AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA,
LINDA LYE - #215584
llye@aclunc.org
VASUDHA TALLA - #316219
vtalla@aclunc.org
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (415) 255-8437

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA,

Plaintiff,

v.

TRANSPORTATION SECURITY ADMINISTRATION,

Defendant.

Case No.

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

INTRODUCTION

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. §552, to enforce the public's right to information about the federal government's searches of electronic devices at airports. Government agencies routinely search travelers' phones, computers, tablets and other devices, which hold within them vast quantities of information—photographs, emails, text and audio messages, address books—that reveal intimate and deeply personal details of an individual's life.

2. The federal government's searches of electronic devices at airports—along with intrusive questioning, lengthy detentions, and even refusal to allow certain travelers to enter the country—has generated widespread media interest and public concern. Recent statistics demonstrate that the number of these searches have multiplied year after year. Access to information about electronic device searches at airports is necessary to inform meaningful public debate over the scope of government conduct that potentially threatens core civil rights and liberties protected by the Constitution. Federal agencies have published their policies regarding searches of electronic devices at international borders. But the federal government's policies on searching electronic devices of *domestic* air passengers remains shrouded in secrecy.

3. Over two months ago, on December 20, 2017, Plaintiff American Civil Liberties Union of Northern California ("ACLU-NC"), a non-profit civil rights organization, submitted two FOIA requests to Defendant Transportation Security Administration ("TSA") seeking records about policies, procedures, and protocols regarding the search of airplane passengers' electronic devices; training of relevant personnel related to the search or examination of electronic devices; and equipment used to search, examine, or extract data from electronic devices.

4. Since that time, TSA has provided ACLU-NC with *no* records.

5. ACLU-NC now brings this action to obtain the information to which it is statutorily entitled.

///

PARTIES

6. Plaintiff American Civil Liberties Union of Northern California is an affiliate of the American Civil Liberties Union, a national, non-profit, non-partisan organization with the mission of protecting civil liberties from government incursions, safeguarding basic constitutional rights, and advocating for open government. ACLU-NC is established under the laws of the state of California and is headquartered in San Francisco, California. ACLU-NC has over 90,000 members. In support of its mission, ACLU-NC uses its communications department to disseminate to the public information relating to its mission, through its website, newsletters, in-depth reports, and other publications.

7. Defendant Transportation Security Administration is an agency within the meaning of 5 U.S.C. §552(f). The agency has its headquarters in Arlington, Virginia, and field offices all over the country, including San Francisco, California.

JURISDICTION

8. This Court has subject matter jurisdiction and personal jurisdiction over the parties pursuant to 5 U.S.C. §§552(a)(4)(B) and 552(a)(6)(C)(i). This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§1331 and 1346.

VENUE AND INTRADISTRICT ASSIGNMENT

9. Venue is proper in this district pursuant to 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. §§1391(e) and 1402. Plaintiff has its principal place of business in this district.

10. Pursuant to Local Rule 3-2(c) and (d), assignment to the San Francisco division is proper because Plaintiff is headquartered in San Francisco.

FACTUAL ALLEGATIONS

The Federal Government's Searches of Electronic Devices at Airports and Borders Are a Matter of Significant Public Interest

11. Mobile phones, computers, tablets, digital cameras—these electronic devices and others possess the most intimate details of an individual's life. They are also ubiquitous, carried by millions of passengers who travel in and out of airports in the United States each day. With these devices, passengers take with them photographs of themselves, their families, and their

friends; text and audio messages with an array of colleagues and loved ones; emails and archives; social media messages and networks; confidential business and legal information; protected medical records; bank statements; and a wealth of other information that lay bare how and with whom people communicate, work, and live each day.

12. The Supreme Court has recognized the significant privacy interests an individual possesses in electronic devices. In a 2014 opinion addressing searches of cell phones, the Court noted that cell phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). The data contained in cell phones reaches far back in time, "place[s] vast quantities of personal information literally in the hands of individuals," and collects several pieces of information that "reveal much more in combination than any isolated record." *Id.* at 2485, 2489. Cell phones are unique not only for containing certain types of data with no physical analogue—such as internet search and browsing history, location data, and apps—but also for serving as a portal to data stored on remote or "cloud" servers. *Id.* at 2489, 2491. In light of the privacy concerns posed by searches of cell phones, the Court declined to allow warrantless searches by police incident to an individual's arrest.

