptops at U.S. Border are Illegal, Lawsuit Claims*, N.Y. TIMES (Sept. 13, 2017), https://www.nytimes.com/2017/09/13/technology/aclu-border-patrol-lawsuit.html

[8] Riley v. California, 134 S. Ct. 2473, 2495 (2014).

non-U.S. persons entering the country under the Visa Waiver Program (VWP) to disclose their social media identifiers.[9]

Initially, the program was to be entirely voluntary. With only the provider/platform and social media identifier provided, the government stated that it would only consider publicly-available information. In January 2017, however, the Council on American-Islamic Relations (CAIR) filed complaints with the U.S. Department of Homeland Security, alleging that *U.S. citizens* were being directed to disclose not just their passwords to their phones, but also their social media login information.[10] Media reported that officials were considering new policies to expand CBP scrutiny of cloud content. In February 2017, newly-appointed DHS Secretary John Kelly told a Congressional Committee that the agency might adopt a provision requiring login information from all foreign visa applicants, with the failure to comply resulting in denial of entry. Starting in May 2017, login information became required in cases tied to national security. Less than a year later, in March 2018, the U.S. Department of State submitted a formal proposal to the Office of Management and Budget, requiring that almost all visa applicants list all social media identities used over the previous five years, all telephone numbers, all email addresses, all international travel, all prior immigration violations, and whether specified family members have been involved in terrorist activity.[11] The rule change would allow the government to vet and identify about 14.7 million people per year, searching any social media platforms associated with the individual.[12]

The Executive Branch is divided in how it addresses border search of electronic devices. In January 2018, CBP issued updated guidelines, superseding the previous directive of August 2009.[13] The new document explicitly excluded information held on the cloud from its search provisions.[14] It distinguished between basic and advanced searches (the latter involves connecting external equipment "to an electronic device not merely to gain access…but to review, copy, and/or analyze its contents."[15] Officers must meet a standard of reasonable suspicion or instances "in which there is a national security concern."[16] The equivalent 2009 ICE directive has not been updated since the last review

---

[9] Under the VWP, foreign citizens can visit the U.S. for up to 90 days without a visa, if they have been cleared by the Electronic System for Travel Authorization.

[10] *CAIR-FL files 10 complaints with CBP after the Agency Targeted and Questioned American-Muslims about Religious and Political Views,* CAIR Florida (Jan. 18, 2017), https://www.cairflorida.org/newsroom/press-releases/720-cair-fl-files-10-complaints-with-cbp-after-the-agency-targeted-and-questioned-american-muslims-about-religious-and-political-views.html. *See also* Sophia Cope, *Fear Materialized: Border Agents Demand Social Media Data from Americans,* ELECTRONIC FRONTIER FOUND. (Jan. 25, 2017), https://www.eff.org/deeplinks/2017/01/fear-materialized-border-agents-demand-social-media-data-americans.

[11] U.S. Dep't of State, 83 Fed. Reg. 13807, 13807-13808 (proposed Mar. 30, 2018).

[12] Brendan O'Brien, *U.S. Visa Applicants to be Asked for Social Media History: State Department,* REUTERS (Mar. 29, 2018), https://www.reuters.com/article/us-usa-immigration-visa/u-s-visa-applicants-to-be-asked-for-social-media-history-state-department-idUSKBN1H611P; Matthew Lee, *U.S. to Seek Social Media Details from All Visa Applicants,* BLOOMBERG (Mar. 29, 2018), https://www.bloomberg.com/news/articles/2018-03-29/us-to-seek-social-media-details-from-all-visa-applicants.

[13] CBP DIRECTIVE, *supra* note 1.

[14] *Id.* at para 5.1.2 ("The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted…Officers will themselves disable network connectivity.")

[15] *Id.* at para 5.1.4.

[16] *Id.*

in 2012.[17] Like its CBP counterpart, the directive applies to any item containing electronic or digital information.[18] But unlike its counterpart, it authorizes ICE Special Agents to "search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion."[19] Agents are not required to perform the search in the presence of the owner.[20] Consent is not necessary.[21] In addition, "At any point during a border search, electronic devices, or copies of information therefrom, may be detained for further review either on-site at the place of detention or at an off-site location."[22] Searches can take place up to 30 days after the information is seized, with continuations subject to supervisory approval every 15 days thereafter.[23]

The disjunction we are seeing between CBP and ICE reflect two (historical) streams of border search authorities: customs and immigration.[24] Their objects differ. The first stems from efforts to prevent commercial goods from avoiding duties. The second focuses on individuals: i.e., who should (or should not) be admitted to the country. In the post-9/11 environment, a third, novel approach has steadily entered the legal discussion, seeking to use weaker Fourth Amendment protections at the borders as a way to combat *all* criminal activity. Thus far, the courts have provided a backstop, rejecting some of the more egregious cases to come forward. The lack of legislation is of particular concern, as it leaves citizens' privacy at the mercy of each agency's regulatory regime. The more recent cases of *Riley v. California* and *Carpenter v. United States* herald an evolving Supreme Court doctrine that is cognizant of the greater Fourth Amendment issues at stake in digital information. Further First Amendment, Fifth Amendment, and Sixth Amendment concerns present.

II. BORDER SEARCH AUTHORITIES RELATED TO CUSTOMS

Historically, the Executive Branch has had a wide latitude to conduct searches at the border without first establishing probable cause and obtaining a warrant.[25] That breadth derives in part from the evolution of customs law. During the early colonial period,

---

[17] U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, ICE DIRECTIVE No. 7-6.1: BORDER SEARCHES OF ELECTRONIC DEVICES (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf [hereinafter 2009 ICE DIRECTIVE].

[18] *Compare id.* at para. 5.2 ("Any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices."), *with* CBP DIRECTIVE, *supra* note 1, at para 3.2 ("Any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.")

[19] 2009 ICE DIRECTIVE, *supra* note 17, at para. 6.1.

[20] *Id.* at para 8.1.2.

[21] *Id.* at para 8.1.3.

[22] *Id.* at para 8.1.4.

[23] *Id.* at para 8.3.1.

[24] Certain border search powers also derive from disease monitoring. These areas of law, however, are less relevant to the search of electronic devices and so I do not address them here. For further discussion of the evolution of quarantine authorities, see generally Laura K. Donohue, *Pandemic Disease, Biological Weapons, and War*, in LAW AND WAR 84 (Austin Sarat, Lawrence Douglas & Martha Merrill Umphrey eds. 2014), http://scholarship.law.georgetown.edu/facpub/1296/; Laura K. Donohue, *Biodefense and Constitutional Constraints*, 4 NAT'L SEC. & ARMED CONFLICT. L. REV. 82 (2014), http://scholarship.law.*georgetown*.edu/facpub/677/.

[25] In Stacey v. Emery, the Supreme Court explained the contours of probable cause: 'If the facts and circumstances before the officer are such as to warrant a man of prudence and caution in believing that the offense has been committed, it is sufficient." 97 U. S. 642, 645 (1878). *See also* Locke v. United States, 11 U.S. (7 Cranch) 339 (1813); The George, 10 Fed. Cas. 201 (1815) (No. 5328); The Thompson, 70 U.S. (3 Wall.) 155 (1865).

England considered customs in the context of commercial regulation—an opportunity to ensure dominance in shipping and trade. Over time, and particularly following the Seven Years' War during which England developed substantial debt, the approach shifted to using customs authorities as a way of generating revenue. Officials obtained broad powers to interdict "uncustomed," or illegal materials. Following the American Revolution, the latter emphasis survived, laying the groundwork for today's CBP authorities. This history matters, as it demonstrates both the purposes of customs searches (i.e., to interdict uncustomed materials and so generate revenue), as well as the special protections afforded the home, even where customs issues arise. Both aspects of customs searches serve as a limit on the border search exception.

A. Commercial Regulation versus Revenue Generation

The American colonies provided England with an opportunity to strengthen its global mercantile dominance. From 1621 until 1756, the colonial power thus focused on how to structure its laws to control trade. As early as 1621, the Privy Council recognized the gains at stake, arguing that "the Commodities brought from" the colony of Virginia ought to be "appropriated unto his Majesties subjects" instead of being "communicated to forraine countries."[26] Accordingly, the council adopted an ordinance requiring that "all Tobacco and other commodities" from Virginia "not be carried into any forraine partes until the same have beene first landed here and his Majesties Customes paid therefore."[27]

In the first Navigation Act of 1651, Parliament went on to require that any materials to or from the Americas be carried on English ships.[28] The aim was to prevent European powers from trading with the colonies. Following the Stuart Restoration, in 1660 Parliament passed the second Navigation Act, re-entrenching the rule that colonial trade only be carried out on English vessels: they had to be English-owned, operated by an English master, and carry a crew of which three quarters must be English.[29] The statute did not entirely prevent foreign imports into the colonies—it merely required that they be shipped under English flag. Three years later, Parliament addressed this oversight via the third Navigation Act, requiring that any European commodities bound for the colonies first be taken to England, unloaded, and duties paid, prior to their return to North America.[30] The preamble to the statute underscored the importance of strengthening the connections between England and the colonies, "keeping them in a firmer dependence upon" the Crown, and ensuring that English shipping benefitted.[31] The goal was to establish a monopoly over colonial trade.

The early navigation statutes reflected a fundamentally flawed assumption: namely, that most or all colonial trade involved overseas commerce.[32] In the absence of regulation, intra-colonial trade (not subject to customs duties) began to flourish, with commodities eventually making their way to Europe "to the great Hurt and Diminution of" H.M. Customs and trade.[33] Parliament closed this gap in the Navigation Act of 1673,

---

[26] THOMAS C. BARROW, TRADE & EMPIRE: THE BRITISH CUSTOMS SERVICE IN COLONIAL AMERICA 1660-1775, at 4 (1999).

[27] *Id.*

[28] An Act for Increase of Shipping, and Encouragement of the Navigation of this Nation, (1651) 2 ACTS & ORDS. INTERREGNUM 559-62 (Eng.).

[29] An Act for the Encouraging and Increasing of Shipping and Navigation of 1660, 12 Car. II c. 18 (Eng.) .

[30] An Act for the Encouragement of Trade 1663, 15 Car. II c. 7 (Eng.) .

[31] *Id.*

[32] BARROW, *supra* note 26, at 6.

[33] 9 CALENDAR TREASURY BOOKS 1965 (William A. Shaw eds. 1904), http://www.british-history.ac.uk/search/series/cal-treasury-books [hereinafter C.T.B.] (noting that "[t]he act of 1673 did more to systemize the commercial activities of the colonists than did any other regulation of the navigation acts except the enumeration, of which it was an integral part. It affected not only the commercial relations

requiring that a bond be paid on enumerated items where the ship travelled between plantations.[34] But the enforcement devices were weak. They also differed from those in place in England. In the late 17th century, customs agents could search "any ship, house, or place soever" in London to search for prohibited goods.[35] The Treasurer could provide a warrant to the customs commissions to examine trunks and boxes held at the Custom House in Southampton.[36] There was no equivalent in the new world.

In the 18th Century, Britain tried to tighten its hold, assuming greater powers to search for, and to seize, contraband.[37] Lord Grenville, the First Lord of the Treasury, and Chancellor of the Exchequer, famously considered the colonies to be best source of the revenues needed, charging the colonies with a failure to offset the costs of their own defense.[38] Towards this end, he repeatedly argued in Westminster for more stringent customs enforcement in North America. Many agreed, so when the Molasses Act expired, Parliament passed a measure that emphasized both mercantilism and revenue generation. The preamble to the American Revenue Act of 1764 (a.k.a. the Sugar Act) explained, "[I]t is expedient that new provisions and regulations should be established for improving the revenue of this kingdom, and for extending and securing the navigation and commerce between Great Britain and your Majesty's dominions in America."[39] This statute, along with the Currency Act of 1764 (in which Britain assumed control of the colonial system of currency), laid the groundwork for the revolt that followed the introduction of the Stamp Act of 1765.[40]

B. Contraband in the Early American Republic

Following independence, English mercantile ambitions fell away, but, like England following the Seven Years' War, the United States needed to raise revenue to pay for the recent war. This required efficient enforcement mechanisms. Thus, from the earliest days of the Republic, customs inspectors could board vessels to search for contraband without first obtaining a warrant. To find the same items within a dwelling house, building, or

---

between England and her colonies but also the relations of the colonies among themselves...The new requirement made necessary the installation in colonial ports of a large number of customs officials, whom there had been no need before, appointed after 1696 on the English establishment by the customs commissioners under authority from the Treasury. The business of these officials was to receive, retain, and if necessary prosecute, the bonds in the common law courts and collect the duties, which were supposed to be those of the English book of rates, payable in silver or its equivalent at sterling values. The object of the act was not revenue but the regulation of trade.")

[34] Navigation Act of 1673, 25 Car. II c. 7 (Eng.).

[35] *Compare Entry Book: October 1663*, *in* 1 C.T.B. 547, 550 *with Entry Book: December 1661*, *in* 1 C.T.B. 311, 315 (directing John Seymour and Charles Smith "to search for all wares and merchandize mentioned in the royal proclamation of November 20 last for prohibiting the importation of divers foreign wares and merchandizes into this realm of England and Wales.")

[36] *Entry Book: April 1661*, *in* 1 C.T.B. 232, 236.

[37] GAUTHAM RAO, NATIONAL DUTIES: CUSTOMS HOUSES AND THE MAKING OF THE AMERICAN STATE (2016).

[38] Philip Lawson, *George Grenville and America: The Years of Opposition, 1765-1770*, 37 WM. & MARY Q. 561 (1980).

[39] An act for granting certain duties in the British colonies and plantations in America,; for continuing, amending, and making perpetual, an act passed in the sixth year of the reign of his late majesty King George the Second for applying the produce of such duties, and of the duties to arise by virtue of the said act, towards defraying the expenses of defending, protecting, and securing the said colonies and plantations; for explaining an act made in the twenty fifth year of the reign of King Charles the Second, (intituled, An act for the encouragement of the Greenland and Eastland trades, and for the better securing the plantation trade;) and for altering and disallowing several drawbacks on exports from this kingdom, and more effectually preventing the clandestine conveyance of goods to and from the said colonies and plantation, and improving and securing the trade between the same and Great Britain.

See also FRED ANDERSON, *The American Duties Act (The Sugar Act)*, *in* CRUCIBLE OF WAR: THE SEVEN YEARS' WAR AND THE FATE OF EMPIRE IN BRITISH NORTH AMERICA, 1754-1766, at 572 (2000).

[40] Duties in American Colonies Act 1765, 5 Geo. III c. 12 (Eng.).

other place, customs officers first had to obtain a warrant based upon "cause to suspect."[41]

In 1789, the same year that Congress passed the Bill of Rights to the states for ratification, it enacted statutes setting duties, establishing international ports of entry, requiring vessels to report their contents, and providing for inspectors to board vessels to examine whether the stated goods comported with the items on board.[42] Under the Act of July 31, 1789, officials could board any vessel, "in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed; and therein to search for, seize, and secure any such goods, wares or merchandise."[43] Where suspecting that such materials be concealed in a "dwelling house, store, building, or other place," they could apply to a justice of the peace for a warrant to conduct a search for the goods, "and if any shall be found, to seize and secure the same for trial."[44]

These statutes were followed by statutes in 1790, 1793, and 1799, which underscored the importance of the enforcement of duties.[45] So we find, contemporaneous with the drafting and adoption of the Fourth Amendment, the First, Second, and Fourth Congresses signaling that there was no need to obtain a warrant for goods subject to forfeiture when held in a ship or vessel; however, when held in a warehouse, building, or dwelling, a warrant was required.

Congress continued to follow this line in the Act of July 18, 1866.[46] That statute made it lawful for any customs officer "to go on board of any vessel, as well without as within his district, and to inspect, search, and examine the same, and any person, trunk, or envelope on board, and to this end, to hail and stop such vessel if under way, and to use all necessary force to compel compliance."[47] Where it appeared "that any breach or violation of the laws of the United States [had] been committed" whereby "such vessel,

---

[41] United States v. Ramsey, 431 U.S. 606, 616 (1977).

[42] An Act for laying a Duty on Goods, Wares, and Merchandizes imported into the United States, Act of July 4, 1789, §§ 1, 3, 4, ch. 2, 1 Stat. 24, 24-27 (1789) (setting duties); An Act to regulate the Collection of the Duties imposed by law on the tonnage of ships or vessels, and on goods, wares and merchandises imported into the United States, Act of July 31, 1789, § 1, ch. 5, 1 Stat. 29, 29 (1789) (establishing districts, ports, and officers); §2 (establishing ports for non-U.S. vessels); *id.* §4 (requiring master or commander of every ship or vessel to provide "a true manifest of the cargo on board such ship or vessel"); *id.* §5 (empowering inspection of the vessels "to examine whether the goods imported are conformable to the entries thereof."); *id.* §10 (requiring that the master or commander of the vessel provide the manifest to the inspector with "a true account of the loading which such ship or vessel had on board at the port from which she last sailed, and at the time of her sailing, or at any time since, the packages, marks and numbers, and noting thereon to what port in the United Stats such ship or vessel is bound, and the name or names of the person or persons to whom the goods are consigned, or in cases where the goods are shipped to order, the names of the shippers."); *id.* §12 (prohibiting any goods, wares, or merchandise from being unladen or delivered from any ship or vessel at night or without a permit from the collector); An Act for Registering and Clearing Vessels, Regulating the Coasting Trade, and for other purposes, Sept. 1, 1789, § 3, ch. 11, 1 Stat. 55, 55-56 (1789) (empowering the surveyor to measure every vessel to ascertain its tonnage); An Act to suspend part of an Act, intitled 'An Act to regulate the collection of the Duties imposed by Law on the Tonnage of Ships or Vessels, and on Goods, Wares, and Merchandises, imported into the United States,' Sept. 16, 1789, §3, ch. 15, 1 Stat. 69, 69-70 (1789) (setting duties on certain foreign goods).

[43] Act of July 31, 1789, ch. 5, §§ 24, 36, 1 Stat. 29, 43, 47. (1789) (current version codified at 19 U.S.C §§ 482, 1582).

