IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W., Suite 200
Washington, D.C. 20009,

Plaintiff,

v.

U.S. CUSTOMS AND BORDER PROTECTION,
1300 Pennsylvania Avenue, N.W.
Washington, D.C. 20229

Defendant.

Civ. Action No. 1:19-cv-00279

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, to compel disclosure of records requested by Plaintiff Electronic Privacy Information Center ("EPIC") from Defendant Customs and Border Protection ("CBP"), a subcomponent of the U.S. Department of Homeland Security ("DHS").

2. EPIC seeks the release of records related to CBP's Directive No. 3340-049A titled *Border Search of Electronic Devices*, issued on January 4, 2018. In this Complaint, EPIC challenges (1) CBP's failure to make a timely decision about EPIC's FOIA Request; and (2) CBP's failure to release records responsive to EPIC's FOIA Request. EPIC seeks injunctive and other appropriate relief.

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 and 5 U.S.C. §§ 552(a)(6)(E)(iii), (a)(4)(B). This Court has personal jurisdiction over Defendant CBP.

4. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B).

Parties

5. Plaintiff EPIC is a nonprofit organization, incorporated in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is education, oversight, and analysis of government activities that impact individual privacy, free expression, and democratic values in the information age.[1] EPIC's Advisory Board includes distinguished experts in law, technology, and public policy.

6. EPIC maintains one of the most popular privacy websites in the world, https://epic.org, which provides EPIC's members and the public with access to information about emerging privacy and civil liberties issues. EPIC has a robust FOIA practice and routinely disseminates information obtained under the FOIA to the public through the EPIC website, the biweekly *EPIC Alert* newsletter, and various news organizations. EPIC is a representative of the news media. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003) (determining that EPIC was a representative of the news media for preferred fee status under the FOIA).

7. Defendant Customs and Border Protection is a federal agency within the meaning of the FOIA, 5 U.S.C. § 552(f)(1). CBP is headquartered in Washington, D.C.

Facts

8. Each year, hundreds of millions of individuals cross the United States border;[2] many of these individuals travel with an electronic device such as a cell phone, tablet, or laptop computer.

[1] *See* EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.
[2] U.S. Customs & Border Prot., *CBP Releases Statistics on Electronic Device Searches* (Apr. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0.

For example, in FY2016, U.S. Customs and Border Protection ("CBP") officers processed 390.6 million arriving international travelers and searched the electronic devices of 19,033 travelers.[3]

9. Electronic devices store vast troves of personal data and can be used to access even more data through cloud-based applications. A cellphone may provide access to financial records, medical records, and even password directories. A cellphone may also open home locks, disable security systems, control the operation of cars, and control the management of medical devices in the human body.

10. According to CBP, the agency is permitted to warrantlessly search electronic devices to manage and control activities at the U.S. border. CBP states that it may search "[a]ll persons, baggage, and merchandise arriving in, or departing from" the U.S—including electronic devices hand-carried across the border.[4] The frequency of CBP's searches of electronic devices is increasing at an alarming rate. In 2017, CBP searched 30,200 electronic devices of individuals traveling to and from the U.S.—a nearly 60% increase from 2016.[5]

11. CBP Directive No. 3340-049 titled *Border Search of Electronic Devices Containing Information* ("2009 Directive") sets out the agency's policy for "searching, reviewing, retaining, and sharing information" contained in electronic devices, and superseded previous CBP policies pertaining to device searches.[6] Under the 2009 directive, CBP may seize information with probable cause related to immigration, customs, or other border enforcement mandates.[7] The 2009 Directive stated that information acquired from the searches of electronic devices that is

---

[3] *Id.*
[4] U.S. Customs & Border Prot., *CBP Search Authority* (Jan. 5, 2018), https://www.cbp.gov/travel/cbp-search-authority.
[5] U.S. Customs & Border Prot., *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics* (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.
[6] U.S. Customs & Border Prot., Directive 3340-049, *CBP Directive: Border Search of Electronic Devices Containing Information* 1 (2009), https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.
[7] *Id.* at 5.4.1.