13. Federal agencies, such as Defendant TSA, U.S. Customs and Border Protection ("CBP"), and U.S. Immigration and Customs Enforcement ("ICE"), regularly search passengers' electronic devices at airports. Each year, the number of searches by CBP has grown: from 5,000 searches in Fiscal Year (FY) 2015, to 25,000 searches in FY 2016, to 30,000 searches in FY 2017.

14. CBP and ICE have published policies regarding their authority to search and seize electronic devices at the border, including airports. CBP requires passengers to provide their devices unlocked or the password or PIN so that an officer can view data contained on the device. *See* U.S. Customs and Border Protection, CBP Directive No. 3340-049A, Border Search of Electronic Devices, Jan. 4, 2018, http://bit.ly/2rjmnYj. CBP policy authorizes both a "basic search" and an "advanced search" of passengers' devices. In the former, an officer examines

only information that is resident upon the device, using external equipment only to gain access to the device if necessary. In the latter, external equipment is used not merely to gain access to the device, but to review, copy, and/or analyze its contents.

15. Media accounts highlight the privacy concerns posed by electronic device searches, seizures, and copying of data: a NASA scientist potentially carrying sensitive information on his phone, Loren Grush, "A US-Born NASA Scientist Was Detained at the Border Until He Unlocked His Phone," Feb. 12, 2017, The Verge, http://bit.ly/2ooHzr3; a Canadian photojournalist denied entry to the United States to cover protests when he failed to provide access to his phones, Daniel Victor, "Canadian Journalists Detention at U.S. Border Raises Press Freedom Alarms," N.Y. Times, Dec. 2, 2016, http://nyti.ms/2EN1A5q; a U.S. journalist working for the Wall Street Journal who objected to turning over her cell phones, *id.*; a Muslim-American woman returning from visiting her refugee family overseas, whose phone was searched, Lubana Adi, "My phone was searched at LAX, which apparently is the new normal," Los Angeles Times, April 7, 2017, http://lat.ms/2opysbm; a U.S. citizen asked to unlock his cell phones before he could board a flight from Los Angeles to Saudi Arabia, Daniel Victor, "What Are Your Rights if Border Agents Want to Search Your Phone?," N.Y. Times, Feb. 14, 2017, http://nyti.ms/2lj2AE9.

16. These troubling incidents have produced intense public interest in searches of electronic devices at airports by federal agencies, including individual rights in response to such searches. Plaintiff ACLU-NC and other organizations, along with media outlets, have published guidance for citizens and immigrants as they travel domestically and internationally and encounter requests from TSA, CBP or ICE to search their devices. *See* ACLU of Northern California, "Know the Facts and Know Your Rights for Arab, Middle Eastern, Muslim, and South Asian Communities," May 2017, http://bit.ly/2CDeOMb; Electronic Frontier Foundation, "Digital Privacy at the U.S. Border: Protecting the Data on Your Devices, Dec. 2017, http://bit.ly/2CAwdFu; Patrick J. Lee, "Can Customs and Border Enforcement Search Your Phone? These Are Your Rights," ProPublica.org, Mar. 13, 2017, http://bit.ly/2nJ2Slh; Daniel

Victor, "What Are Your Rights if Border Agents Want to Search Your Phone?," N.Y. Times, Feb. 14, 2017, http://nyti.ms/2lj2AE9.

17. CBP claims the authority to conduct warrantless searches of electronic devices at *international* border crossings without probable cause to support the search. That practice is being challenged by the national ACLU, of which Plaintiff ACLU-NC is an affiliate, as violating the First and Fourth Amendments to the Constitution. *See Alasaad v. Duke*, No. 1:17-cv-11730-DJC (D. Mass. filed Sep. 13, 2017).

18. Alongside CBP, TSA has also been reported as heightening its screening procedures of *domestic* passengers' electronic devices. *See, e.g.*, Russ Thomas, "TSA implements new screening procedures in Montana," KPAX.com, Dec. 14, 2017, http://bit.ly/2sMepaI; Joel Hruska, "TSA Will Now Screen All Electronics 'Larger Than a Cell Phone,'" Extreme Tech, July 26, 2017, http://bit.ly/2sG2Fq4.

19. TSA has not made publicly available any policies or procedures governing searches of electronic devices, especially those held by passengers engaged in purely domestic air travel. As such, the public is unaware of the legal basis for TSA's searches of electronic devices of passengers not presenting themselves at the border and flying on a domestic flight. Further, the public is unaware of TSA's policies and procedures for advanced or forensic searches, in which external equipment is used to search, examine, or extract data from passengers' electronic devices and SIM cards. And the public has no knowledge of TSA's policies and procedures relating to seizure of electronic devices, retention or destruction of data resident on those devices, or use of the device to access data held on a "cloud" or elsewhere.