[44] *Id.*

[45] Act of Aug. 4, 1790, ch. 35, §§ 48–51, 1 Stat. 145, 170 (1790); Act of February 18, 1793, ch. 8, §27, 1 Stat. 305, 315 (1793); Act of March 2, 1799, ch. 22, §§ 68–71, 1 Stat. 627, 677, 678 (1799). *See also* Montoya de Hernandez, 473 U.S. at 537 (noting that Congress has always provided the Executive with plenary power to search and seize at the border, absent probable cause or a warrant to regulate duties/prevent introduction of contraband). *See also* An Act further to regulate the entry of merchandise imported into the United States from any adjacent territory, Mar. 2, 1821, ch. 14, 3 Stat. 616.

[46] An Act further to prevent Smuggling and for other Purposes, Act of July 18, 1866, ch. 201, 14 Stat. 178.

[47] *Id.* § 2.

or the goods, wares, and merchandise, or any part thereof, on board of or imported by such vessel, is or are liable to forfeiture," then the customs officer had the authority to seize the items.[48] The statute also empowered officers to "arrest any person engaged in such breach or violation" and to pursue and arrest anyone who tried to escape.[49] The officers could stop, search, and examine "any vehicle, beast, or person on which or whom he or they shall suspect there are goods, wares, or merchandise which are subject to duty or shall have been introduced into the United States in any matter contrary to law."[50] The statute reflected the importance of securing *things* to demonstrate the illegal movement of uncustomed goods—namely, the vehicle, beast, "goods, wares, merchandize, and all other appurtenances, including trunks, envelopes, covers, and all means of concealment, and all the equipage, trappings, or other appurtenances of such beast."[51]

C. Contemporary Search Authorities at Border Crossings

In 1930, the (ill-fated) Smoot-Hawley Tariff Act significantly increased tariffs on agricultural and industrial goods.[52] Eight years later, an amendment to the act also provided for special inspection, examination, and search authorities.[53] As subsequently amended, the law now reads:

> Whenever a vessel from a foreign port or place or from a port or place in any Territory or possession of the United States arrives at a port or place in the United States or the Virgin Islands, whether directly or via another port or place in the United States or the Virgin Islands, the appropriate customs officer for such port or place of arrival may, under such regulations as the Secretary of the Treasury may prescribe and for the purpose of assuring compliance with any law, regulation, or instruction which the Secretary of the Treasury or the Customs Service is authorized to enforce, cause inspection, examination, and search to be made of the persons, baggage, and merchandise discharged or unladen from such vessel, whether or not any or all such persons, baggage, or merchandise has previously been inspected, examined, or searched by officers of the customs.[54]

The law empowers customs officers, at any time, to board any vessel or vehicle,

> within a customs-enforcement area established under the Anti-Smuggling Act [19 U.S.C. 1701 et seq.], or at any other authorized place, without as well as within his district, and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any

---

[48] *Id.*
[49] *Id.*
[50] *Id.* § 3.
[51] *Id.*
[52] Tariff Act of 1930, ch. 497, 46 Stat. 590 (codified at 19 U.S.C. ch. 4). *See also* Robert Whaples, *Where Is There Consensus Among American Economic Historians? The Results of a Survey on Forty Propositions*, 55 J. ECON. HIST. 139, 151 (1995) (finding consensus among economic historians that the Act "exacerbated the Great Depression.")
[53] Customs Administrative Act of 1938, ch. 679, 52 Stat. 1077, 1083 (codified as amended at 19 U.S.C.A. § 1467).
[54] 19 U.S.C. § 1467. *See also* 19 U.S.C. § 1496 ("The appropriate customs officer may cause an examination to be made of the baggage of any person arriving in the United States in order to ascertain what articles are contained therein and whether subject to duty, free of duty, or prohibited notwithstanding a declaration and entry therefor has been made."); 19 U.S.C. § 1499 (providing for entry examination of imported merchandise).

> person, trunk, package, or cargo on board, and to this end may hail and stop such vessel or vehicle, and use all necessary force to compel compliance.[55]

The Secretary of the Treasury may issue regulations for searching persons and baggage.[56] Further, "he is authorized to employ female inspectors for the examination and search of persons of their own sex; and all persons coming into the United States from foreign countries shall be liable to detention and search by authorized officers or agents of the Government under such regulations."[57] The border exception applies both to ingress and egress to and from the United States.[58]

The level of suspicion required to search travelers for illegal goods as they cross the border increases as the search becomes more intrusive. Courts, for instance, do not require particularized suspicion for the contents of a traveler's briefcase, luggage, purse, or pockets.[59] Nor is it required for documents contained within containers in such items.[60] Pictures, films and other graphic materials do not earn any higher level of protection.[61] A pat-down warrants "minimal suspicion."[62]

In contrast, the search of a travelers' undergarments and strip searches require "real suspicion."[63] The only context thus far recognized by the Supreme Court as requiring individualized suspicion is related to the intimate physical search of a woman believed to be smuggling drugs in her alimentary canal.[64] In the 1985 case *United States v. Montoya de Hernandez*, customs officials suspected that a woman had swallowed balloons containing drugs.[65] The Supreme Court determined that reasonable suspicion was required to detain the individual until the drugs had passed.[66] This decision followed on a series of lower court cases rejecting mere suspicion for intrusive body searches, requiring a "clear indication" or "plain suggestion" of criminal activity.[67]

---

[55] 19 U.S.C. § 1581(a).

[56] 19 U.S.C. § 1582. Implementing regulations can be found at 19 C.F.R. §§ 23.1, 23.5, 23.11.

[57] *Id. See* Tariff Act of 1930, ch. 497, § 582, 46 Stat. 590, 748.

[58] *United States v. Oriakhi*, 57 F.3d 1290 (4th Cir. 1995).

[59] *See, e.g.*, United States v. Tsai, 282 F.3d 690, 696 (9th Cir. 2002); Henderson v. United States,390 F.2d 805, 808 (9th Cir. 1967). But note that suspicion cannot be based merely on ancestry as a basis for detention and questioning. See United States v. Brignoni-Ponce, 422 U.S. 873 (1975).

[60] *See* United States v. Grayson, 597 F.2d 1225, 1228–29 (9th Cir.1979).

[61] United States v. Thirty–Seven Photographs, 402 U.S. 363, 376 (1971).

[62] *See, e.g.*, People of the Territory of Guam v. Sugiyama, 846 F.2d 570, 572 (9th Cir. 1988) (pat-down appropriate when suspect known to be connected to packages of marijuana previously sent to airport); United States v. Des Jardins, 747 F.2d 499, 504-05 (9th Cir.1984), *vacated in part*, 772 F.2d 578 (9th Cir. 1985) (pat-down justified when objects frequently used in narcotics smuggling found in the traveler's suitcase); United States v. Quintero-Castro, 705 F.2d 1099, 110-01 (9th Cir. 1983) (pat-down appropriate where traveler paid cash for the ticket, appeared nervous, and story conflicted with co-traveler); United States v. Carter, 563 F.2d 1360, 1361 (9th Cir. 1977) (pat-down appropriate when traveler appeared nervous and did not directly answer questions about trip); United States v. Rivera-Marquez, 519 F.2d 1227, 1228 (9th Cir. 1975) (pat-down appropriate when informer told agents that individual with traveler's name would be smuggling drugs on that day). *See also* United States v. Romero, 71 F. Supp.2d 1021 (N.D. Cal. 1999) (pat-down of traveler did not meet the minimal suspicion standard).

[63] *Des Jardins*, 747 F.2d at 505; United States v. Couch, 688 F.2d 599, 604 (9th Cir. 1982); United States v. Guadalupe-Garza, 421 F.2d 876 (9th Cir. 1970).

[64] United States v. Montoya de Hernandez, 473 U.S. 531 (1985).

[65] *Id.*

[66] *Id.*

[67] *See, e.g.*, United States v. Vance, 62 F.3d 1152 (9th Cir. 1995) (holding "real suspicion" was present when Mr. Vance, traveling from Hawaii to Guam, underwent a pat-down search). In that case, a customs officer observed that the traveler was glassy-eyed, disoriented, and had trouble answering questions. A pat-down revealed two pairs of underwear and a bulge at the traveler's crotch. When directed to drop his underwear, two packs of methamphetamine fell out.

Vehicles are subject to a much less rigorous standard than searches of the person. In *United States v. Flores-Montano*, for instance, reasonable suspicion was considered sufficient for removing a gas tank to search for contraband.[68] The Supreme Court, however, has held open the possibility "that some searches of *property* are so destructive as to require" particularized suspicion.[69]

D. Mail Search

Customs officers, by statute, have the authority to stop and to search domestic mail headed outside the United States, as well as foreign mail transiting the United States.[70] The law is specifically tied to six areas: exportation or importation of monetary instruments;[71] material related to obscenity or child pornography;[72] controlled substances;[73] nuclear materials covered by the Export Administration Act;[74] defense articles and services;[75] and emergency matters that fall within the International Emergency Economic Powers Act, such as foreign exchange, transfers of credit or payments, or the import or export of currency or securities.[76] Mail that has not been sealed against inspection, and to which the sender or addressee has consented a search, can be examined.[77] Mail weighing more than 16 ounces that has been sealed against inspection can only be opened and searched by a customs officer where there is reasonable grounds to suspect that it contains monetary instruments, a weapon of mass destruction, or material related to one of the six categories listed above.[78] The law explicitly forbids reading any correspondence contained in mail sealed against inspection absent consent by the sender or addressee, or a search warrant obtained consistent with rule 41 of the Federal Rules of Criminal Procedure.[79] Customs officers do not have the authority to open and inspect mail weighing 16 ounces or less.[80]

A different provision in the code, whose origins stem from 19th century statutes, deals specifically with opening trunks or envelopes.[81] The standard it sets is "reasonable cause." The statutory language reads:

> Any of the officers or persons authorized to board or search vessels may search any trunk or envelope, wherever found, in which he may have a reasonable cause to suspect there is merchandise which was imported contrary to law.[82]

---

[68] United States v. Flores-Montano, 541 U.S. 149 (2004). In this case, the Ninth Circuit had taken the term "routine" from United States v. Montoya de Hernandez, created a balancing test, and applied it to vehicle searches. The Supreme Court objected, determining that searches of vehicles were subject to a much less rigorous standard than searches of the person. The 9th circuit went on in United States v. Chaudhry, 424 F.3d 1051, 1054 (9th Cir. 2005) to find the distinction between "routine" and "non-routine" inapplicable to searches of property.

[69] Flores-Montano at 155–56, 124 S. Ct. 1582 (holding that complete disassembly and reassembly of a car gas tank did not require particularized suspicion.)

[70] 19 U.S.C. § 1583.

[71] 31 U.S.C. § 5316.

[72] 18 U.S.C. §§ 1461, 1463, 1465, and 1466.

[73] 21 U.S.C. § 953.

[74] 50 U.S.C. §§ App. 2401 et seq.

[75] 22 U.S.C. § 2778.

[76] 50 U.S.C. §§ 1701, 1702 et seq.

[77] 19 U.S.C. § 1583(b).

[78] *Id.* § 1583(c)(1).

[79] *Id.* § 1583(c)(2).

[80] *Id.* § 1583(d).

[81] *Id.* § 482 (re-codified Rev. Stat.§3061, which derived from the Act of July 18, 1866, ch. § 3, 14 Stat. 178, 178.)

The Supreme Court has noted that the "reasonable cause to suspect" test presents "a less stringent requirement than that of 'probable cause' imposed by the Fourth Amendment as a requirement for the issuance of warrants."[83] The Court has upheld this test as applied to border searches as constitutional.[84]

E. Special Protections Afforded the Home

As the Supreme Court noted in 1977, "[A] port of entry is not a traveler's home."[85] For the latter, as a matter of law, for centuries special protections have applied. From the time of Coke's *Institutes* (and, arguably, Magna Carta) forward, outside of a fleeing felon or the hue and cry, common law forbade access to the home absent a warrant.[86] The need for such a document pushed on what, precisely would satisfy the requirement. As the Crown made increasing use of general warrants, treatise writers and jurists roundly condemned the practice as unreasonable—i.e., against the Reason of the common law.[87] Only particular warrants, issued by a magistrate, naming the individual, establishing probable cause for a specific crime, and supported by oath or affirmation, met the standard.[88] The U.S. founders incorporated this common law rule into the Bill of Rights:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[89]

It is important here to remember the mere evidence rule, which similarly continued the common law tradition and did not fall out of favor in the United States until 1967, just a few months prior to *Katz v. United States*.[90] This rule made it clear that even with a particularized warrant, there were certain things that the government could not obtain because it interfered with the privacies of life. The court thus drew a distinction between the fruits and instrumentalities of crime, on the one hand, and other types of materials. In *Boyd v. United States*, Justice Bradley explained for the Court,

> The search for and seizure of stolen or forfeited goods, or goods liable to duties and concealed to avoid the payment thereof, are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him. The two things differ *toto coelo*. In the one case, the government is entitled to the possession of the property; in the other it is not.[91]

This distinction reflects in the customs law tradition:

---

[82] *Id.* § 482.
[83] United States v. Ramsey, 431 U.S. 606, 612 (1977).
[84] *Id.*
[85] *Id.* at 618 (1980 (quoting United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971)).
[86] Laura K. Donohue, *The Original Fourth Amendment*, 83 CHI. L. REV. 1181 (2016).
[87] *Id.*
[88] *Id.*
[89] U.S. CONST. amend IV.
[90] Katz v. United States, 389 U.S. 347 (1967).
[91] Boyd v. United States, 116 U.S. 616, 623 (1886).

> The seizure of stolen goods is authorized by the common law; and the seizure of goods forfeited for a breach of the revenue laws, or concealed to avoid the duties payable on them, has been authorized by English statutes for at least two centuries past; and the like seizures have been authorized by our own revenue acts from the commencement of the government. The first statute passed by Congress to regulate the collection of duties, the Act of July 31, 1789, 1 Stat. 29, 43, contains provisions to this effect. As this act was passed by the same Congress which proposed for adoption the original amendments to the Constitution, it is clear that the members of that body did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the amendment....So, also, the laws which provide for the search and seizure of articles and things which it is unlawful for a person to have in his possession for the purpose of issue or disposition, such as counterfeit coin, lottery tickets, implements of gambling, etc., are not within this category. Many other things of this character might be enumerated.[92]

In other words, Congress (and the Courts) drew a clear distinction between a store or dwelling house, or other structure for which a proper warrant was required, and the search of a ship, motorboat, wagon, or automobile, where it was not practicable to obtain a warrant because the vehicle could be quickly moved. Thus, under the Act of March 3, 1815, it was not only lawful to board and search vessels within the customs' officers' districts and those adjoining, but also to stop and search any vehicle, beast, or person for whom there was probable cause to believe unlawful goods had unlawfully been brought into the United States.[93] The Court, and the government, considered it a valid exercise of constitutional power.[94] To the extent that a question of distance from the border arose, in the 19th century, the Attorney general drew the line at three miles.[95]

In this way, the border exception bore a striking resemblance to the fleeing felon exception: it was only in the process of hot pursuit of goods illegally brought into the country that broader powers applied. But limits applied:

> It would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor, and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search. 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

---

[92] *Id.* at 623-24 (internal citations omitted).

[93] Act of Mar. 3, 1815, ch. 94, 3 Stat. 231, 232. For total or partial renewals of the statute, see Act of Apr. 27, 1816, ch. 110, 3 Stat. 315; Act of Feb. 28, 1865, ch. 67, 13 Stat. 441; Act of July 18, 1866, c. 201, 14 Stat. 178; section 3061 of the Revised Statutes.

[94] Cotzhausen v. Nazro, 107 U.S. 215 (1883). *See also* United States v. One Black Horse, 129 F. 167 (D. Me. 1904). Similar provisions applied to Indian agents who, suspecting the introduction of alcohol, could cause the boats, stores, packages, wagons, sleds, and places of deposit of such person to be searched and seized. Rev. Stat. § 2140 (1875). This power arose from an 1822 statute, which allowed for traders' goods to be searched/seized on basis of suspicion of alcohol (Act of May 6, 1822, ch. 58, 3 Stat. 682), as well as the Act of June 30, 1834, § 20, ch. 161, 4 Stat. 729, 732. The Supreme Court recognized the Statute of 1822 as sufficient for search and seizure in American Fur Co. v. United States, 27 U.S. (2 Pet.) 358. All statutes cited and discussed in Carroll v. United States, 267 U.S. 132 (1925).

[95] Section 174 of Act of Mar. 3, 1899, ch. 429, 30 Stat. 1254, 1280. The Attorney General, construing the Act, wrote, "If your agents reasonably suspect that a violation of law has occurred, in my opinion they have power to search any vessel within the three-mile limit according to the practice of customs officers when acting under section 3059 of the Revised Statutes [Comp. St. § 5761], and to seize such vessels.' 26 Op. Attys. Gen. 243. Cited and quoted in *Carroll*, 267 U.S. at 153.

> may be lawfully brought in. But those lawfully within the country, entitled to use the public highways, have a right to free passage without interruption or search unless there is known to a competent official, authorized to search, probable cause for believing that their vehicles are carrying contraband or illegal merchandise.[96]

In *Carroll v. United States*, the Court noted the necessity of establishing probable cause of a felony for a search that occurred away from the border. The border was only relevant insofar as it helped to establish probable cause.[97]

Reflecting these traditions, the current state of play, as both a statutory and a doctrinal matter, is that customs searches of homes require a warrant, issued by a third party federal judge or magistrate, and supported by probable cause that merchandise has been illegally brought into the United States, or that the goods in question are subject to forfeiture.[98] The search of vehicles or vessels, however, is not limited to the time and place of actual international crossings.[99]

F. Extended Border Search and the Functional Equivalent

For searches away from ports of entry, courts look at whether such actions can be upheld as "extended border searches" as well as whether they take place at the "functional equivalent" of the border.[100] Airports, for instance, are considered the functional equivalent of the border.[101] The validity of such searches depends upon a variety of factors, suggesting a totality of circumstances test. As with searches at the actual border, the Fourth Amendment standard of "reasonableness" still applies; however, mere suspicion is sufficient.[102]

---

[96] *Carroll*, 267 U.S. at 153-54.