"determined to be protected by law as privileged or sensitive" will only be shared with "federal agencies."[8] Information not deemed "privileged or sensitive" can be shared more broadly. Specifically, the 2009 Directive does not limit the general sharing of information contained in electronic devices with "federal, state, local, and foreign law enforcement agencies."[9] The 2009 Directive also included an auditing requirement where CBP "will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted inconformity" with the Directive.[10]

12. On January 4, 2018, CBP issued an updated directive on device searches that the agency claimed would increase "transparency, accountability, and oversight of electronic device border searches performed by CBP."[11] This updated policy describes when and how CBP officials may search electronic devices, how agents will handle and review passcode-protected or encrypted information, how long the agency will retain data seized or copied from devices, under which circumstances CBP will transfer seized data to other federal agencies, and when the seized data will be deleted or destroyed.

13. The current CPB policy sets different standards for "basic" and "advanced" device searches. An advanced search (also referred to as a "forensic search")—which can only be conducted based on reasonable suspicion—occurs when an officer uses specialized equipment to "review, copy, and/or analyze [the] contents" of an electronic device via wired or wireless means.[12] Any search of an electronic device that is not "advanced" is considered a basic search

[8] *Id.* at 5.2.4.
[9] *Id.* at 5.4.1.3.
[10] *Id.* at 7.
[11] U.S. Customs & Border Prot., *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistic*s, *supra* note 5.
[12] U.S. Customs & Border Prot., Directive 3340-049A, *Border Search of Electronic Devices Containing* 5.1.4 (2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

and does not require any suspicion.[13] During a basic search, a CBP officer may manually examine the electronic device and review and analyze the contents stored locally through the device's operating system or other software, tools or applications on the device.[14] CBP officers may not intentionally use the device to access information that is "solely stored remotely"—i.e., cloud services.[15] The CBP officer will either request the individual to disable network connectivity, such as putting the device on airplane mode, or will manually disable network connectivity if warranted by "national security, law enforcement, officer safety, or other operational considerations."[16] The updated guidance states that searches of electronic devices should be conducted in the presence of the individual but "remaining present during a search does not necessarily mean that the individual shall observe the search itself."[17]

14. CBP is responsible for ensuring the compliance and enforcement of customs, immigration, and many other Federal laws and regulations at the border. The CBP Directive also authorizes the agency to retain information if officers determine there is probable cause to seize the device or information contained within the device. Without probable cause, CBP may retain information related to "immigration, customs, and other enforcement matters if such retention is

[13] *Id.* at 5.1.3.
[14] *Id.* at 5.1.2.
[15] *Id.*
[16] *Id.*
[17] *Id.* at 5.1.6.

consistent with the applicable system of records notice."[18] CBP has interpreted "relating" broadly, which leads to a lower standard than reasonable suspicion.

15. Like the 2009 Directive, the updated policy allows CBP to broadly disseminate copies of seized information with "federal, state, local, and foreign law enforcement agencies" and third parties for assistance.[19]

16. The CBP Directive also states that travelers are "required" to "present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents" and authorizes officers to request traveler's passcodes and/or seize their electronic devices if the traveler refuses to provide the requested information.[20] The CBP Directive authorizes the agency to retain passcodes "as needed" to facilitate the search, which includes passcodes to information accessible through software applications on the device.[21] The updated policy does not limit CBP's ability to "seek technical assistance" or "use external equipment or take other reasonable measures" to allow for inspection of the device.[22]

17. The CBP Directive includes an auditing requirement similar to the 2009 Directive. The *2018 Privacy Impact Assessment for CBP Border searches of Electronic Devices* states that the DHS should "audit the actual use of PII to demonstrate compliance" under the Principle of Accountability and Auditing.[23] The auditing procedures and auditing reports have yet to be made publicly available.