20. The information sought in ACLU-NC's FOIA request would reveal for the first time information concerning TSA's searches of *domestic* passengers' electronic devices, and allow members of the public a meaningful opportunity to vet the government's broad claim of authority to conduct such searches.

///

///

Plaintiff Submitted a FOIA Request to TSA Headquarters But TSA Has Failed to Produce Any Records

21. On December 20, 2017, ACLU-NC submitted a FOIA request to the TSA headquarters ("TSA Headquarters") in Arlington, Virginia seeking information about its searches of passengers' electronic devices (the "TSA Headquarters Request"). A copy of Plaintiff ACLU-NC's TSA Headquarters Request request is appended hereto as Exhibit 1.

22. In particular, the TSA Headquarters Request seeks records, from January 1, 2012 to the present, regarding any of the following:

1. Policies, procedures, or protocols regarding the search of passengers' electronic devices. This includes but is not limited to any policies, procedures, or protocols related to the "enhanced screening of electronic devices" referenced by then-Secretary of Homeland Security John Kelly in June 2017.[1]
2. Equipment, including but not limited to SIM-card readers and software manufactured by Cellebrite [2], used to search, examine, or extract data from passengers' electronic devices and SIM cards at all airports in California. This request seeks records including but not limited to: documentation related to the acquisition, testing, use, maintenance, and location of such equipment; any inventories of the number of each type of equipment.[3] This request includes any records in the possession of TSA but generated by third-party service providers.
3. Training of transportation security officers or contractors retained to provide security screening services, related to the search or examination of passengers' electronic devices.

23. More than 20 working days have passed since TSA received the TSA Headquarters Request.

24. As of the date of the filing of this Complaint, Plaintiff ACLU-NC has not received any response from TSA to the TSA Headquarters Request.

---

[1] https://www.dhs.gov/news/2017/06/28/remarks-council-new-american-security-conference

[2] Examples of such devices include, but are not limited to, a Universal Forensic Extraction Device (UFED) manufactured by Cellebrite. E.g., https://www.cellebrite.com/en/press/cellebrite-introduces-ufed-touch2-platform/.

[3] According to the Government Accountability Office, TSA possesses ""acquisition documentation for passenger and baggage screening technologies," including memorandums and "information regarding the number of each technology deployed in airports nationwide." http://www.gao.gov/assets/680/674297.pdf at 28.

25. As of the date of the filing of this Complaint, Plaintiff ACLU-NC has not received a determination from TSA of whether TSA will comply with the TSA Headquarters Request.

26. As of the date of the filing of this Complaint, Plaintiff ACLU-NC has not received any documents from TSA that are responsive to the TSA Headquarters Request or any correspondence indicating when TSA might provide any documents.

27. Plaintiff ACLU-NC has exhausted all applicable administrative remedies.

28. TSA has wrongfully withheld the requested records from Plaintiff ACLU-NC.

Plaintiff Submitted a FOIA Request to TSA's San Francisco Field Office But TSA Has Failed to Produce Any Records

29. On December 20, 2017, Plaintiff ACLU-NC submitted a FOIA request to the TSA field office in San Francisco, California (the "TSA Field Office") seeking information about its searches of passengers' electronic devices (the "TSA Field Office Request"). A copy of Plaintiff ACLU-NC's TSA Field Office Request is appended hereto as Exhibit 2.

30. In particular, the TSA Field Office Request seeks records, from January 1, 2012 to the present, regarding any of the following:

1. Policies, procedures, or protocols regarding the search of passengers' electronic devices. This includes but is not limited to any policies, procedures, or protocols related to the "enhanced screening of electronic devices" referenced by then-Secretary of Homeland Security John Kelly in June 2017.[4]
2. Equipment, including but not limited to SIM-card readers and software manufactured by Cellebrite[5], used to search, examine, or extract data from passengers' electronic devices and SIM cards at the San Francisco International Airport. This request seeks records including but not limited to: documentation related to the acquisition, testing, use, maintenance, and location of such equipment; any inventories of the number of each type of equipment.[6] This request includes any records in the possession of the TSA San Francisco Field Office but generated by Covenant Aviation Security.

[4] https://www.dhs.gov/news/2017/06/28/remarks-council-new-american-security-conference.

