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.