18. The data collected from these electronic device searches can reveal highly sensitive and intimate information about travelers including religious affiliations, political beliefs, financial

[18] *Id.* at 5.5.1.2.
[19] *Id.* at 5.5.1.3, 5.4.2.
[20] *Id.* at 5.1.3.
[21] *Id.* at 5.3.1.
[22] *Id.* at 5.3.4.
[23] U.S. Dep't of Homeland Sec., DHS/CBP/PIA-008(a), *Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices* 20 (2018),

status, medical conditions, and confidential work product—including information protected under attorney-client privilege.[24] The CBP Directive asserts that the agency has broad authority to search and seize electronic devices, retain this sensitive data and disseminate it to third parties and other federal agencies.

19. In an Office of Inspector General ("OIG") Report concerning CBP searches of electronic devices at the border, the OIG found that between April 2016 and July 2017, CBP "did not always conduct searches of electronic devices at U.S. ports of entry according to its [standard operating procedures]."[25] The OIG also found that CBP did not properly document these electronic device searches and could not "maintain accurate quantitative data or identify and address performance problems related to these searches."[26] The OIG found that CBP did not consistently disconnect devices from data networks before searching the devices due to the "inconsistent guidance" provided from CBP headquarters.[27] The OIG also found that CBP officers did not ensure the security of data or adequately manage technology to effectively search the devices.[28] The OIG reported that CBP "has not yet developed performance measures to evaluate the effectiveness of a pilot program, begun in 2007, to conduct advance searches . . . ."[29]

---

https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp008-bordersearcheselectronicdevices-january2018.pdf.

[24] *See Riley v. California*, 135 S. Ct. 2473 (2014).

[25] Office of Inspector General, U.S. Dep't of Homeland Sec., OIG-19-10, *CBP's Searches of Electronic Devices at Ports of Entry – Redacted* (2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-12/OIG-19-10-Nov18.pdf.

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

The pilot program includes copying information from the electronic device to law enforcement databases.[30]

20. The agency has acknowledged the OIG's recommendations and committed to develop performance measures for advanced searches and to evaluate the effectiveness of the advanced search pilot program by January 31, 2019.[31]

21. CBP is searching electronic devices without reasonable suspicion despite the U.S. Supreme Court having recognized a significant privacy interest in mobile devices.[32]

22. On January 28, 2019, the American Bar Association ("ABA") passed a resolution urging the federal judiciary to recognize the substantial privacy risks implicated by electronic device searches at the border.[33] The ABA urged Congress to enact legislation to address the risks associated with device searches at the border. Until legislation is adopted, the ABA urged the DHS to adopt policy that would require a warrant based on probable cause for search and seizure of electronic devices at the border unless an exception other than the border search exception applies; prohibit the government from denying Americans or lawful permanent residents entry or exit based on their refusal to provide access to their electronic devices for search; protect the attorney-client privilege and work product privilege at border crossings; and require the government to record each instance of a forensic search and issue an annual summary report of these electronic device searches.

23. The warrantless searches of electronic devices at the border pose significant privacy risks and could violate an individual's Fourth Amendment rights. Since 2011, almost 250 complaints have been filed with DHS regarding warrantless border searches of electronic devices, many of

[30] *Id.*
[31] *Id.* at 12.
[32] *Riley v. California*, 135 S.Ct. 2473 (2014).
[33] Section of Civil Rights and Social Justice Criminal Justice Section, A.B.A., Revised Resolution 107A (2019), https://www.americanbar.org/content/dam/aba/images/news/2019mymhodres/107a.pdf.

which complain about the loss of privacy.[34] To date, CBP has not published the auditing requirements for its electronic search procedures nor has it published the results of those audits. Without disclosure of the auditing mechanism, the public is left in the dark on how the agency assesses the strength of its electronic device border search policy.

EPIC's FOIA Request

24. On July 31, 2018, EPIC submitted a FOIA request ("EPIC's FOIA Request") to CBP's FOIA Division via facsimile.

25. EPIC's FOIA Request sought records about CPD's Directive No. 3340-049A titled *Border Search of Electronic Devices*, issued on January 4, 2018. Specifically, EPIC sought:

1) All records, including but not limited to communications, memoranda, and policy, about the development and implementation of an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive;

2) All audits, including any statistical reports conducted under the auditing mechanisms, used to review whether border searches of electronic devices are being conducted in conformity with this Directive;

3) A copy of CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-0SC.