[97] *Id.*, at 160.

[98] 19 U.S.C. § 1595.

[99] *Id.* § 482: "(a) Any of the officers or persons authorized to board or search vessels may stop, search, and examine, as well without as within their respective districts, any vehicle, beast, or person, on which or whom he or they shall suspect there is merchandise which is subject to duty, or shall have been introduced into the United States in any manner contrary to law, whether by the person in possession or charge, or by, in, or upon such vehicle or beast, or otherwise, and to search any trunk or envelope, wherever found, in which he may have a reasonable cause to suspect there is merchandise which was imported contrary to law; and if any such officer or other person so authorized shall find any merchandise on or about any such vehicle, beast, or person, or in any such trunk or envelope, which he shall have reasonable cause to believe is subject to duty, or to have been unlawfully introduced into the United States, whether by the person in possession or charge, or by, in, or upon such vehicle, beast, or otherwise, he shall seize and secure the same for trial. (b) Any officer or employee of the United States conducting a search of a person pursuant to subsection (a) of this section shall not be held liable for any civil damages as a result of such search if the officer or employee performed the search in good faith and used reasonable means while effectuating such search." This section dates back to Act of March 3, 1815, ch. 94, 3 Stat. 231, 232; Act of July 18, 1866, ch. 201, 14 Stat. 178.

[100] United States v. Carter, 760 F.2d 1568 (11th Cir. 1985); Torres v. Puerto Rico, 442 U.S. 465 (1979) (Search of individual arriving in Commonwealth of Puerto Rico from the United States not satisfied because no functional equivalent to international border of the United States)

[101] Almeida–Sanchez v. United States, 413 U.S. 266, 273 (1973) ("For ... example, a search of the passengers and cargo of an airplane arriving at a St. Louis airport after a non-stop flight from Mexico City would clearly be the functional equivalent of a border search.").

[102] Alexander v. United States, 362 F.2d 379 (9th Cir. 1966) (citing Cervantes v. United States, 263 F.2d 800, 803, n. 5 (9th Cir. 1959); Carroll v. United States, 267 U.S. 132, 154, (1925); Boyd v. United States, 116 U.S. 616, 623, (1886); Hammond v. United States, 356 F.2d 931 (9th Cir. 1966); King v. United States, 348 F.2d 814, 817 (9th Cir. 1965); Jones v. United States, 326 F.2d 124, 130 (9th Cir. 1964, Duniway, J., concurring); Denton v. United States, 310 F.2d 129 (9th Cir. 1962); Mansfield v. United States, 308 F.2d 221 (5th Cir. 1962); Plazola v. United States, 291 F.2d 56 (9th Cir. 1961); Witt v. United States, 287 F.2d 389 (9th Cir. 1961); Murgia v. United States, 285 F.2d 14 (9th Cir. 1960); Landau v. United States Attorney, 82

In cases of continuous surveillance of vehicles transiting the border, the lower courts have upheld searches 20 miles from the border that occur 15 hours after entry.[103] On the other hand, for roving searches, the Supreme Court has held that a warrantless search, 25 miles north of the border, on an East-West Highway located at all points at least 20 miles from border, absent probable cause and reasonable suspicion, was invalid.[104] There is no border exception outside the actual border or its functional equivalent.[105]

G. Restrictions on Customs Searches: Who and Why

The Courts have held that an "officer of the customs" includes customs officers, inspectors, investigators, and mail entry aids, certain Immigration and Naturalization Service officials (e.g., border patrol agents), and Coast guard officers.[106] It has also included a doctor aiding a customs search. The right to undertake border searches *does not extend to the FBI or to law enforcement when acting for general law enforcement purposes.* Thus, In the 1979 case of *United States v. Vidal Soto-Soto*, the 9th Circuit considered the FBI's warrantless search of a Chevrolet pickup truck at the border to determine whether it had been stolen.[107] The agent's sole basis for stopping the truck was due to the make and model of the vehicle.[108] The Court looked to the Supreme Court's recent decision in *Delaware v. Prouse*, in which it had required articulable and

---

F.2d 285 (2nd Cir. 1936); United States v. Wischerth, 68 F.2d 161 (2d Cir. 1933); United States v. Yee Ngee How, 105 F. Supp. 517 (N.D. Cal. 1952).

[103] *See, e.g.*, King v. United States 348 F.2d 814 (9th Cir. 1965), *cert. denied*, 382 US 926 (customs agent, based on a tip, followed car at Tijuana crossing); Leeks v. United States, 356 F.2d 470 (9th Cir. 1966) (upholding search 15 miles north of San Ysidro border entry, continuous tailing); Alexander v. United States 362 F.2d 379 (9th Cir. 1966), *cert. denied*, 385 U.S. 977 (heroin discovered after placing vehicle crossing into Arizona after surveillance, with only a one or two minute break, reasoning that by statute customs officers had long had the express authority to stop, search, examine vehicles suspected of carrying merchandise subject to duty, making it possible for them to do what would be "unreasonable" for police, supported by courts, use a totality of the circumstances—e.g., time, distance, manner and extent of surveillance, etc.); Lee v. United States 376 F2d 98 (9th Cir. 1967), *cert. denied*, 389 U.S. 837 (customs agent acting on tip placed car from Mexico under surveillance, arrested and found narcotics—upheld because continuously under surveillance); Rodriguez-Gonzalez v. United States 378 F2d 256 (9th Cir. 1967) (mere suspicion acceptable for search that took place 15 hours and 20 miles from the border found marijuana hidden in rear door; met totality of the circumstances test—time and distance, extent and manner; constant surveillance until car stopped a few miles north of San Diego); Gonzalez-Alonso v. United States 379 F.2d 347 (9th Cir. 1967) (marijuana; followed from border, stopped and searched 11 miles inland, found valid, applying totality of the circumstances test); Bloomer v. United States 409 F.2d 869 (9th Cir. 1969) (Oldsmobile with marijuana under constant surveillance from time it crossed the border).

[104] Almeida-Sanchez v. United States, 413 U.S. 266 (1973). In *Almeida-Sanchez*, a Mexican citizen with a valid U.S. work permit was convicted for possession and transfer of marijuana following a warrantless search of his automobile. 413 U.S. at 267. The government argued that the Immigration and Nationality Act, which provided for warrantless searches "within a reasonable distance [defined by regulations as 100 air miles] from any external boundary" authorized the search. Immigration and Nationality Act, § 287(a)(3), codified at 8 U.S.C.A. § 1357(a). *See also* 8 C.F.R. § 287.1 (cited in *Almeida-Sanchez*, 413 U.S. at 268. In a 5-4 opinion, the Supreme Court ruled that the statute and regulation were inconsistent with the Fourth Amendment. While border searches could take place at functional equivalent of the border, searches within 100 miles of the border violated the reasonableness clause. The Court also held that the search could not be justified on the basis of the rules applied to search of automobiles. In Carroll v. United States, the Court had upheld the clause in the Volstead Act that allowed for warrantless search of automobiles where probable cause existed that the vehicle in question contained illegal alcoholic beverages. 267 U.S. 132 (1925). In this case, however, the standard of probable cause had not been met.

[105] United States v. Ortiz, 422 U.S. 891 (1975).

[106] *See also* 19 U.S.C.A. § 1401(i).

[107] United States v. Vidal Soto-Soto, 598 F.2d 545, 546 (9th Cir. 1979).

[108] *Id.*

reasonable suspicion that a motorist was unlicensed or an automobile not registered, to detain a vehicle and request the registration papers.[109]

The reason for the broader authority granted to customs officers than to ordinary law enforcement is because the basic purpose behind a border search is *to obtain things illegally brought into the country*. As the 9th circuit noted, "Validity for this distinction is found in the fact that the primordial purpose of a search by customs officers is not to apprehend persons, but to seize contraband property unlawfully imported or brought into the United States."[110] The Court observed, "The authorization of section 581 (19 USC §1581) is to ascertain whether there are any dutiable articles concealed in the vessel; it is not to discover acts of criminality. If by chance contraband merchandise or dutiable articles are discovered, then the Coast Guard officer must arrest any person connected with the smuggling of such merchandise."[111] The purpose is "to effectuate the provisions of the navigation and tariff laws and to protect the revenue of the United States, Congress, by section 581 of the Tariff Act 1930."[112] The purpose of customs law is not to deter criminal activity writ large.[113]

III. BORDER SEARCH AUTHORITIES RELATED TO IMMIGRATION

Immigration law has a considerably different history and appears in a different area of the code. This history sheds light on the differences between CBP and ICE in terms of their regulations. It is also a doctrine fraught with contradictions.

On the one hand, more than a century ago the plenary power doctrine emerged, rejecting any constitutional challenge to Congress's initial immigration laws.[114] In *Chae Chan Ping v. United States*, the Court stated that although the Constitution did not explicitly address immigration, Congress had the general power to pass a statute amending prior Treaties and excluding Chinese citizens.[115] Justice Field, writing for the Court, said, "The question whether our government is justified in disregarding its engagements with another nation is not one for the determination of courts."[116] The decision fell to the political branches, rendering any judicial "reflection upon [Congress's] motives, or the motives of any of its members," immaterial.[117]

> That the government of the United States, through the action of the legislative department, can exclude aliens from its territory is a proposition which we do not think open to controversy. Jurisdiction over its own territory to that extent is an incident of every independent nation. It is a part of its independence. If it could not exclude aliens it would be to that extent subject to the control of another power.[118]

---

[109] Delaware v. Prouse, 440 U.S. 648 (1979).
[110] Alexander v. United States, 362 F.2d 379, 382 (1966). *See also* The Atlantic. Olson v. United States, 68 F.2d 8 (2d Cir. 1933).
[111] *Atlantic. Olson*, 68 at 9.
[112] *Id.* at 10.
[113] But note that seizure may rest on a violation of criminal law. *See* Maul v. United States, 274 U.S. 501 (1927); Wood v. United States, 41 U.S. 342 (1842); Awalt v. United States, 47 F.2d 477 (3d Cir. 1931).
[114] Chae Chan Ping v. United States, 130 U.S. 581 (1889). *See also* Hiroshi Motomura, *Immigration Law After a Century of Plenary Power: Phantom Constitutional Norms and Statutory Interpretation*, 100 YALE L. J. 545 (1990).
[115] *Id.*; An act to Execute Certain Treaty Stipulations Relating to Chinese, May 6, 1882, ch. 1, 22 Stat. 58.
[116] *Id.* at 602.
[117] *Id.* (citing Taylor v. Morton, 23 F. Cas. 784 (C.C.D. Mass. 1855), *aff'd*, 67 U.S. 481 (1862)).
[118] *Id.* at 603-604.

Such authority was part of the foreign affairs power of any country, found in the interstices of Article I(8) and Article II.[119]

Over time, however, the rule that the executive branch and Congress have absolute authority over immigration decisions has eroded.[120] Thus, while entry without the appropriate status may be unlawful, the Supreme Court has held that a child's immigration status cannot impact their access to public elementary and secondary education.[121] Professor Hiroshi Motomura has argued that the gap between the Court and the dissent in that case stems from disparate views of immigration outside legal constraints: namely, a contribution to the economy and society, versus "egregious lawbreaking."[122] Further complicating the debate is the role of states and cities, as well as how (and whether) to integrate unlawful immigrants—including and up to providing a path to formal citizenship.[123]

Questions of individual rights have gained ground. U.S. citizens, and individuals with a substantial connection to the United States, benefit from the protections of the Fourth Amendment.[124] Non-U.S. persons, however, have no such rights. Immigration officials thus have much broader authorities as to aliens. As a matter of statutory law,

> Any officer or employee of the Service authorized under regulations prescribed by the Attorney General shall have power without warrant—
>
> (1) to interrogate any alien or person believed to be an alien as to his right to be or to remain in the United States;
>
> (2) to arrest any alien who in his presence or view is entering or attempting to enter the United States in violation of any law or regulation made in pursuance of law regulating the admission, exclusion, expulsion, or removal of aliens, or to arrest any alien in the United States, if he has reason to believe that the alien so arrested is in the United States in violation of any such law or regulation and is likely to escape before a warrant can be obtained for his arrest, but the alien arrested shall be taken without unnecessary delay for examination before an officer of the Service having authority to examine aliens as to their right to enter or remain in the United States;
>
> (3) within a reasonable distance from any external boundary of the United States, to board and search for aliens any vessel within the territorial waters of the United States and any railway car, aircraft, conveyance, or vehicle, and within a distance of twenty-five miles from any such external boundary to have access to private lands, but not dwellings, for the purpose of patrolling the border to prevent the illegal entry of aliens into the United States;

---

[119] *Id.* at 604. ("The powers to declare war, make treaties, suppress insurrection, repel invasion, regulate foreign commerce, secure republican governments to the states, and admit subjects of other nations to citizenship, are all sovereign powers, restricted in their exercise only by the constitution itself and considerations of public policy and justice which control, more or less, the conduct of all civilized nations").

[120] *See id.* at 549 ("Immigration law, as it has developed over the past one hundred years under the domination of the plenary power doctrine, represents an aberrational form of the typical relationship between statutory interpretation and constitutional law. The aberrant quality is attributable to the prolonged nature of the contradiction between these two sets of "constitutional" norms in immigration law. The constitutional norms that courts use when they directly decide constitutional issues in immigration cases are not the same constitutional norms that inform interpretation of immigration statutes. To serve the latter function, many courts have relied on what I call "phantom constitutional norms," which are not indigenous to immigration law but come from mainstream public law instead. The result has been to undermine the plenary power doctrine through statutory interpretation.) (internal citations omitted)

[121] Plyler v. Doe, 457 U.S. 202 (1982).

[122] Hiroshi Motomura, *Immigration Outside the Law*, 108 COLUM. L. REV. 2037 (2008).

[123] *Id.*

[124] United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

> (4) to make arrests for felonies which have been committed and which are cognizable under any law of the United States regulating the admission, exclusion, expulsion, or removal of aliens, if he has reason to believe that the person so arrested is guilty of such felony and if there is likelihood of the person escaping before a warrant can be obtained for his arrest, but the person arrested shall be taken without unnecessary delay before the nearest available officer empowered to commit persons charged with offenses against the laws of the United States; and
>
> (5) to make arrests [for any offense against the United States or felony] if the officer or employee is performing duties relating to the enforcement of the immigration laws at the time of the arrest and if there is a likelihood of the person escaping before a warrant can be obtained for his arrest.[125]

The law recognizes the protected status of the home, requiring either consent or a properly-executed warrant to enter onto farm land or any agricultural operation to interrogate individuals as to their right to be in the United States.[126] As for "reasonable distance," lower courts have held that this provision, which allows the Attorney General to ascertain how far from the border probable cause and a warrant is not required, is not unconstitutional because it does not insert a neutral magistrate into the review process.[127]

In terms of searches at the border itself,

> Any officer or employee of the [immigration] [s]ervice authorized and designated under regulations prescribed by the Attorney General, whether individually or as one of a class, shall have power to conduct a search, without warrant, of the person, and of the personal effects in the possession of any person seeking admission to the United States, concerning whom such officer or employee may have reasonable cause to suspect that grounds exist for denial of admission to the United States under this chapter which would be disclosed by such search.[128]

The standard is thus one of "reasonable cause." Congress, to date, has not made any special exceptions for the personal effects that may be searched, with the result that, as noted in the introduction, guidance on electronic devices has been left to the agencies themselves.

IV. Border Search of Electronic Devices

There are increasing calls in the public to exempt electronic devices from the border search exception. The argument put forward is that these devices contain a tremendous amount of private information. Prior to the Supreme Court's decisions in *Riley v. California*, *United States v. Jones*, and *Carpenter v. United States*, courts generally rejected the argument based either on the grounds that the search was routine and did not require reasonable suspicion (pursuant to the border search exception), or that it was conducted with reasonable suspicion. However, three courts determined that *forensic* examination requires a higher standard than exists in the ordinary border search exception. Following *Riley*, *Jones*, and *Carpenter*, moreover, there is every reason to

---

[125] 8 U.S.C.A. § 1357(a).
[126] 8 U.S.C.A. § 1357(e).
[127] United States v. King, 485 F.2d 353 (10th Cir. 1973), *rev'd on other grounds*, Bowen v. United States, 422 U.S. 916 (1975).
[128] 8 U.S.C.A. § 1357(c).

believe that the Fourth Amendment places a limit on the search of electronic devices, at least as to U.S. persons and individuals who have a substantial connection to the United States.

