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/ice_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