26. EPIC sought "news media" fee status under 5 U.S.C. § 552(4)(A)(ii)(II) and a waiver of all duplication fees under 5 U.S.C. § 552(a)(4)(A)(iii).

27. EPIC also sought expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II).

28. EPIC received no acknowledgement letter from the CBP.

29. On November 27, 2018, EPIC contacted the CBP FOIA office to inquire about the status of the request and for the request's tracking number. The CBP FOIA officer stated there was no

[34] Charlie Savage & Ron Nixon, *Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011*, N.Y. Times (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/us/politics/us-border-privacy-phone-searches.html.

record of the original request in the system and requested that EPIC's Counsel call back the next day when more people in the office could assist in locating the request.

30. On November 28, 2018, EPIC contacted the CBP FOIA office again to inquire about the status of the request and the CBP FOIA officer could not locate EPIC's request. The CBP FOIA officer recommended EPIC to resubmit the request by mail or FOIAonline, CBP's online submission portal. EPIC reconfirmed the fax number originally used to submit the request and the CBP Officer stated that the fax number used to transmit EPIC's FOIA Request was correct. On the same day, EPIC resubmitted the original request via United States Postal Service ("USPS") certified mail. Delivery of the request was confirmed by USPS on December 3, 2018.

EPIC's Constructive Exhaustion of Administrative Remedies

31. Today is the 66th day since CBP received EPIC's FOIA Request.

32. CBP has failed to make a determination regarding EPIC's FOIA Request for expedited processing within the time period prescribed by 5 U.S.C. § 552(a)(6)(E)(ii)(I).

33. Additionally, CBP has failed to make a determination regarding EPIC's FOIA Request within the time period required by 5 U.S.C. § 552(a)(6)(A)(i).

34. EPIC has exhausted all administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

Count I

Violation of FOIA: Failure to Comply with Statutory Deadlines

35. Plaintiff asserts and incorporates by reference paragraphs 1–30.

36. Defendant CBP has failed to make a determination regarding EPIC's FOIA Request for 66 days. Thus, CBP has thus violated the deadlines under 5 U.S.C. §§ 552(a)(6)(E)(ii)(I), (a)(6)(A)(ii).

37. Plaintiff has constructively exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

Count II

38. **Violation of FOIA: Failure to Grant Request for Expedited Processing**

1. Plaintiff asserts and incorporates by reference paragraphs 1–30.

2. Defendant's failure to grant plaintiff's request for expedited processing violated the FOIA, 5 U.S.C. § 552(a)(6)(E)(i).

3. Plaintiff is entitled to injunctive relief with respect to an agency determination on EPIC's request for expedited processing.

Count III

Violation of FOIA: Unlawful Withholding of Agency Records

39. Plaintiff asserts and incorporates by reference paragraphs 1–30.

40. Defendant CBP has wrongfully withheld agency records requested by Plaintiff.

41. Plaintiff has exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

42. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested records.

Count IV

Claim for Declaratory Relief

43. Plaintiff asserts and incorporates by reference paragraphs 1–30.

44. Plaintiff is entitled under 28 U.S.C. § 2201(a) to a declaration of the rights and other legal relations of the parties with respect to the claims set forth in Counts I–IV.

Requested Relief

WHEREFORE, Plaintiff requests this Court:

A. Order Defendant to immediately conduct a reasonable search for all responsive records;

B. Order Defendant to take all reasonable steps to release non-exempt records;

C. Order Defendant to disclose promptly to Plaintiff all responsive, non-exempt records;

D. Order Defendant to produce the records sought without the assessment of search fees;

E. Order Defendant to grant EPIC's request for a fee waiver;

F. Award EPIC costs and reasonable attorney's fees incurred in this action; and

G. Grant such other relief as the Court may deem just and proper.

Respectfully Submitted,

MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

/s/ Jeramie D. Scott
JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: February 1, 2019