A. Not Subject to Reasonable Suspicion

Although the Supreme Court in *Flores-Montano* left open the possibility, under certain circumstances, of requiring reasonable suspicion for particular property searches at the border, some courts have considered the search of electronic devices to fall within the ordinary border search exception.[129] In *United States v. Arnold*, for instance, a traveler arrived at LAX after a nearly twenty-hour flight from the Philippines.[130] When he went to clear customs, CBP pulled him aside for secondary questioning, inspected his luggage, and found a laptop, a separate hard drive, a USB stick, and six disks. Agents directed Mr. Arnold to turn on his computer. On the desktop, there were folders labeled "Kodak Pictures" and "Kodak Memories." When agents opened the folders, they found naked women. CBP called in DHS and ICE, who, believing the pictures to include children, detained and questioned him. They seized his computer and the storage devices and, a fortnight later, obtained a warrant. DOJ charged Michael Arnold with transporting child pornography. Despite the considerable amount of information that could be held on the computer, the court did not see any Fourth Amendment concerns. Neither of the two narrow grounds laid out by the Supreme Court in *Flores-Montano* that would require reasonable suspicion ("exceptional damage to property" or "particularly offensive manner") applied.[131] "[W]e are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."[132] When a similar case arose in regard to fraudulent alien cards, which were found on a traveler's hard drive while crossing the border, the Ninth Circuit considered the requirement of reasonable suspicion to be foreclosed by *Arnold*.[133]

The Fourth Circuit reached a similar conclusion in *United States v. Ickes*.[134] In that case, the defendant, driving a van that appeared to be packed with everything he owned, crossed the U.S./Canadian border. A search of the van uncovered a video camera with a tape of a tennis match in which the camera was focused on a young ball boy. Border agents found marijuana seeds and pipes and several photo albums of child pornography. They also found a computer and 75 diskettes with additional child pornography on them. The court found the search permissible:

> Both Congress and the Supreme Court have made clear that extensive searches at the border are permitted, even if the same search elsewhere would not be. We refuse to undermine this well-settled law by restrictively reading the statutory language in 19 U.S.C. 1581(a) or by carving out a First Amendment exception to the border search doctrine.[135]

At least one other published lower court published opinion has reached a similar conclusion.[136]

---

[129] *See* United States v. Flores-Montano, 541 U.S. 149, 155-56 (2004).
[130] United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008), *cert. denied*. 129 S. Ct. 1312 (2009).
[131] *Id.* at 1008-09.
[132] *Id.* at 1009.
[133] United States v. Singh, 295 Fed. App'x. 190 (9th Cir. 2008).
[134] United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).
[135] *Id.* at 502.
[136] *See, e.g.*, United States v. McAuley, 563 F. Supp. 672 (W.D. Tex. 2008) (A name check on a driver crossing at Del Rio, Texas Port of entry from Mexico showed that the individual was the subject of an

B. Supported by Reasonable Suspicion

Two categories of cases have found the search of electronic devices to be supported by reasonable suspicion: those premised on criminal investigations and records, and those based on the presence of illegal substances. In *United States v. Hassanshahi*, for example, a 2014 case from Washington, D.C., a traveler's laptop was seized during an international border stop at a U.S. airport.[137] An inquiry into the traveler's identity revealed a federal investigation into the defendant's participation in a conspiracy to build a computer production facility in Iran in violation of U.S. trade embargoes. The court in that case considered agents to have established reasonable suspicion sufficient to support a forensic examination of the laptop. Similarly, in *United States v. Saboonchi*, the traveler's name came up in connection with two different export violation investigations.[138] The government had information that the defendant had purchased two cyclone separators which had then been shipped overseas to an entity linked to a company in Iran. The court determined that the forensic search of the defendant's smart phone and flash drive had been supported by reasonable suspicion. *Pari passu*, in *Cotterman*, border agents had reasonable suspicion for their initial search based on the fact that the defendant had a prior conviction for child molestation, frequently traveled to a country associated with sex tourism, and carried password-protected files. A handful of lower courts have found the presence of illegal substances during the search to be sufficient for the examination of electronic devices.[139]

C. Special Protections Extended to Forensic Investigations

One of the most prominent cases on the forensic investigation of electronic devices at the border comes from the Ninth Circuit. In *United States v. Cotterman*, agents entered a traveler's name into the Treasury Enforcement Communication System (TECS) which revealed a 15-year old child sexual molestation charge. Agents referred the defendant and his wife for secondary questioning, ordering them to leave their car and belongings behind. A search of the vehicle yielded two laptop computers with password-protected files. The defendant offered to assist agents in accessing the information, but the agent declined because of concern that the defendant would use the opportunity to sabotage the

---

investigation in New York involving child pornography. The defendant was referred to secondary inspection where, two hours later, ICE began to question him about his computer equipment, including a zip drive and two external hard drives as well as a laptop that had been observed in vehicle. He consented to the search and provided them with the password, whereupon they found child pornography on the device. The court rules the search constitutional). *See also* United States v. Hampe, Crim. No. 07-3-B-W, 2007 WL 1192365 (D. Me. Apr. 18, 2007). The court in this case held that the search of a laptop was a routine search and no reasonable suspicion was required, but it then concluded that the particular facts of the case gave rise to reasonable suspicion that child pornography was involved.

[137] United States v. Hassanshahi, 75 F. Supp. 3d 101 (D.D.C. 2014).

[138] United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014).

[139] *See, e.g.*, United States v. Molina-Isidoro, 267, F. Supp. 3d 911 (W.D. Tex. 2016) (mobile phone searched with reasonable suspicion at Mexican border after agents found methamphetamine in the traveler's suitcase); United States v. Mendez, 240 F. Supp. 3d 1005 (D. Ariz. 2017) (mobile phone search at border after finding drugs in the car considered to have been conducted with reasonable suspicion); United States v. Cano, 222 F. Supp. 3d 876 (S.D. Cal. 2016) (agents, finding 16 kg of cocaine in the spare tire of the defendant's truck had reasonable suspicion to download mobile phone data on grounds that it had been used as an instrumentality of the crime); United States v. Ramos, 190 F. Supp. 3d 992 (S.D. Cal. 2016) (agents found methamphetamine in the car and questioned defendant who said he been in cell phone communication with person to whom he was reporting; court determined that DHS manual search of phone and examination of incoming calls, text messages, and the call log was reasonable); United States v. Caballero, 178 F. Supp. 3d 1008 (S..D. Cal. 2016) (CBP found illegal drugs in defendant's car and searched the defendant's mobile phone which had photos of large sums of money; the court said reasonable, particularized suspicion present).

files. Agents seized the computers and transported them to Tucson, 150 miles away, for forensic evaluation. After three days, seventy-five images of child pornography had been found. The court determined that border searches were limited in time and distance: agents needed to have reasonable suspicion that the subject was involved in criminal activity. Mere suspicion was not enough.[140] The court recognized the unique nature of the type of information contained in electronic devices:

> The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. This is no longer the case. Electronic devices are capable of storing warehouses full of information.* * *Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails.* * *Electronic devices often retain sensitive and confidential information far beyond the point of erasure, notably in the form of browsing histories and records of deleted files. This quality makes it impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel.[141]

A second case from the District Court in Maryland held that the border search of any computer or electronic device should be considered non-routine and require reasonable suspicion.[142] The court's argument was that, while the government has legitimate concerns about child pornography, it does not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information—which is what is involved in forensic examination of a hard drive. The court took a different approach than the Ninth Circuit in *Cotterman*: in the former, the court determined that the forensic search of a computer that had been imaged was as invasive of the defendant's privacy as a strip search. In *Saboonchi*, the Maryland court took issue with the Ninth Circuit's failure to provide guidelines for what constituted a "forensic" search. The court distinguished between routine and non-routine border searches and tried to construct a test for determining when a conventional computer search becomes a forensic investigation:

> A conventional search at the border of a computer or device may include a Customs officer booting it up and operating it to review its contents, and seemingly, also would allow (but is not necessarily limited to) reviewing a computer's directory tree or using its search functions to seek out and view the contents of specific files or file types. . . . And, just as a luggage lock does not render the contents of a suitcase immune from search, a password protected file is not unsearchable on that basis alone.[143]

In contrast, "[i]n a forensic search of electronic storage, a bitstream copy is created and then is searched by an expert using highly specialized analytical software—often over the course of several days, weeks, or months—to locate specific files or file types, recover hidden, deleted, or encrypted data, and analyze the structure of files and of a drive."[144] The court provided three explanations for why forensic searches should be considered sui

---

[140] United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc) (requiring reasonable suspicion for forensic examination of the laptop).
[141] 709 F.3d at 964-65.
[142] U.S. v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014).
[143] *Id.* at 560-61.
[144] *Id.* at 561.

generis: first, it creates a copy and uses specialized software to analyze the computer's contents; second, it provides access to deleted material; third, it provides insight into an individual's actions away from the border which would not otherwise be discoverable.[145]

The First Circuit, in evaluating other kinds of searches, offered the following non-exhaustive list of factors may be relevant when determining whether a search can be characterized as routine:

> (i) whether the search results in the exposure of intimate body parts or requires the suspect to disrobe; (ii) whether physical contact between Customs officials and the suspect occurs during the search; (iii) whether force is used to effect the search; (iv) whether the type of search exposes the suspect to pain or danger; (v) the overall manner in which the search is conducted; and (vi) whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search.[146]

D. *Riley v. California*: Stronger Constitutional Protections for Mobile Devices

The above cases pre-dated *Riley v. California*,[147] in which the Supreme Court "made it clear that the breadth and volume of data stored on computers and other smart devices make today's technology different in ways that have serious implications for the Fourth Amendment analysis."[148] One of the first border search cases to incorporate and apply *Riley* was *United States v. Kim*, in which the court determined that the question of electronic searches was settled neither by the border exception nor by application of what was meant by "forensic." Instead, it considered the extent to which the search "intrudes upon an individual's privacy, and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[149] The court noted:

> while the courts in *Ickes*, *Cotterman*, and *Saboonchi* had little in the way of Supreme Court precedent to guide their way, the Supreme Court has since issued its opinion in *Riley v. California*. And in *Riley*, the Court made it clear that the breadth and volume of data stored on computers and other smart devices make today's technology different in ways that have serious implications for the Fourth Amendment analysis.[150]

Riley dealt with the search of a mobile phone incident to arrest. In that case, the Court underscored the distinction between electronic devices and physical items. "Modern cell phones, as a category, implicate privacy concerns far beyond those implicate by the search of a cigarette pack, a wallet, or a purse."[151] Even the term was misleading, as "many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."[152] A key distinguishing feature is the "immense storage capacity" of such devices: "Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or

---

[145] *Id.* at 563. *See also* Gretchen C.F. Shappert, The Border Search Doctrine: Warrantless Searches of Electronic Devices After Riley v. California, U.S.ATTY'S BULL., Nov. 2014, at 10.
[146] United States v. Braks, 842 F.2d 509, 512 (1st Cir. 1988) (footnotes omitted).
[147] Riley v. California, 134 S. Ct. 2473 (2014).
[148] United States v. Kim, 103 F. Supp. 3d 32, 54 (D.D.C. 2015).
[149] *Riley*, 134 S. Ct. at 2484 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
[150] *Kim*, 103 F. Supp. 3d at 54.
[151] *Riley*,134 S. Ct. at 2488-89
[152] *Id.* at 2489.

article they have read."[153] Mobile phones can store "millions of pages of text, thousands of pictures, or hundreds of videos."[154] The sheer capacity of mobile devices has numerous implications for privacy:

> First, a cell phone collects 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. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.[155]

More than 90% of American adults own and carry cell phones, keeping "on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[156] The type of information that could be gleaned, moreover, different in important respects from what could be uncovered from the search of a physical item. Medical records, location information, relationship details, political beliefs, religious convictions—all of this, *more* than could be ascertained even from a search of an individual's home, can be gleaned.[157] Beyond this, mobile phones provide a gateway to the cloud. The court in *Riley* was utterly unsatisfied with the solution the government proposed here: namely, "to disconnect a phone from the network before searching the device."[158] (This is precisely what CBP is doing in regard to search of electronic devices at the border).

In *Kim*, as aforementioned, the court applied *Riley* and determined, under a totality of circumstances test, that the imaging and search of a laptop, for an unlimited period and without any limits on the scope of the analysis, invaded the traveler's privacy to such an extent that it was unreasonable under the Fourth Amendment.[159] The court noted: "given the vast storage capacity of even the most basic laptops, and the capacity of computers to retain metadata and even deleted material, *one cannot treat an electronic storage device like a handbag simply because you can put things in it and then carry it onto a plane*."[160]

The *Kim* case is notable not just for its application of *Riley*, but because it involved a conscious decision by investigators to wait until a suspect left the United States before *using* the border exception to search his laptop and thereby obtain detailed information about his activities.[161] The court ultimately rejected agents' instrumentalist approach—i.e., using the border search exception to obtain information to which they otherwise would not be entitled.[162]

---

[153] *Id.*
[154] *Id.*
[155] *Id.*, at 2489.
[156] *Id.*, at 2490.
[157] *Id.*, at 2490-91.
[158] *Id.* at 2491.
[159] *Kim*, 103 F. Supp. 3d at 56.
[160] *Id.* at 50 (emphasis added).
[161] *Id.* at 38-39.
[162] *Id.* at 45 (citing Hassanshahi, 75 F.Supp.3d at 120-21).

E. Impact of *Carpenter v. United States*

As with *Riley*, the Court's recent decision in *Carpenter v. United States* has significant implications for how to think about potential Fourth Amendment limits on electronic border searches. In *Carpenter*, the Court decided not to extend third party doctrine from *United States v. Miller* and *Smith v. Maryland* to cell site location information (CSLI).[163] In *United States v. Jones*, five justices (the so-called "shadow majority") had adopted the view that individuals have a reasonable expectation of privacy in the whole of their physical movements.[164] The *Carpenter* court built on *Jones*, underscoring the sensitivity of the information that could be gleaned from location data. It highlighted a number of factors that suggested a higher privacy incursion: accuracy; retroactive application; length of time (implicating the amount of information); the revealing nature of the information; the nature of the information obtained; and the ease with which it could be obtained.[165]

These elements are all present in the border search of electronic devices, suggesting a higher intrusion into travelers' privacy than is present with the simple search of a traveler's baggage or pockets. To the extent that electronic devices contain a record of the traveler's physical movements, warrantless search runs directly contrary to the holding in *Carpenter*.

F. The Problem of Digitization

The two streams of authorities, customs and immigration, both deal with the transportation of physical objects: articles and people. Before concluding, it is worth noting that digitization presents two particular challenges for these regimes.

First, for customs, what happens when the illicit materials being sought are digital, and not physical? In the past, if an object was carried into the country, then the inspection regime would uncover it at the border. But what happens if the illicit material can merely be uploaded onto the cloud, to be accessed once someone enters the United States? If a traveler in Thailand, for instance, uploads child pornography onto the cloud, should there be a way to use the traveler's movement to uncover the material? Or what if the material in question consists of documents, such as plans for a nuclear reactor or technology designs which have been forbidden by the export regime. Should a traveler be able to upload this material to the cloud, only to pull it down elsewhere? In the past, the material would have either have been mailed through the post, or carried by hand. Should there be a way to foreclose a digital end-run around the customs regime?

There are at least three possible responses to this argument. Foremost, it is important to note that part of the reason this issue even presents is because of the post-War expansion of the customs mail search regime to include not just uncustomed items, but also child pornography, weapons of mass destruction, emergency matters under the IEEPA, and the like. The historical purpose of the customs regime was *not* to uncover illegal activity generally. The purpose of customs searches was to identify the illegal transportation of contraband or undeclared items.[166] To the extent that a border search exception, derived from sovereignty applies, it is specifically with this end in mind.

In addition, in light of the expansion of the Foreign Intelligence Surveillance Act (FISA) post-9/11 and the infamous demise of the wall, such matters may be relegated more appropriately to the surveillance realm. That is, to the extent that matters, such as drawings of a nuclear reactor being provided to third countries, implicate foreign affairs,

---

[163] United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).
[164] United States v. Jones, 565 U.S. 400 (2012).
[165] Carpenter v. United States, No. 16-402, slip op. at 12-22 (June 22, 2018).
[166] U.S. v. Seljan, 547 F.3d 993 (9th Cir. 2008).

surveillance would appropriately fall within FISA. Even where the investigation may be primarily criminal in nature, such surveillance still comes within FISA's ambit.

Further, to the extent that electronic searches reveal information that would otherwise be held in the home, then allowing such searches forces the historic protections afforded to the home, even in customs matters, to drop away. Email has replaced letter correspondence, electronic calendars now take the place of planners, and the contacts list now serves as a telephone book. The border exception, applied to electronic devices, threatens to swallow the protections which, for centuries, have limited customs searches. This is true not just for the *type* of data at stake, but actual views of the home. Consider, for instance, the Blink Home Monitor. An application can be downloaded to smartphones and tablets, providing homeowners with real-time coverage of what is happening inside their houses.[167]

The second challenge presents for immigration. Here, part of the reason behind subjecting non-citizens to searches prior to entering the United States has to do with ascertaining (a) whether they are who they say they are, and (b) what sorts of individuals are being admitted to the country. Surely, the type of information present in travelers' electronic devices is relevant to such a determination. By *not* taking into account social media, or the full range of an individual's background, moreover, U.S. security may be harmed. Notwithstanding PPD-28 and its extension to non-citizens of privacy rights, as Chief Justice Rehnquist noted in *Verdugo-Urquidez*, non-U.S. persons without a substantial connection to the United States lack Fourth Amendment protections.

V. CONCLUDING REMARKS

Like the search incident to arrest exception at issue in *Riley*, the border search exception is still subject to the reasonableness requirement of the Fourth Amendment. Numerous cases are beginning to move through the courts, challenging whether electronic devices fall outside constitutional norms.[168] The American Bar Association has raised particular concerns about the extent to which the reading, duplication, and seizure of legal documents violates client-attorney privilege.[169] Similar issues have been raised in regard

---

[167] *See* https://blinkforhome.com/pages/blink-home-monitor-app?locale=en&gclid=EAIaIQobChMIpZ-lhMeS3AIVC4GzCh2AQQZnEAAYASAAEgJCM_D_BwE&gclsrc=aw.ds.

[168] *See, e.g.*, Abidor v. Napolitano, 990 F. Supp. 2d 260 (E.D.N.Y 2013) (dual U.S./French citizen had laptop searched confiscated at Canadian border and returned eleven days later, with evidence that his personal files (including his research, photos, chats with his girlfriend) had been searched); Complaint, Alasaad v. Duke, 1:17-cv-11730-DJC (D. Mass. filed Sept. 13, 2017) (challenging search and seizure of smartphones, laptop, and other electronic devices at the U.S. border in violation of the First and Fourth Amendments). See also Daniel Victor, *Forced Searches of Phones and Laptops at U.S. Border are Illegal, Lawsuit Claims*, N.Y. TIMES (Sept. 13, 2017), https://www.nytimes.com/2017/09/13/technology/aclu-border-patrol-lawsuit.html; Deb Riechmann, *Are Searches of Laptops and Cellphones by Border Agents Unconstitutional?*, PBS (Sept. 13, 2017) http://www.pbs.org/newshour/rundown/searches-laptops-cellphones-border-agents-unconstitutional/.