[5] Examples of such devices include, but are not limited to, the UFED Touch Platform manufactured by Cellebrite: https://www.cellebrite.com/en/press/cellebrite-introduces-ufed-touch2-platform/.

[6] According to the Government Accountability Office, TSA possesses ""acquisition documentation for passenger and baggage screening technologies," including memorandums and

3. Logs referencing the use or maintenance of any equipment used to search, examine, or extract data from passengers' electronic devices at the San Francisco International Airport.
4. All communications between SFO and TSA referencing the replacement, supplementation, or relocation of any piece of Transportation Security Equipment ("TSE") at SFO.[7]
5. Training of transportation security officers or contractors retained to provide security screening services, related to the search or examination of passengers' electronic devices.

31. By letter dated January 4, 2018, TSA acknowledged receipt of the TSA Field Office Request, assigned it an "unperfected case number," and requested additional information about Plaintiff's request. TSA also determined that the TSA Field Office Request met the "unusual circumstances" criteria of FOIA, and stated that it would not be able to complete the processing of the request within 30 working days (20 working days plus 10 additional working days). A copy of this letter is appended hereto as Exhibit 3.

32. By letter dated January 19, 2018, Plaintiff responded to TSA's request for further information on the following items contained in the TSA Field Office Request. A copy of this letter is appended hereto as Exhibit 4.

> Item 2: This request seeks all records in the possession of the TSA San Francisco Field Office, regardless of the author of the document, related to (1) the acquisition, testing, use, maintenance, and location of equipment used to search, examine, or extract data from passengers' electronic devices and SIM cards and (2) any inventories of the number of each type of such equipment.
> Item 3: This request seeks all use or maintenance logs related to the search, examination, or extraction of data from passengers' electronic devices. Any applicable exemption from disclosure under FOIA does not alleviate the agency of its duty to search for responsive records. Rather, the proper procedure is to search for and identify the records, and then to assert an applicable FOIA exemption.
> Item 4: This request seeks all communications between SFO and TSA about TSE with a nexus to the search of, examination of, or extraction of data from passengers' electronic devices at SFO.

"information regarding the number of each technology deployed in airports nationwide." http://www.gao.gov/assets/680/674297.pdf at 28.

[7] According to a TSA 2015 report to Congress, "If TSA has identified the need to replace, supplement, or relocate a piece of TSE," TSA "informs the airport of the decision through a memo and follow-on communication as needed." https://www.fbo.gov/utils/view?id=62bf59d0ee09e6681071db6c5b15d803 at 17. This request seeks any such memos, as well as follow-up communications.

33. By letter dated January 25, 2018, TSA notified Plaintiff of a "perfected case number" for the TSA Field Office Request and stated that no additional information was needed at that time. A copy of this letter is appended hereto as Exhibit 5.

34. More than 30 working days have passed since TSA received the TSA Field Office Request.

35. More than 30 working days have passed since TSA notified Plaintiff on January 25, 2018 of a "perfected case number" and that no further information was needed from Plaintiff at that time.

36. As of the date of the filing of this Complaint, Plaintiff has not received a determination from TSA of whether TSA will comply with the TSA Field Office Request.

37. As of the date of the filing of this Complaint, Plaintiff has not received any documents from TSA that are responsive to the TSA Field Office Request or any correspondence indicating when TSA might provide any documents.

38. Plaintiff has exhausted all applicable administrative remedies.

39. TSA has wrongfully withheld the requested records from Plaintiff.

FIRST CLAIM FOR RELIEF
Violation of Freedom of Information Act For Wrongful Withholding Of Agency Records

40. Plaintiff incorporates the above paragraphs as if fully set forth herein.

41. Defendant TSA has wrongfully withheld agency records requested by Plaintiff under FOIA and has failed to comply with the statutory time for the processing of FOIA requests.

42. Plaintiff has exhausted the applicable administrative remedies with respect to TSA's wrongful withholding of the requested records.

43. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested documents because Defendant TSA continues to improperly withhold agency records in violation of FOIA. Plaintiff will suffer irreparable injury from, and have no adequate legal remedy for, TSA's illegal withholding of government documents pertaining to the subject

of Plaintiff's FOIA request.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that this Court:

A. Order Defendant TSA to promptly process and release all responsive records;

B. Declare that Defendant TSA's failure to disclose the records requested by Plaintiff is unlawful;

C. Award Plaintiff its litigation costs and reasonable attorney's fees incurred in this action;

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

Dated: March 12, 2018

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA

By: /s/ Vasudha Talla
Vasudha Talla
Linda Lye

Attorneys for Plaintiffs