[169] *See, e.g.*, Looper v. Morgan, Civ. No. H-92-0294, 1995 U.S. Dist. LEXIS 10241 (S.D. Tex. June 23, 1995); U.S. v. United Shoe Machinery Corp., 89 F. Supp. 357 (D. Mass 1950); Upjohn Co v. United States, 449 U.S. 383 (1981). This creates a possible conflict between Rule 1.6 of the ABA Model Rules of Professional Conduct, which deals with Confidentiality of Information, and searches at the border. Under work product doctrine, such materials are not discoverable (Fed. R. Civ. P. 26(b)(3)(A)), although it can be overcome by the demonstration of "substantial need" (Fed. R. Civ. P. 26(b)(3)(A)(ii). There is a distinction to be drawn between attorney-client material generally versus information and material related to litigation, the confidentiality requirement, and common interest doctrine. See, e.g., Bank of Am. v. Terra Nova Ins. Co. Ltd., 211 F. Supp. 2d 493 (S.D.N.Y. 2002). The ABA Criminal Justice Section currently has a Task Force looking into electronic border searches, considering, inter alia, the impact on client-attorney privilege.

to doctor-patient records, and journalists' privileges, spousal communications, information covered by a U.S. federal court protective order, proprietary information, and intellectual property.

As a matter of constitutional law, at least in terms of the Fourth Amendment issues, the Court's recent decisions in *Riley* and *Carpenter*, and the concerns raised by the shadow majority in *Jones*, suggest that electronic devices warrant a higher level of protection. As a matter of First Amendment doctrine, the Court in *United States v. Ickes* found such arguments to be unpersuasive.[170] In that case, Ickes argued that border search doctrine does not apply when the material being searched is expressive. "[T]his cannot be the case," the court wrote. That doctrine "is justified by the 'longstanding right of the sovereign to protect itself.'"[171] National security interests in the contemporary age inescapably implicate expressive material, such as terrorist communications. Recognizing First Amendment interests, moreover, would create difficulties in determining where the line should be drawn.[172] Notwithstanding the court's decision in *Ickes*, the implications of access to electronic devices for religious freedom, free speech, and free association are substantial. The type of information contained in mobile phones, tablet, and computers, goes to the most intimate aspects of individuals' politics, beliefs, and relationships. One of the more recent cases to raise these issues settled.[173] In addition to the important Fourth and First Amendment issues at stake are those related to the Fifth Amendment right against self-incrimination, as well as due process, and the Sixth Amendment right to counsel.

As recognized in the introduction to these written remarks, border searches of electronic devices are increasing at an alarming rate. Thus far, CBP and ICE have been largely left to determine, for themselves, whether and to what extent they can search travelers' devices. While border searches are supported by claims of sovereignty, technological advances increasingly implicate individual rights. In *Riley*, the Government offered as an alternative that it be allowed to develop its own protocols to address the unique questions posed by cloud technologies. The Court observed, "the Founders did not fight a revolution to gain the right to government agency protocols."[174] The Founders fought for rights—rights that are now endangered by the government's search of electronic devices as citizens depart, and re-enter, the United States. The time is ripe for Congress to take action.

---

[170] United States v. Ickes, 393 F.3d 501, 506-08 (4th Cir. 2005).
[171] *Id.* at 506 (internal citations omitted).
[172] *Id.*
[173] House v. Napolitano, No. 11-cv-10852-DJC, 2012 WL 1038816 (D. Mass. Mar. 28, 2012) (David House, part of the Bradley Manning Support Network, had his laptop seized at the border and imaged).
[174] *Id.*

STATEMENT OF

NEEMA SINGH GULIANI
SENIOR LEGISLATIVE COUNSEL, WASHINGTON LEGISLATIVE OFFICE
AMERICAN CIVIL LIBERTIES UNION

For a Hearing on:

"Examining Warrantless Smartphone Searches at the Border"

Before

United States Senate
Committee on Homeland Security and Governmental Affairs
Subcommittee on Federal Spending Oversight and Emergency Management

July 11, 2018

For further information, please contact Neema Singh Guliani, Senior Legislative Counsel, at nguliani@aclu.org.

Chairman Paul, Ranking Member Peters, and Members of the Subcommittee,

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU)[1] and for holding this hearing on "Examining Warrantless Smartphone Searches at the Border." The ACLU is actively engaged in litigation and advocacy to protect individuals' rights at the border and in the digital age.

The government's efforts to protect the border must comply with the Constitution. As the Supreme Court has ruled, the Fourth Amendment prohibits unreasonable searches and seizures at the border. Nevertheless, each year, tens of thousands of travelers are subjected to unconstitutional searches and confiscations of their electronic devices at U.S. ports of entry. Journalists, attorneys, and veterans have had their most intimate information – including private emails, photos, and text messages – seized and searched without a warrant, probable cause, or even reasonable suspicion. The government's failure to obtain a warrant prior to device searches invites abusive practices that improperly target individuals based on race, religion, political beliefs, or other impermissible factors.

The number of unconstitutional border device searches has increased dramatically in recent years. Despite the clear difference between searching traveler's luggage and the contents of their electronic devices, U.S. Customs and Border Protection (CBP) policy continues to improperly permit officers to search travelers' cell phones, laptops, and other electronic devices at the border without a warrant that is based on probable cause. In addition, the CBP policy fails to make clear that CBP cannot perform device searches for general law enforcement purposes or for vague national security reasons; that travelers are under no obligation to disclose their passwords to CBP upon request and cannot be coerced into providing this information; and that other agencies must comply with the same standards when conducting searches of electronic devices seized by CBP at the border.

Congress should press the Department of Homeland Security (DHS) to remedy the deficiencies in its policies. In addition, it should pass legislation, including the bipartisan *Protecting Data at the Border Act* sponsored by Senators Rand Paul (R-KY) and Ron Wyden (D-OR), that ensures that travelers are not subject to border device searches without a warrant, are not obligated to assist in unlocking an electronic device at the border, and cannot be unreasonably detained for failing to consent to a device search.

A. The number of border device searches has increased dramatically in recent years.

Despite their small size, smartphones, laptops, tablets, and other electronic devices have "immense storage capacity." Standard portable electronic devices permit the storage of millions

[1] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country. With more than a million members, activists and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico and Washington, D.C., to preserve American democracy and an open government.

of pages of text, thousands of pictures, or hundreds of videos – far more information than could historically be stored in a traveler's luggage.[2] At the same time, individuals are increasingly reliant on portable electronic devices for day-to-day activities. Today, virtually every American owns a cell phone, 77 percent own a smartphone, over half own a tablet, and nearly three quarters own a computer of some kind.[3] Many individuals are reliant on these devices to obtain health data, look for employment, manage their banking, navigate, and communicate with their loved ones.[4]

Despite the volume and sensitivity of information stored on electronic devices, CBP increasingly searches these devices without a probable cause warrant. In 2015, CBP searched 8,503 devices at the border[5]; this number climbed to 19,051 and 30,200 in 2016 and 2017, respectively.[6] Device searches appear to be increasing rapidly in part due to technological advances that have enabled DHS to quickly extract sensitive information such as contact lists, travel patterns, and even deleted call logs.[7]

No travelers are immune to a possible warrantless device search. Lawyers, journalists, students, veterans, and others have been ensnared in this unconstitutional practice. In some cases, device searches appear to have been accompanied by concerning questions regarding individuals' religious beliefs and political affiliations, further raising concerns that they are being employed in a discriminatory manner. In one complaint obtained through a Freedom of Information Act request by the Knight Institute, an individual describes being questioned regarding their religious activity, civic engagement, political engagement, and charitable contributions during the same encounter in which CBP confiscated documents from her electronic device, which included sensitive religious prayer requests.[8] Other individuals that have been impacted by warrantless device searches include:

- Diane Maye: Ms. Maye is a U.S. citizen and former Air Force captain who served six years as an officer. In June 2017, Ms. Maye was traveling from Norway to Miami when she was detained by CBP officers upon arrival. She was escorted into a small room, where CBP officers seized her smartphone and laptop. The CBP officers asked her to unlock her devices. Because she had no meaningful choice, Ms. Maye unlocked both devices, and then watched the officers search her laptop, while her unlocked phone was seized for

[2] *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).
[3] *Mobile Fact Sheet*, PEW RESEARCH CENTER (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/
[4] Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CENTER (April 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/
[5] McFadden, et al., *American Citizens: US Border Agents Can Search Your Cellphone*, NBC News (Mar. 13, 2017), https://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746
[6] U.S. Customs and Border Protection, "CBP Releases Updated Border Search for Electronic Device Directive and FY17 Statistics (January 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and
[7] McFadden, supra note 5.
[8] *See* Knight Foundation FOIA Response (Sept.. 21, 2017), https://assets.documentcloud.org/documents/4334752/KFAI-FOIA-TRIP-Complaints-Border-Electronics.pdf; Decell, Carrie, *Warrantless Border Searches: The Officer "Searched Through…Intimate Photos of My Wife,"* THE KNIGHT FOUNDATION (Dec. 22, 2017), https://knightcolumbia.org/news/warrantless-border-searches-officer-searched-throughintimate-photos-my-wife

approximately two hours.[9]

- Ghassan and Nadia Alasaad: Mr. and Ms. Alasaad are U.S. citizens residing in Massachusetts. In July 2017, they were returning to the U.S. from a family vacation when their entire family was detained by CBP. Upon arrival, they were directed to secondary inspection where CBP officers questioned Mr. Alasaad and searched through his unlocked phone. Concerned, Mr. Alasaad asked the officers why his family was being detained and searched, to which a CBP supervisor responded that he had simply felt like ordering a secondary inspection. The CBP officers later requested Ms. Alasaad's cell phone password. The couple refused, in particular because Ms. Alasaad wears a headscarf in public in accordance with her religious beliefs and her cell phone had pictures of her without her headscarf on that she did not want any CBP officers, especially male officers, to view. The CBP officers explained that failure to comply would result in Ms. Alasaad's phone being confiscated. Because they had no meaningful choice, the Alasaads provided the password.[10]

- Sidd Bikkannavar: Mr. Bikkannavar is a U.S. citizen who works as an engineer at NASA's Jet Propulsion Laboratory in California. In January 2017, Mr. Bikkannavar was returning to the United States from a trip to Chile. Upon his return, CBP officers seized his cell phone and ordered him to disclose the password. After initially refusing, Mr. Bikkannavar was given a form explaining to him the consequences of failing to comply. The CBP officer repeated his order to disclose the phone's password and coerced Mr. Bikkannavar into disclosing it. The CBP officer wrote down the password and took the phone to another room for about 30 minutes. Upon returning, the CBP officer informed Mr. Bikkannavar that officers had used "algorithms"[11] to search his phone.

- Jeremy Dupin: Mr. Dupin is an award-winning journalist and filmmaker who covers news in South America and the Caribbean. He is a legal permanent resident of the U.S. and lives in Massachusetts. In December 2016, Mr. Dupin was returning home from reporting in Haiti when he was detained by CBP officers at Miami International Airport. The officers seized Mr. Dupin's phone and ordered him to disclose his phone's password. Because he had no meaningful choice, Mr. Dupin provided the password. After several hours of being detained and questioned, including about his journalism work, Mr. Dupin was finally released. A day later, Mr. Dupin was detained again by CBP after traveling across the border with his young daughter. CBP officers seized and searched the same phone that CBP had searched a day previously, and released Mr. Dupin after about seven hours of detention.[12]

- Akram Shibly: Mr. Shibly is a U.S. citizen, a resident of New York, and a professional filmmaker. In January 2017, Mr. Shibly and his fiancée were detained by CBP officers upon returning to the United States from a film project in Canada. Upon arrival, a CBP officer

[9] Amended Complaint for Injunctive and Declaratory Relief at 30-31, *Alasaad v. Duke*, No. 17-cv-11730-DJC (D. Mass filed Sept. 13, 2017).
[10] *Id.* at 17-20.
[11] *Id.* at 22.
[12] *Id.* at 23-25.

ordered Mr. Shibly to provide the password to his phone. After Mr. Shibly stated that he did not feel comfortable doing so, the officer told Mr. Shibly that if he had nothing to hide, then he should unlock his phone. Because he had no meaningful choice, Mr. Shibly unlocked his phone and watched the officer take his phone out of sight. He was also coerced into disclosing his social media identifiers. A few days later, Mr. Shibly was detained again after returning from a day trip to Canada. A CBP officer ordered him to hand over his phone. When Mr. Shibly declined to do so because officers had searched his phone only days earlier, three CBP officers used physical force to seize his phone.[13]

B. The Fourth Amendment requires a warrant based on probable cause to search devices at the border.

The Supreme Court has made clear that the Fourth Amendment applies to searches at the border, and in recent years has also made clear that searches of digital data are highly sensitive and entitled to the full panoply of Fourth Amendment protection—namely, a warrant based on probable cause.

In *Riley*, the court held that the government must obtain a warrant before searching a cell phone seized incident to arrest.[14] In its opinion, the court highlighted the differences between the information that could be stored on a person versus on a digital device – noting that even basic cell phones could store photographs, text messages, Internet browsing history, and a thousand-entry phone book, and that smartphones can store a great deal more.[15] Thus, information obtained from a phone would allow the government to reconstruct "the sum of an individual's private life." More recently, in the *Carpenter* decision released this term, the Supreme Court held that historical location information is subject to the Fourth Amendment's warrant requirement.[16] Similarly sensitive location information can also be gleaned from searches of electronic devices.

Riley made clear that traditional exceptions to the Fourth Amendment's warrant requirement do not automatically extend to searches of digital data. Indeed, the volume and sensitivity of information that can be obtained from an electronic device distinguishes these searches from the searches of physical luggage that were previously understood to fall under the border search exception to the Fourth Amendment's warrant requirement.

Notwithstanding this, CBP and ICE's policies reflect their position that they have "plenary authority . . . . [to] control[] the entry and exit of persons and property,"[17] which they believe allows them to conduct warrantless, and even suspicionless, border device searches pursuant to

[13] *Id.* at 33-35.
[14] *Riley*, 134 S.Ct. at 2495.
[15] *Id.* at 2489.
[16] *Carpenter v. U.S.*, No. 16-402, 2018 WL 3073916 (June 22, 2018).
[17] Memorandum in Support of Defendants' Motion to Dismiss at 1, 19, *Alasaad v. Nielsen*, No. 17-cv-11730-DJC (D. Mass. Dec. 15, 2017); *see also* CBP Directive No. 3340-049A, *Border Search of Electronic Devices* (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

the border search exception. This position ignores the immense privacy harms of such searches and numerous developments in Fourth Amendment law.

Several courts have rejected the government's claim that the border search exception places no limit on device searches at the border. The Fourth Circuit recognized that a forensic search of an electronic device seized at the border requires some level of individualized suspicion, but did not reach the question of whether a warrant or probable cause is required.[18] In a Fifth Circuit case, while the court declined to set a rule, a judge expressed strong skepticism that the traditional rationale for warrantless border searches should extend to searches of electronic devices.[19] While the Eleventh Circuit has unpersuasively held that warrantless border device searches are permissible, a dissenting judge concluded that the Constitution requires a warrant for such searches.[20] And even without the benefit of the Supreme Court's reasoning in *Riley*, an older case from the Ninth Circuit determined that the government had to have reasonable suspicion to conduct a forensic search of a device.[21] Some district courts have also rejected government arguments that the Constitution permits suspicionless device searches at the border.[22]

In rejecting government arguments that warrantless border device searches are constitutional, courts have noted that the government's border search authority is subject to the Fourth Amendment's requirement of reasonableness, and that the volume and sensitivity of information on electronic devices distinguishes these searches from searches of luggage and other physical objects. Judges have also emphasized the danger of border device searches being performed for general law enforcement purposes, which can evade the Fourth Amendment's firm restrictions on warrantless searches by police.[23]

The constitutionality of DHS's policies and practices in conducting suspicionless border device searches is currently being litigated in a case brought by the ACLU and Electronic Frontier Foundation on behalf of 11 travelers who were subjected to unlawful searches, where a judge in the District of Massachusetts recently denied the government's motion to dismiss and has allowed the plaintiffs to press their claims that such searches are unconstitutional.[24]

C. Current DHS policies permit unconstitutional border device searches and fail to protect travelers' rights.

In 2018, following inquiries from members of Congress, including Senators Paul and Wyden, DHS announced an updated CBP border device search policy.[25] While the policy represents a

[18] *See U.S. v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018).
[19] *See U.S. v. Molina-Isidoro* 884 F.3d 287 (5th Cir. 2018).
[20] *See U.S. v. Vergara*, 884 F.3d 1309 (11th Cir. 2018); *see also U.S. v. Toussaint*, 117 F.Supp. 3d 822 (E.D. La. 2015).
[21] *U.S. v. Cotterman*, 709 F.3d 952 (9th Cir. 2013).
[22] *See U.S. v. Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014); *U.S. v. Kim*, 103 F. Supp. 3d 32 (D.D.C. 2015).
[23] *See Kim*, 103 F. Supp 3d. at 58.
[24] *See Alasaad v. Nielsen*, No. 17-cv-11730-DJC, 2018 WL 2170323 (D. Mass filed May 9, 2018).
[25] CBP Directive No. 3340-049A, *Border Search of Electronic Devices* (Jan. 4, 2018),

marginal improvement over prior guidance, it still falls short of meeting Fourth Amendment standards. Congress should press DHS to amend this guidance to (1) require a warrant for border searches of the contents of an electronic device; (2) prohibit searches for general law enforcement purposes and for vague "national security concerns"; (3) clarify travelers' rights not to unlock a device or provide a password; and (4) ensure that all agencies abide by the same standards.

1. Requiring a warrant for searches

CBP's 2018 guidance permits CBP to conduct "basic searches" – defined as any search that is not an "advanced" search – with no suspicion whatsoever. Basic searches can include an officer manually searching any information stored on the device, including photos, emails, or other sensitive information. Even for so-called "advanced" searches, which involve the use of external equipment to copy, review, and/or analyze the contents of a device, the guidance only requires CBP to have reasonable suspicion of unlawful activity in violation of laws enforced or administered by CBP or a vague "national security concern."[26] Searches may be performed off-site and devices may be detained for five days by default and often longer.[27] The guidance requires that any search be confined to data stored on a device itself.

CBP's new policy fails to provide an appropriate level of protection for device searches. What the agency deems a "basic" search, in fact, could implicate sensitive information regarding an individual's religious beliefs, political affiliations, location information, communications, and more. Additionally, the increasing sophistication of search functions on devices themselves provides the government the practical ability to quickly filter though this information with extraordinary precision, enabling even a so-called "basic search" to inflict the extraordinary privacy harms that the Supreme Court identified in *Riley*. To address this concern, DHS should amend its policy to require a warrant based on probable cause for *any* search involving content on an electronic device.

2. Prohibiting searches for general law enforcement purposes and for vague "national security concerns"

Current CBP policy fails to prevent border device searches from being used for general law enforcement purposes. Specifically, the policy fails to prohibit the agency from engaging in searches at the request of other agencies or to assist other agencies for law enforcement purposes. In one case, CBP purportedly flagged an individual because they were wanted for questioning in a Department of Justice investigation involving a leak of classified information.[28] Such searches circumvent Fourth Amendment requirements that apply to

---

https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf

[26] The guidance provides requires special procedures for the handling and segregation of privileged materials. *Id.* at 5.2

[27] *Id.* at 5.4.

[28] *See* Tecs II Document, available at https://www.aclu.org/files/assets/house-settlement/TECS%20Lookout%20for%20David%20House.pdf; Hauss, Brian, *Documents Shed Light on Border*

domestic law enforcement investigations, reflecting a concern that has been raised by federal courts.

In addition, the guidance permits officers to conduct a border search in cases involving a purported "national security concern."[29] "National security concern" is poorly defined, and the policy's language is vague enough to be interpreted as applying in a variety of situations when an individual poses no threat and is not suspected of having violated any law. That language also increases the likelihood of arbitrary and discriminatory application of the policy. To address these deficiencies, DHS should amend the guidance to eliminate "national security concern" as grounds for engaging in a device search.

3. Clarifying travelers' right not to unlock a device or consent to a search

The CBP guidance states that travelers have an obligation to present devices in a manner that allows "inspection." However, this language fails to make clear whether CBP believes that individuals must provide a password or other unlocking assistance at the request of CBP personnel. In addition, it fails to provide clarity as to whether DHS believes that it can detain or, in the case of non-citizens, deny entry to individuals for refusing to consent to a search or unlock their electronic devices. DHS should update its policy to make clear that travelers are under no obligation to provide a password or otherwise provide a means to unlock their device, particularly where they can otherwise demonstrate their admissibility to the United States. In addition, to prevent travelers from being coerced into providing such assistance, the policy should clearly prohibit DHS from unreasonably detaining or denying entry to individuals who refuse to provide such information.

4. Adopting agency-wide guidance

The CBP policy makes clear that if a device is transferred to another component of DHS for search, that component's policies will apply.[30] In practice, CBP often hands devices seized at the border to U.S Immigration and Customs Enforcement (ICE) for search, and ICE's current policy on border device searches does not prohibit searches of data stored on the cloud and accessible from the device. Unlike CBP, ICE continues to maintain a policy issued in 2009 that, similar to CBP's prior policy, permits ICE to conduct a border search of an electronic device without any suspicion, fails to make clear that any search must be confined to data stored on the device and should not extend to cloud-stored data, and permits confiscation of a device for up to 30 days or longer.[31] DHS has provided no rationale for why ICE and CBP are governed by different standards.

To remedy this inconsistency, DHS should adopt agency-wide guidance that applies to border

---

Laptop Searches, ACLU (Sep. 9, 2013), https://www.aclu.org/blog/national-security/documents-shed-light-border-laptop-searches

[29] No. 3340-049A. at 5.1.4.

[30] *Id.* at 5.4.2.

[31] U.S. Immigration and Customs Enforcement Directive No. 7-6.1, *Border Searches of Electronic Devices*, (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

searches of electronic devices performed by any department component.

D. Congress should pass legislation to ensure that border searches respect travelers' rights

The ACLU continues to actively engage in litigation that challenges the government's practice of unconstitutionally searching travelers' electronic devices without a warrant. However, as court challenges continue, DHS officers continue to violate the rights of tens of thousands of travelers every year. Congress should pass legislation, including the bipartisan *Protecting Data at the Border Act* sponsored by Senators Paul and Wyden, which protects travelers' rights at the border. Such legislation should:

- Require a warrant for all border searches of the contents of electronic devices;
- Make clear that travelers are under no obligation to unlock devices or provide device passwords to CBP or other government personnel;
- Prohibit DHS from unreasonably detaining an individual for failing to consent to a device search or failing to unlock a device; and
- Ensure appropriate reporting and transparency regarding border device search practices.

The ACLU thanks you for the opportunity to testify today and commends Senator Paul for his leadership on this important issue. We urge Congress to pass legislation that makes clear that travelers do not have to sacrifice their constitutional rights as a condition of international travel. In the meantime, we also urge members to press DHS to amend its policies to ensure that border device searches comport with the Constitution.

Statement of

Matthew Feeney
Director, Project on Emerging Technologies
Cato Institute

Before

Subcommittee on Federal Spending Oversight and Emergency Management
Committee on Homeland Security and Government Affairs
United States Senate

Hearing on

"Examining Warrantless Smartphone Searches at the Border"

July 11, 2018

Chairman Paul, Ranking Member Peters, and Members of the Subcommittee—thank you for the opportunity to speak with you today about an important topic that should worry every American concerned about the state of civil liberties.

In *Riley v. California* the U.S. Supreme Court recognized that searches of cellphones implicate privacy concerns beyond those associated with searches of wallets, cigarette packs, and other everyday items.[1] Writing the *Riley* majority opinion, Chief Justice Roberts stated that the government's claim that the search of a cellphone and the search of a wallet are "materially indistinguishable" is "like saying a ride on horseback is materially indistinguishable from a flight to the moon."[2]

Roberts was correct. Our cellphones and laptops contain troves of revealing information about our personal relationships, careers, religious affiliations, and hobbies. It's no exaggeration to say that unfettered access to a cellphone allows investigators to uncover details about almost every intimate communication and relationship associated with the owner of the cell phone.

Officials with access to cell phones can easily view photos, calendars, email accounts, social media postings, and other revealing data. *Riley*'s holding, that police need a warrant to search phones belonging to arrested persons, recognizes the privacy interests American adults have in the content of cell phones.

Despite *Riley*, cell phones and other electronic devices enjoy reduced protections at the border and functional border equivalents, such as airports. This is thanks to the long-standing "border exception" to the Fourth Amendment.[3] This exception was recognized at the founding, but was not formally recognized until 1977 in *United States v. Ramsey*.[4] The exception and Customer and Border Protection's (CBP) search authorities have also been codified in law.[5]

---

[1] *Riley v. California*, 134 S. Ct. 2473, 2488 (2014). Pg. 17 of slip opinion. https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

[2] Ibid.

[3] U.S. Const. amend. IV
"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[4] "That searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration." J. Rehnquist, *United States v. Ramsey*, 431 U.S. 616 (1977)

[5] See: 8 U.S.C. §§ 1225 1357 19 U.S.C. §§ 482 507 1461 1496 1581 1582 1589a 1595a

The Supreme Court has yet to consider the constitutionality of warrantless searches of electronic devices at the border. However, Congress can extend the *Riley* standard to the border via legislation[6]

Although warrantless electronic searches affect a minority of travelers, the number of these searches has been increasing. According to CBP's figures, there was an almost 60 percent increase in the number of international travelers processed with an electronic device search between FY 2016 and FY 2017 (See Appendix A).[7]

A 2009 CBP directive on electronic device searches stated, "In the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information encountered at the border."[8]
In the wake of widespread concern about warrantless searches of electronic devices at airports CBP issued an updated directive earlier this year.[9]

The 2018 directive improved the 2009 directive, but not enough. The latest directive distinguishes between "Basic" and "Advanced" searches. Under current DHS policy, a search of an electronic device that doesn't involve an officer connecting the device to external investigatory equipment is a Basic search. Basic searches do not require suspicion, which is required for Advanced searches.[10] The new directive includes a worrying provision that allows officers to examine a phone with external equipment if there is a "national security concern."[11] This is especially worrying because the directive notes that "the presence of an individual on a government-operated and government-vetted terrorist watch list" creates reasonable suspicion.[12] Government watch lists don't

---

[6] Two pieces of legislation already aim to do this:

U.S. Congress, Senate, Protecting Data at the Border Act, S 823, 115th Cong., introduced in Senate April 4th, 2017.

U.S. Congress, Senate, To Place Restrictions On Search and Seizures of Electronic Devices at the Border, S 2462, 115th Cong., introduced in Senate February 27, 2018.
[7] CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics, published by U.S. Customs and Border Protection, January 5, 2018. https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and
[8] CBP Directive No. 3340-049 by Acting CBP Commissioner Jay Ahern, August 20, 2009. https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf
[9] CBP Directive No. 3340-049A by Acting CBP Commissioner Kevin McAleenan, January 4, 2018. https://www.dhs.gov/sites/default/files/publications/CBP%20Directive%203340-049A_Border-Search-of-Electronic-Media.pdf
[10] CBP Directive No. 3340-049A Section 5.1.3 (pg.4)
[11] Ibid. Section 5.1.4 (pg. 5)
[12] Ibid.

only include terrorists. Officials have placed law-abiding American citizens on watch lists designed to prevent dangerous people from flying.[13]

The 2018 directive also requires travelers to unlock their phones.[14] CBP officers have compelled American citizens to unlock and hand over their phones, even after being told that the phone contained sensitive data, including those from NASA's Jet Propulsion Laboratory.[15]

According to the latest directive, officers conducting a search must either have travelers disable network connectivity or disable the connection themselves by (for example) putting the device in airplane mode.[16]

---

[13] Ramzi Kassem, "I Help Innocent People Get Off Terrorism Watch Lists. As a Gun Control Tool, They're Useless," *The Washington Post*, June 28, 2016. https://www.washingtonpost.com/posteverything/wp/2016/06/28/i-help-innocent-people-get-off-terror-watch-lists-as-a-gun-control-tool-theyre-useless/?utm_term=.844f3c4719cc

[14] "Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents."
Ibid. Section 5.3.1 (pg.6)

[15] "But the agent never touched Bikkannavar's bag—instead, he asked for his smartphone. Bikkannavar handed it over, assuming the agent might just want to inspect it to make sure it wasn't something more dangerous in disguise. The agent turned it over in his hand and asked for the passcode.

Bikkannavar was taken aback. The phone was Jet Propulsion Lab property, he explained, pointing out the barcode stuck to the back. It was his duty to protect its sensitive contents, and he couldn't give out the passcode.

The border agent wouldn't relent. He needed to access the device, he said, and had the authority to do so. [...].

Bikkannavar didn't feel like he had a choice. 'I'd read the headlines of people being stranded in airports and having problems entering the country, so I was still in the mode of being as cooperative and polite and courteous as possible,' he said to me."

Kaveh Waddell, "A NASA Engineer Was Required to Unlock His Phone at the Border," *The Atlantic*, February 13, 2017. https://www.theatlantic.com/technology/archive/2017/02/a-nasa-engineer-is-required-to-unlock-his-phone-at-the-border/516489/

[16] CBP Directive No. 3340-049A Section 5.1.2 (pg.4)

These policies are of little reassurance to travelers. Even in airplane mode, cellphones contain revealing information. Text messages, emails, photos, browsing histories, videos, and calendars are still available to officers examining a cellphone in airplane mode. In addition, cellphones in airplane mode do not conceal apps that the cellphone owners may use. You hardly need to have a phone connected to a network to uncover information about someone who has downloaded the Muslim Pro, Coinbase, Tinder, or Diabetes and Blood Glucose Tracker apps.

Current DHS policy does not do enough to protect travelers' civil liberties. S.823, the "Protecting Data at the Border Act," sponsored by Senator Wyden (D-OR) and S.2462, "A Bill to Place Restrictions on Searches and Seizures of Electronic Devices at the Border," sponsored by Sen. Leahy (D-VT) would improve the status quo, but they are not without their own issues.[17]

A welcome provision of S.823 is its warrant requirement for advanced/forensic searches. Alternatively, the legislation permits officers to request travelers to allow access to digital contents through informed consent, overriding the warrant requirement. However, unlike S.2462, it does not require DHS to report the number of electronic devices searches that resulted in criminal charges.[18]

S.2462, would also improve the current situation by requiring that CBP officers have reasonable suspicion an individual is carrying contraband or is inadmissible before conducting a search that does not involve the entry of passwords or assistance from other electronic devices.[19] Like S.823, this bill requires probable cause for an advanced/forensic search.[20]

Under current policy, these searches are justified on the basis that they help CBP in its mission to prevent and investigate terrorism and the trafficking and possession of child pornography.[21] However, DHS has not published figures showing how many of the warrantless searches of electronic devices have contributed to terrorism or child pornography-related convictions. Such data would be welcome, as it would allow the public to better assess the efficiency of warrantless searches that endanger their privacy. Both S.823 and S.2462 would improve DHS transparency regarding these searches.

Some of the United States courts of appeals have considered questions concerning the standard of suspicion necessary for CBP to conduct forensic searches of electronic

---

[17] Ibid.
[18] U.S. Congress, Senate, To Place Restrictions On Search and Seizures of Electronic Devices at the Border, S 2462, 115th Cong., introduced in Senate February 27, 2018.
[19] Ibid.
[20] Ibid.
[21] CBP Directive No. 3340-049A Section 1 (pg.1)

devices.[22] As things stand, there is no consensus.[23] Until the Supreme Court addresses this issue, lawmakers can provide CBP with requirements that go beyond the unsatisfying directive issued by DHS.

The question of warrantless searches of electronic device searches at the border is only one of the many civil liberty concerns associated with immigration enforcement. CBP is interested in using drones with facial recognition capability.[24] In addition, DHS is using facial recognition technology at select American airports, despite Congress never explicitly authorizing the collection of American citizens' biometrics via facial recognition.[25]

Again, thank you for your attention to this important matter and for the opportunity to testify before you. I look forward to answering any questions you may have.

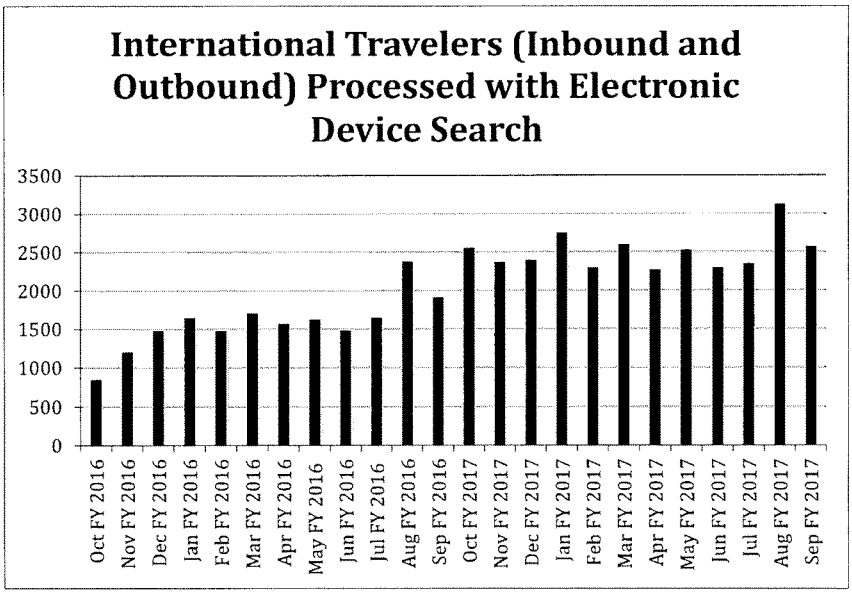
---

[22] *United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013)(acknowledging child pornography is a legitimate concern and holding reasonable suspicion is a "modest, workable standard");
United States v. Kolsuz, No. 16-4687, 2018 WL 2122085 (4th Cir. May 9, 2018). (holding warrantless border searches of digital devices should, at minimum, adhere to a reasonable suspicion standard);
United States v. Touset, No. 17-11561, 2018 WL 2325350 (11th Cir. May 23, 2018). (deferring to legislature to set the standard of suspicion and admitting evidence obtained through forensic search based on reasonable suspicion).
[23] Ibid.
[24] Department of Homeland Security Small Unmanned Aircraft System (sUAS) Solicitation Number: HSHQDC-16-R-00114, last updated April 6, 2017. https://www.fbo.gov/index?s=opportunity&mode=form&id=5bb697a0dd83dccb4e011e905865f914&tab=core&_cview=0
[25] "Harrison Rudolph, Laura M. Moy, Alvaro M. Bedoya, "Not Ready for Takeoff: Face Scans at Airport Departure Gates," Georgetown Law Center on Privacy & Technology. December 21, 2017. (pg. 2).
https://www.airportfacescans.com/sites/default/files/Biometrics_Report_Not_Ready_For_Takeoff.pdf

Appendix A: International Travelers (Inbound and Outbound) Processed with Electronic Device Search between October FY 2016 and September FY 2017[26]

Oct FY 2016	857
Nov FY 2016	1208
Dec FY 2016	1486
Jan FY 2016	1656
Feb FY 2016	1484
Mar FY 2016	1709
Apr FY 2016	1578
May FY 2016	1626
Jun FY 2016	1487
Jul FY 2016	1656
Aug FY 2016	2385
Sep FY 2016	1919
Oct FY 2017	2561
Nov FY 2017	2379
Dec FY 2017	2404
Jan FY 2017	2760
Feb FY 2017	2303
Mar FY 2017	2605
Apr FY 2017	2275
May FY 2017	2537
Jun FY 2017	2304
Jul FY 2017	2359
Aug FY 2017	3133
Sep FY 2017	2580

[26] CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics, published by U.S. Customs and Border Protection, January 5, 2018. https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and


International Travelers (Inbound and Outbound) Processed with Electronic Device Search
3500
3000
2500
2000
1500
1000
500
0
Oct FY 2016
Nov FY 2016
Dec FY 2016
Jan FY 2016
Feb FY 2016
Mar FY 2016
Apr FY 2016
May FY 2016
Jun FY 2016
Jul FY 2016
Aug FY 2016
Sep FY 2016
Oct FY 2017
Nov FY 2017
Dec FY 2017
Jan FY 2017
Feb FY 2017
Mar FY 2017
Apr FY 2017
May FY 2017
Jun FY 2017
Jul FY 2017
Aug FY 2017
Sep FY 2017

Letter for the Congressional Record
Hearing on Examining Warrantless Smartphone Searches at the Border
July 11, 2018

The Honorable Dr. Rand Paul
Chair
Subcommittee on Federal Spending
Oversight and Emergency Management
Committee on Homeland Security and
Governmental Affairs
United States Senate

The Honorable Gary C. Peters
Ranking Member
Subcommittee on Federal Spending
Oversight and Emergency Management
Committee on Homeland Security and
Governmental Affairs
United States Senate

Dear Chairman Paul and Ranking Member Peters,

The U.S. Constitution recognizes civil liberties such as freedoms of speech, assembly, religion, right to privacy, right to a fair trial, and equal protection under the law. For minority and immigrant communities here in the U.S., however, these rights are not applied equally and consistently. Specifically, Arab Americans continually face prfiling by law enforcement officers, including U.S. Customs and Border Protection (CBP) officers, a breach of constitutional protections under the guise of national security.

According to data released by the Department of Homeland Security (DHS), the number of electronic searches at American borders on in American airports reached an estimated 30,200 in 2017, representing nearly a 60 percent jump from the previous year, and more than tripling to toal from 2015, when the number was 8,503 devices.[1] This increase indicates a worrying trend towards policies that violate civil liberties and constitutional rights, as well as likely opening the door for more discriminatory and prejudiced actions to take place.

Although the government retracts the names of many plaintiffs who filed complaints against DHS pertaining to warrantless searches at the border, "many identified themselves as Muslims or people who were not of European descent."[2] One man, who was identified as a Muslim

[1] Ron Nixon, "Cellphone and Computer Searches at U.S. Border Rise Under Trump," The New York Times, January 05, 2018, https://www.nytimes.com/2018/01/05/us/politics/trump-border-search-cellphone-computer.html.
[2] Charlie Savage and Ron Nixon, "Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011," The New York Times, December 22, 2017, https://www.nytimes.com/2017/12/22/us/politics/us-border-privacy-phone-searches.html.

American citizen described being "'treated like a terrorist' when he, his wife and their toddler daughter arrived at San Francisco International Airport..."[3] He and his family were detained for almost four hours and agents went through each of every of their electronic devices. The man stated that "my family and I feel belittled, ashamed, humiliated and disgraced."[4] One Syrian American man named in an American Civil Liberties Union (ACLU) lawsuit, film director Akram Shibly, described being physically forced into giving up his electronic devices. After refusing to hand over his phone, "The officers physically restrained him and took his phone from his pocket, with one agent choking him and another holding his legs..."[5] These experiences are representative of the experiences of thousands of Arab Americans over decades of government suspicion unsupported by any evidence beyond the ethnicity of the traveler.

Troublingly, under the Trump Administration, DHS and agencies under its purview have increased the systematic violation of rights of visitors, immigrants, green card holders, and even U.S. citizens. For example, DHS has admitted[6] that CBP violated court orders in enforcing the president's first Muslim Ban executive order. Immigration and Customs Enforcement (ICE) has unlawfully detained thousands of individuals pursuant to immigration raids[7] and has documented systematic use of racial profiling.[8] Warrantless searches of phones at the border only give DHS agencies greater opportunities to find religious, ethnic, or political reasons to enforce the law in a discriminatory way.

In light of these realities, Congress must implement increased oversight, accountability, and transparency over DHS and its subordinate offices to curb the unacceptable use of force, profiling, and detention at U.S. ports of entry. Instead of authorities which violate the Fourth Amendment to the U.S. Constitution[9] and prove as a vehicle to further racial profiling, CBP and other DHS officers and agents must be provided the training, support, and oversight needed to ensure that they and the communities they serve are safer.

---

[3] Ibid
[4] Ibid
[5] Erik Larson, "Trump Administration Sued Over Phone Searches at U.S. Border," Bloomberg.com, September 13, 2017, https://www.bloomberg.com/news/articles/2017-09-13/trump-administration-sued-over-phone-searches-at-u-s-border.
[6] United States, Department of Homeland Security, Office of the Inspector General, *DHS Implementation of Executive Order #13769 "Protecting the Nation From Foreign Terrorist Entry Into the United States"*, by John V. Kelly, https://www.oig.dhs.gov/sites/default/files/assets/2018-01/OIG-18-37-Jan18.pdf
[7] *Duncan Roy at al. v. County of Los Angeles et al.* (United States District Court: Central District of California February 7, 2018), https://www.aclusocal.org/sites/default/files/aclu_socal_roy_20180208_order_re_msjs.pdf
[8] Kavitha Surana, "How Racial Profiling Goes Unchecked in Immigration Enforcement," ProPublica, June 8, 2018, https://www.propublica.org/article/racial-profiling-ice-immigration-enforcement-pennsylvania.
[9] In the case *Riley v. California* (2014) the Supreme Court indicated that it was illogical to equate the search of an electronic device to that of a physical item, stating that "a ride on horseback is materially indistinguishable from a flight to the moon". *See*: https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

BOARD CHAIRMAN
Nasser Beydoun

VICE CHAIRMAN
James P. Allen, Esq.

TREASURER
Wally Jadan

SECRETARY
Mona Fadlallah, Esq.

FOUNDER
Nabih Ayad, Esq.

BOARD OF DIRECTORS

Ismael Ahmed

Rev. Dr. Wendell Anthony

Chaker Aoun

Dr. Mohamad Ayad, MD

Marvin Beatty

Hussein Berry

Nader Fakhouri

Nabil Fakih

Dr. Samuel Fawaz, MD

Helal Farhat, Esq.

Mike Jaafar

313-633-0231
F: 313-633-1976

4917 Schaefer Rd.
Suite 209
Dearborn, Michigan 48126

rula@acrlmich.org
acrlmich.org

July 11, 2018

The Honorable Gary C. Peters, Ranking Member
U.S. House Committee on Homeland Security
Subcommittee on Federal Spending Oversight and Emergency Management Subcomittee
432 Hart Senate Office Building
Washington, DC 20510

Dear Senator Peters,

We write to you regarding the hearing on "Examining Warrantless Smartphone Searches at the Border."

Since its inception in 2011, The Arab-American Civil Rights League (ACRL), a nonprofit based in Dearborn, Michigan, has grown to be an influential Arab American civil rights organization. The organization is committed to protecting the civil rights of marginalized groups, promoting positive images and combating stereotypes. The ACRL's constituents are regularly confronted with the very issues that this Committee seeks to address. In the past, the ACRL has filed lawsuits challenging adverse action on the Arab American community, including government "no-fly" and watch lists, a suit challenging mass bank closures of Arab owned business accounts.

We welcome and support this Committee's efforts to learn more about how the current digital device search policies affect travelers in the hopes of passing functional legislation.

According to data from the Department of Homeland Security (DHS), searches of mobile phones by border agents grew from fewer than 5,000 in 2015 to 25,000 in 2016, and these searches have further increased under the current administration. It is the ACRL's reasoned belief that Arabs and Muslims comprise a sizable proportion of individuals who are subject to secondary screening at the border. These individuals subject to hours-long screening often include United States Citizens, many of whom are placed on government watch lists and fly-lists without cause or crime. Often, the screening process includes a device search, an extremely intrusive practice that government agents are conducting without cause.

The ACRL does not support any policy that permits the digital devices of United States citizens to searched without a warrant, any practice of obtaining social media passwords. There is not only a basic privacy concern with forcing people to be subjected to a digital strip-search simply for having crossed the nation's borders, but a heightened concern that device searches will further the government's longstanding practice of racially profiling Arab and Muslim travelers without a shred of evidence of suspicious activity.

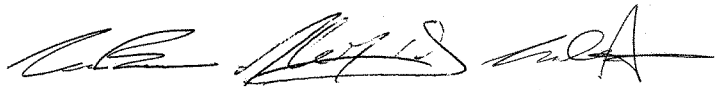
Further, the ACRL opposes legislation which would permit device searches without simultaneously creating a transparency mechanism to account for government officers use of discretion, which is often solely based on the traveler's religious or ethnic identity alone rather than an articulable security concern. Putting this kind of unfettered power in the hands of border agents invites abuse and continued discrimination and will inevitably have a chilling effect on the freedoms of speech and association.

Currently, there is no indication that the Department of Homeland Security performs any anti-discrimination assessment or audit of its policies. Further, no data is gathered on the individuals that are screened, the devices that are searched, or the implications of the data collected. Over the past several years, ACRL has been persistent in its request that a system be implemented to collect data on the race, religion, and nationality of individuals screened, including the screening officer and a description of the reason the individual was subject to additional screening. Our belief is that which such a system in place, border officers can be held accountable for their actions and offer transparency to the American people.

The ACRL is greatly concerned about confiscating devices to conduct forensic examinations and copies of data on devices to share with other government agencies. While a device search policy may affect a minimal percentage of travelers, our fear is that this discretionary search will continue to disproportionately impact our constituents if protections are not in place.

We ask that this letter be entered in the hearing record. The ACRL looks forward to working with the Subcommittee on these issues of vital importance to the American public, and the Arab and Muslim communities.

Sincerely,



Nasser Beydoun
Chairman

Nabih Ayad
Founder

Rula Aoun
Director

The American-Arab Anti-Discrimination Committee

Statement for the Record on the

Warrantless Smartphone Searches at The Border

Before the

U.S. Senate Committee on Homeland Security and Governmental Affairs

Subcommittee on Federal Spending Oversight and Emergency Management

July 11, 2018

Abed A. Ayoub, Esq., ADC Legal & Policy Director
American-Arab Anti-Discrimination Committee
1705 DeSales St., N.W
Washington, DC 20036
Phone: (202) 244-2990
Fax: (202) 333-3980
E-mail: legal@adc.org
Web: www.adc.org

To: Senator Rand Paul, Chairman of the Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Federal Spending Oversight and Emergency Management; and Senator Gary Peters, Ranking Member of the Committee

I am writing to you on behalf of the American-Arab Anti-Discrimination Committee (ADC), the country's largest Arab-American grassroots organization. ADC holds a seat on the National Executive Board of the Leadership Conference on Civil and Human Rights, a coalition of hundreds of civil society organizations committed to liberty and justice for all. ADC's distinguished history is marked by support for the human and civil rights of all Americans and opposing racism, discrimination, and bigotry in all forms. Founded by former U.S. Senator James Abourezk in 1980, ADC currently has members in every State of the union. ADC routinely works with a broad coalition of national organizations to ensure that the rights of ethnic minorities in the United States are protected. The constitutional, civil, and human rights of Arab-Americans are at risk now more than ever. ADC respectfully takes this opportunity to provide a statement for the record with recommendations and comments to the United States Senate Judiciary Committee.

Reigning in executive overreach

ADC encourages the passage of legislation that ensures adequate protection for the privacy rights of all Americans, and the nation's guests and visitors. The executive overreach of United States Customs and Border Patrol (CBP) Directive No. 3340-049A, allowing warrantless searches of electronic devices at U.S. borders, necessitates legislative regulation to safeguard America's cherished constitutional rights to privacy, due process, and protection from unreasonable search and seizure. Furthermore, ADC has serious concerns about the efficacy of the current executive policy in addition to fears that the policy is used disproportionately against minorities.

Unprecedented search powers

According to the Department of Homeland Security, U.S. Customs and Border agents searched nearly 30,000 electronic devices belonging to international travelers in 2017.[1] Since the program's inception under the Obama Administration, the frequency of these searches has increased steadily from approximately 8,500 in 2015 to 19,000 in 2016, to 30,000 in 2017, with that number likely growing through 2018.[2]

---

[1] U.S. Customs and Border Protection, CBP Public Affairs, CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (2018), http://www.americanbar.org/groups/legal_education/resources/statistics.html

[2] Keith Fisher, U.S. Border Searches of Electronic Devices: Recent Development and Lawyers' Ethical Responsibilities, Business Law Today (2018), https://businesslawtoday.org/2018/03/u-s-border-searches-of-electronic-devices-recent-developments-and-lawyers-ethical-responsibilities/

P: 202.244.2990 | F: 202.333.6470| 1705 DeSales Street, NW Suite 500 | Washington, DC 20036 | www.adc.org

The regulations outlined in CBP Directive No. 3340-049A empower CBP Agents to conduct warrantless searches[3] on people traveling legally from any country by way of any "railway car, aircraft, conveyance, or vehicle" within 100 air miles[4] from "any external boundary" of the United States. That gives invasive search powers to CPB agents in a CBP zone consisting almost two-thirds of the entire U.S. population, including residents of New York City, Los Angeles, Chicago, Philadelphia, and Houston.[5]

Furthermore, much of "CBP's law enforcement and patrol activities, such as questioning individuals, collecting evidence and making arrests, are not subject to the 100-mile rule, the agency says. This means that, for instance, the geographical limit does not apply to stops in which border agents pull a vehicle over as part of a "roving patrol" and not a fixed checkpoint."[6]

CBP carries out these searches and seizures without a warrant or individualized suspicion, much less probable cause of any wrongdoing by the traveler.[7] With unwarranted searches of electronic data, including intimate personal information such as photos, emails, text messages, and digital application data, the CBP violates its own stated policy to protect the constitutional "rights of individuals against unreasonable search and secure and ensure privacy protections."[8]

Ineffective and Unsupported Policies

The CBP purports that the searches are longstanding practices "essential to enforcing the law at the U.S. border and to protecting border security."[9] However, CBP is currently unable to produce any statistics to support the efficacy of such invasive search policies. In response to formal requests for data that ADC submitted, the CBP responded that no statistics are available on how many arrests or determinations of inadmissibility into the U.S. were made on the basis of the warrantless electronic searches CBP conducted. As it stands, we cannot conclude that the searches are in the least bit effective, let alone "essential to enforcing the law."

---

[3] 8 U.S.C. § 1357(e) (2010)
[4] 3. 8 CFR § 287.1(2a)(2b) (2009)
[5] ACLU, The Constitution in the 100-Mile Border Zone (2018), https://www.aclu.org/other/constitution-100-mile-border-zone?redirect=node/4524
[6] Patrick G. Lee, Can Customs and Border Officials Search Your Phone? These Are Your Rights, ProPublica (2017), https://www.propublica.org/article/can-customs-border-protection-search-phone-legal-rights
[7] Keith Fisher, U.S. Border Searches of Electronic Devices: Recent Development and Lawyers' Ethical Responsibilities, Business Law Today (2018), https://businesslawtoday.org/2018/03/u-s-border-searches-of-electronic-devices-recent-developments-and-lawyers-ethical-responsibilities/
[8] U.S. Customs and Border Protection, Directive NO. 3340-049A: Border Search of Electronic Devices (2018)
[9] *Ibid.*

Targeting Minorities

The policies at the boarder are particularly concerning to Arab-Americans because of the suspect class of the community. ADC has cause for concern that the broad executive mandate for unwarranted electronic searches will be disproportionately used against Arabs, Muslims, and immigrants, especially given the anti-Muslim animus expressed by the current President.[10]

Law enforcement trends continue to show that Arab-Americans and other minority communities are disproportionately targeted for searches, interrogations, and arrests. This has led to the criminalization of Arab-Americans, evidenced by : 1) disproportionate sentencing of Arab-Americans for crimes compared to their Caucasian counterparts who commit the same crime; 2) discriminatory anti-Arab materials used to train law enforcement; 3) arbitrary placement of Arabs and Muslims on watch-list's and secondary screening lists at airports; 4) denial of the right to due process for those designated to watch-lists, as demonstrated by *Latif v. Holder*; 5) denial of entry of Arab doctors, lawyers and other professionals with no ties to crime and/or terrorism into the U.S.; and 5) targeting of Arab communities through countering violent extremism programs.

Real Life Examples

ADC has been contacted by numerous individuals that have faced the illegal and intrusive searches allowed under Directive No. 3340-049A. All these individuals faced substantial delays and hardships at ports of entry based on the searches. One such individual was a professional based in the state of Texas with no prior history with police or immigration authorities. That individual was stopped and, without identifying any reason for the request, asked for his electronic devices. The devices were subsequently searched comprehensively. ADC received a similar complaint to this out of Michigan, where a similarly situated individual was stopped by CBP for no clear reason and had his electronics searched for some time.

Perhaps the most troubling situation brought to ADC's attention occurred in Virginia, where an individual was stopped returning from vacation with her family. That individual, a community activist, was never given a legitimate reason for the stop or search but was held up, with her entire family, for some time as her electronics were examined comprehensively. The stories that have been brought to ADC are concerning because they show that CPB acts with impunity, targets minorities, and, perhaps most troubling, has targeted outspoken activists.

---

[10] Dan Spinelli, "Motivated by Anti-Muslim Animus": Must-Reads From Justice Sotomayor's Dissent on Trump's Travel Ban, MotherJones (2018).
https://www.motherjones.com/politics/2018/06/sotomayor-dissent-trump-travel-ban/

Conclusion

ADC reiterates its opposition to the current policies codified in CPB Directive No. 3340-049A that infringe on constitutional rights and civil liberties. We believe that the proposed legislation is vital to ensuring that CBP policies are both effective at keeping America safe and legal. We also believe that the proposed legislation is necessary to stem the current discriminatory practices of CPB and to progress a more just and fair border protection system.

P: 202.244.2990 | F: 202.333.6470| 1705 DeSales Street, NW Suite 500 | Washington, DC 20036 | www.adc.org

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

July 10, 2018

The Honorable Rand Paul, Chairman
The Honorable Gary C. Peters, Ranking Member
U.S. House Committee on Homeland Security
Subcommittee on Federal Spending Oversight and Emergency Management
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman Paul and Ranking Member Peters:

We write to you regarding the hearing on "Examining Warrantless Smartphone Searches at the Border."[1] EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues and manages one of the most extensive open government litigation programs in the United States.[2] EPIC is focused on protecting individual privacy rights, and we are particularly interested in the privacy problems associated with warrantless searches and surveillance at the border.

Searches of cell phones and other electronic devices by border agencies have skyrocketed in recent years. In 2017, U.S. Customs and Border Protection (CBP) searched 30,200 electronic devices of individuals entering and leaving the U.S.—almost a 60% increase over 2016."[3] In January, CBP released updated guidance regarding border searches of electronic devices, allowing officers to request traveler's passcodes and seize a device if the traveler refuses to provide the information.[4] Though this policy is an improvement over previous policies, it still allows CBP agents to conduct a "basic" search without even reasonable suspicion. A "basic" search is when an agent manually searches the device to "review and analyze information encountered at the border."[5]

---

[1] *Examining Warrantless Smartphone Searches at the Border*, 115th Cong. (2018), H. Comm. on Homeland Security, Subcomm. on Federal Spending Oversight and Emergency Management, https://www.hsgac.senate.gov/subcommittees/fso/hearings/examining-warrantless-smartphone-searches-at-the-border (July 11, 2018).
[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] Press Release, Customs & Border Protection, CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (Jan. 5, 2018), *available at* https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.
[4] U.S. Customs and Border Protection, *Border Search of Electronic Devices*, CBP Directive No. 3340-049A (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.
[5] *Id* at 5.1.3.

And ICE has not even updated its policy. ICE's law enforcement activities include conducting warrantless electronic device searches "without individualized suspicion."[6] The electronic device searches conducted by ICE often include inspecting text messages, private emails, contact lists, and photos and other personal information.[7]

CBP and ICE are searching electronic devices without even reasonable suspicion despite the U.S. Supreme Court having recognized a Constitutionally significant privacy interest in mobile devices.[8] This practice should be stopped. EPIC has sued ICE under the Freedom of Information Act for details of the agency's use of mobile forensic technology to conduct warrantless searches of mobile devices.[9] That case is pending in the D.C. Circuit. An updated Privacy Impact Assessment and Border Search Device policy are long overdue from ICE.

Congress should also consider legislation to establish procedures, consistent with Fourth Amendment requirements, to restrict government access to personal data stored in cellphones during border searches. Senator Leahy (D-VT) and Senator Daines (R-MT) recently introduced S. 2462 a bill that would place restrictions on searches and seizures of electronic devices at the border.[10] The bill sets out detailed procedures for seizing electronic devices, including a warrant requirement prior to inspection of the device, data minimization, and exclusion of evidence that is obtained in violation of the Act. The bill also establishes reporting requirements to determine the scope and frequency of device searches.

Use of Mobile Forensic Technology by ICE

Since 2013, ICE has tested the devices made by[11] and signed contracts with multiple providers of mobile forensic technology, totaling nearly $10.8M.[12] In March 2017, ICE made their largest purchase yet, a new $2M purchase from Cellebrite for "IT and Telecom-Web-Based Subscription."[13] All previous purchases from Cellebrite were tagged for "Communications Security Equipment and Components" or "Operation Training Devices."[14] In April 2018, ICE signed another contract with Cellbrite for $1.26M for "Communications Security Equipment and

---

[6] U.S. Immigration and Customs Enforcement, *Directive No. 7-6.1 Border Searches of Electronic Devices* (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/icc_border_search_electronic_devices.pdf.
[7] Charlie Savage and Ron Nixon, *Privacy Complaints Mount Over Phones Searches at U.S. Border Since 2011* (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/us/politics/us-border- privacy-phone-searches.html.
[8] *Riley v. California*, 135 S.Ct. 2473 (2014).
[9] EPIC, *EPIC Sues ICE Over Technology Used to Conduct Warrantless Searches of Mobile Devices* (Apr. 9, 2018), https://epic.org/2018/04/epic-sues-ice-over-technology-.html.
[10] To Place Restrictions on Searches and Seizures of Electronic Devices at the Border, S. 2462, 115th Cong. (2018).
[11] Dept. of Homeland Security, *Test Results for Mobile Device Acquistion*, https://www.dhs.gov/publication/mobile-device-acquisition.
[12] *See* Federal Procurement Data System report, available at https://www.fpds.gov/ezsearch/search.do?q=cellebrite+CONTRACTING_AGENCY_NAME%3A%22U.S.+IMMIGRATION+AND+CUSTOMS+ENFORCEMENT%22&s=FPDSNG.COM&templateName=1.4.4&indexName=awardfull.
[13] *Id.*
[14] *Id.*

Components."[15] Cellebrite offers a suite of Universal Forensic Extraction Devices (UFED) which unlock, decrypt, and extract phone data including "real-time mobile data, . . . call logs, contacts, calendar, SMS, MMS, media files, apps data, chats, passwords."[16] These tools include Cellebrite's UFED Cloud Analyzer, which can extract private information – even without assistance from the owner - from users cloud based accounts, such as Facebook, Gmail, iCloud, Dropbox, and WhatsApp.[17]

Despite numerous new purchases from Cellebrite and other similar manufacturers, DHS's public policies, assessments, and other public documents have not kept pace. In 2009, DHS published guidance and polices for electronic device searches at the border.[18] The directive applies to all electronic devices and "information contained therein", but does not mention cloud based data. It also offers no specifics about forensic mobile searches. Likewise, a DHS internal review of policies for copying data on electronic devices does not clarify if the procedures outlined apply only to data physically on the device or also to data accessed *through* the device.[19] An ICE directive pertaining to border searches of electronic devices was released in 2009.[20] The ICE Directive 7-6.1 did not provide policies or procedures for the retrieval of personal data stored at cloud-based services from personal electronic devices.[21] The purchases at issue began in 2016, with testing of "mobile device acquisition" tools increasing over the past three years[22], well after the last Privacy Impact Assessment (PIA).

Conclusion

Absent exigent circumstances, a warrant should be required for searches of electronic devices at the border.

ICE's data retrieval techniques for mobile devices pose significant threats to privacy. These techniques allow ICE to collect a significant amount of personal data directly from

---

[15] Federal Procurement Data System Report, Award ID 70CMSD18FR0000056 (Apr. 25, 2018), https://www.fpds.gov/ezsearch/search.do?q=cellebrite+CONTRACTING_AGENCY_NAME%3A%22U.S.+IMMIGRATION+AND+CUSTOMS+ENFORCEMENT%22+PIID%3A%2270CMSD18FR0000056%22&s=FPDSNG.COM&templateName=1.4.4&indexName=awardfull.

[16] Cellebrite Mobile Forensics, *Unlock Digital Intelligence: Accelerate Investigations Anywhere, available at* https://web.archive.org/web/20170614063253/https://www.cellebrite.com/Media/Default/Files/Forensics/Solution-Briefs/Mobile-Forensics-Solution-Brief.pdf.

[17] *See* Cellebrite, *UFED Cloud Analyzer: Unlock cloud-based evidence to solve the case sooner*, https://www.cellebrite.com/en/products/ufed-cloud-analyzer/.

[18] Dept. of Homeland Security, *Privacy Impact Assessment for the Borders Searches of Electronic Devices* (Aug. 25, 2009), https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_laptop.pdf.

[19] *Id.*

[20] U.S. Immigration and Customs Enforcement, ICE Directive No. 7-6.1 (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

[21] *Id.*

[22] U.S. Department of Homeland Security Science and Technology Division, *Test Results for Mobile Device Acquisition*, https://www.dhs.gov/publication/mobile-device-acquisition.

electronic devices and cloud-based services without individualized suspicion or warrant authority. It remains unclear what the agency does with the personal information it obtains.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Jeramie Scott*
Jeramie Scott
EPIC National Security Counsel

WRITTEN STATEMENT FOR THE RECORD OF
U.S. Customs and Border Protection
For A Hearing Entitled "Examining Warrantless Smartphone Searches at the Border"
U.S. Senate
Committee on Homeland Security and Governmental Affairs
Subcommittee on Federal Spending Oversight and Emergency Management
July 11, 2018, Washington, DC

Introduction

Chairman Paul, Ranking Member Peters, and Members of the Subcommittee: Thank you for the opportunity to testify before you today on U.S. Customs and Border Protection's (CBP) authorities on border searches of electronic devices. Keeping Americans safe by enforcing our nation's laws in an increasingly digital world depends on our ability to lawfully inspect all materials—electronic or otherwise—entering the United States.

All persons, baggage, and merchandise arriving in or departing from the United States are subject to inspection, search, and detention by CBP—and signage posted throughout the port areas informs travelers of this fact. These border searches further CBP's customs, immigration, law enforcement, and homeland security responsibilities, and ensure compliance with customs, immigration, and other laws that CBP is authorized to administer and enforce. All individuals crossing the border, regardless of citizenship, must present themselves and their effects for border inspection. CBP's search authority is essential to enforcing the law at the U.S. border, preserving our national security, ensuring public safety, and protecting our country's economic interests.

CBP's authority to engage in border searches has been repeatedly affirmed by the Supreme Court of the United States. In addition to longstanding federal court precedent recognizing the constitutional authority of the U.S. government to conduct border searches, numerous federal statutes and regulations also authorize CBP to inspect and examine all individuals and merchandise entering or departing the United States, including all types of personal property, which would include electronic devices. Congress' long-standing recognition of the vital importance of inspections at the border reaches back to the First Congress. The long history of statutes authorizing CBP and its predecessor agencies to inspect and examine all individuals and merchandise entering or departing the United States demonstrates the importance of this authority. Congress has entrusted CBP with conducting border inspections to interdict threats to our nation, and we take this responsibility very seriously.

CBP Border Searches of Electronic Devices

Electronic devices are defined as any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, and music and other media players—and there is no question that these devices are prevalent in this digital age. In the past, someone might bring a briefcase across the border. This briefcase might contain pictures of their friends or family, work

materials, personal notes, diaries or journals, or any other type of personal information. Today, all of that material can fit neatly in a smartphone. As the world of information technology evolves, techniques used by CBP and other law enforcement agencies must also evolve to identify, investigate, and prosecute individuals who use new technologies to commit crimes.

Because of CBP's authority to inspect electronic devices at the border, CBP personnel have uncovered evidence related to terrorism, bulk cash smuggling, contraband, human trafficking, and child pornography. Our CBP personnel have also uncovered information about financial and commercial crimes, such as those relating to copyright, trade, and export control violations. Through these search authorities, CBP has gained vital information that has helped us assess and analyze terrorist threat information. Furthermore, searches at the border are often integral to determining an individual's intentions upon entry into the United States, providing additional information relevant to their admissibility under our country's immigration laws.

CBP personnel are trained to assess a "totality of circumstances" when determining appropriate actions to take during a border inspection. CBP may engage in various actions during a border inspection, such as an examination of the travelers' belongings including their personal vehicle, suitcase, briefcase, and now, electronic devices. In the context of border searches of electronic devices, a search may be conducted for a variety of reasons. For example, if the traveler is suspected of illegal activity, that traveler may be referred for additional scrutiny and a search of their device. A search of an electronic device may also assist CBP personnel in verifying information that may be pertinent to the admissibility of a foreign national who is applying for admission.

CBP takes the responsibility associated with these search authorities seriously. On January 5, 2018, CBP released an update to the agency Directive governing Border Searches of Electronic Devices, superseding the previous Directive released in August 2009. The January 2018 Directive, *Border Search of Electronic Devices*, includes updated guidance and standard operating procedures on searching, reviewing, retaining, and sharing information contained on electronic devices. It also furthers our commitment to a culture of transparency, accountability, and oversight of electronic device border searches performed by CBP.

The Directive governs border searches of electronic devices—including any inbound or outbound search pursuant to longstanding border search authority—conducted by CBP at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy.

With respect to border searches of information contained in electronic devices, the original 2009 policy did not differentiate between the types of searches that CBP conducts on an electronic device. Under the new 2018 policy, CBP has updated the definitions of these searches and outlined the procedures that apply to each respective type of search. CBP now follows different procedures depending on whether the search is a "basic search" or an "advanced search." A basic search may be conducted with or without suspicion, while the Directive requires, strictly as a matter of policy, additional justification for an advanced search.

Notably, while a basic search is not a necessary precursor to an advanced search, information identified during a basic search may lead to an advanced search, consistent with Section 5.1.4 of the Directive.

Policy-based Limits and Controls on Border Searches of Electronic Information

The updated Directive includes provisions above and beyond prevailing constitutional and legal requirements. CBP's authority for the border search of electronic devices is and will continue to be exercised judiciously, responsibly, and consistent with the public trust.

As a matter of policy, CBP has created robust auditing and accountability measures for this program that build upon the long-standing privacy, trade secrets, and security awareness training CBP employees receive annually. To ensure a traveler's information is used for the proper purpose, all CBP employees with access to the information are trained annually regarding the use, dissemination, and retention of personally identifiable information (PII). Employees are trained not to access the traveler's information without an official need to know, and to examine only that information that might pertain to their inspection or investigation. CBP employees record all electronic media searches, as we do with all secondary inspections, in an auditable system of record that ensures appropriate oversight.

Access to such information is tracked and subject to audit. In addition, CBP employees must pass a full background investigation and are trained regarding the access, use, maintenance, and dissemination of PII before being given access to the system maintaining the information. CBP personnel are instructed not just in the appropriate use of the authority, but also instructed on the consequences – administrative, civil, and criminal – for privacy, trade secrets, and security violations.

Reasonable Suspicion or National Security Concern

An advanced search is defined in CBP policy as "any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."

By applying a heightened standard to all advanced searches of electronic devices, CBP is self-imposing greater policy controls over its border search authority. This shows that CBP is taking responsible steps to ensure and maintain individual privacy and public trust, while still meeting its enforcement mandates.

During inspection of international travelers, CBP Officers ask various questions, including questions about the nature of the international trip – such as, was this trip for business or vacation? That information helps CBP assess the merchandise the individual is seeking to bring into the country. In order to verify the statements made by travelers and assess the items they are seeking to bring across the border, CBP has historically examined paper documents, such as airline tickets for onward flights, letters of employment, housing and lodging information, photos of the individual and persons, and papers. The paper documents provided information about a travelers intentions and other information relevant to the laws CBP is responsible for enforcing at the border. Now that these paper documents are captured electronically, CBP must

have the authority to inspect electronic devices to identify individuals who plan to do harm to the United States or violate the law. Any other rule would render CBP unable to assess the admissibility of individuals and their effects at the border, which would negatively impact both national security and CBP's ability to facilitate legitimate trade and travel.

Among a host of other responsibilities at the border, CBP has a national security mandate, applicable to aliens and citizens alike, that often involves finding the proverbial needle in the haystack. Imposing a probable cause standard on border searches of electronic devices would almost certainly operate to preclude CBP from uncovering a terrorism threat or terrorism information critical to its homeland security mission.

Border searches of electronic devices are a crucial tool in identifying and combatting threats to homeland security. Limitations on CBP's authority to conduct basic searches of electronic devices at the border would adversely impact CBP's ability to achieve its operational mission of securing the border and identifying and interdicting threats to border security and national security. CBP's Directive reflects a careful balancing of CBP's border security mission and its mission of facilitating legitimate trade and travel. As outlined in the Directive, border searches of electronic devices "can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from elements of the federal government responsible for analyzing terrorist threat information. [They are also] integral to a determination of an individual's intentions on entry and provide additional information relevant to admissibility under the immigration laws." CBP's Directive reflects a careful analysis of what is necessary to protect national security and fulfill CBP's mission of interdicting threats – a mission that is enshrined in statute.

Restriction on CBP Access to Information in the "Cloud"

In the 2018 Directive, CBP formally clarifies that a border search includes an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. CBP personnel may not intentionally use the device to access information that is solely stored remotely. Prior to beginning a basic or advanced search, CBP officers and agents must take steps to ensure that a device is not connected to any network and take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

Treatment of Privileged Information

While the original CBP policy provided that privileged information must be protected in accordance with applicable law, the updated Directive provides additional detail regarding the procedures CBP personnel follow when they encounter information that they identify as privileged or over which a privilege has been asserted. The 2018 Directive maintains the provisions from the 2009 Directive regarding the treatment of other possibly sensitive information, such as medical records and work-related information carried by journalists, which shall still be handled in accordance with any applicable federal law and CBP policy.

Handling of Passcode-Protected or Encrypted Information

As technology has enabled more sophisticated data security safeguards to be employed over electronic devices, CBP has self-imposed controls over how and when it will access, store, and destroy information that is passcode-protected or encrypted.

Travelers are obligated to present electronic devices in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode, encryption or other security mechanism, an officer may request the individual's assistance in accessing the device and its contents, such as a passcode or other means of access.

Any passcodes or other means of access provided by the traveler will be used as needed to facilitate the examination; however, they must be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be used to access information that is only stored remotely. If an officer or agent is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the officer may detain the device pending a determination as to its admissibility, exclusion, or other disposition.

Storage of Information Extracted from an Electronic Device

Section 5.5.1.2 of the 2018 CBP Directive provides for retention of information in CBP Privacy Act-Compliant Systems and states that without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and/or other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. CBP's directive further spells out the limited circumstances in which information from an electronic device can be searched at the border can be retained.

Conclusion

In Fiscal Year 2017, only 30,524 electronic media searches were conducted on the more than 416 million passengers processed. Despite being applied to a remarkably small number of the hundreds of millions of travelers who enter and exit our country every year, CBP border searches of electronic devices has yielded significant and valuable law enforcement results. This authority—repeatedly recognized by the Supreme Court of the United States—is judiciously applied, subject to robust oversight, and conducted with strict adherence to all constitutional and statutory requirements. CBP is committed to preserving the rights and privacy of all people while conducting necessary and lawful actions to secure our borders, and will continue to ensure that these authorities—so essential to national security and public safety—are executed in a professional and courteous manner.

○