ACLU
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
Northern California

March 28, 2019

DHS Office of Inspector General/MAIL STOP 0305
Attn: Office of Investigations - HOTLINE
245 Murray Lane SW
Washington, DC 20528-0305

Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
Building 410, Mail Stop #0190
Washington, D.C. 20528
CRCLCompliance@hq.dhs.gov

U.S. Customs and Border Protection
San Francisco Field Office
ATTN: Brian Humphrey, Director or Acting Director
33 New Montgomery St., 16th floor
San Francisco, CA 94105

U.S. Customs and Border Protection
San Francisco International Airport Port of Entry
ATTN: Mr. Steven Baxter, Acting Port Director; Ms. F. Garcia, Assistant Port Director
555 Battery Street
San Francisco, CA 94111

CBP INFO Center
1300 Pennsylvania Avenue N.W., MS: 1345
Washington, DC 20229

Via Email and Certified U.S. Mail, Return Receipt Requested

RE: Policies and Practices Related to the Electronic Device Search of U.S. Citizen at San Francisco International Airport

To Whom It May Concern:

We write on behalf of Dr. Andreas Gal, a U.S. citizen and technologist. This letter documents concerns about U.S. Customs and Border Protection ("CBP") policies and practices raised by CBP's attempts to search Dr. Gal's electronic devices at the San Francisco International

Airport ("SFO"), as he returned to the United States from a business trip to Sweden. Specifically, this letter documents: (1) CBP's baseless detention and intrusive interrogation of Dr. Gal and the attempted search of his devices; (2) CBP's policies allowing invasive searches of electronic devices in violation of the Fourth Amendment; (3) CBP's policies lacking protections for First Amendment rights by allowing interrogation and device searches focused on, and possibly on the basis of, a traveler's expressive activities; and (4) CBP officers' retaliation against Dr. Gal by baselessly threatening him with criminal prosecution and revoking his Global Entry status because he asserted his constitutional rights.

We ask for an investigation into whether CBP's interrogation and search of Dr. Gal was consistent with the First and Fourth Amendments of the U.S. Constitution and CBP's own policies. We also urge a comprehensive review of CBP's policies and practices to determine whether they are consistent with CBP's obligations under the U.S. Constitution and laws.

1. CBP's Detention, Interrogation, and Search of Dr. Gal at the San Francisco International Airport

Andreas Gal is a successful entrepreneur and technologist, currently employed by Apple, Inc. He is the former Chief Executive Officer of a company he founded called Silk Labs and the former Chief Technology Officer of Mozilla Corporation, which makes the popular Firefox web browser and other products. Dr. Gal has a Ph.D. in Computer Science from the University of California at Irvine. He has dedicated his career to confronting challenging technical problems, making a large impact on the world, and ensuring that both users and society are well served by his work. As an engineer and executive at Mozilla, Dr. Gal was closely involved in a number of initiatives to prevent warrantless mass surveillance and spread the use of encryption. He has an active presence on Twitter, where he has expressed his support for online privacy and his strong opposition to the current administration's policies. Dr. Gal was born in Hungary and is a U.S. citizen.

On November 29, 2018, Dr. Gal arrived at SFO, returning to the United States from a business trip to Sweden. Dr. Gal possesses Global Entry status (with Global Entry Program Membership #[redacted] . Global Entry "allows expedited clearance for pre-approved, low-risk travelers upon arrival in the United States."[1]

After immigration agents checked his passport on the jetbridge as he exited the airplane, Dr. Gal proceeded to the Global Entry kiosk in the customs and border area. There, Dr. Gal received a

[1] Global Entry, U.S. Customs and Border Protection, https://www.cbp.gov/travel/trusted-traveler-programs/global-entry.

receipt from the kiosk marked with two designations: "TTRT" and "X."[2] Dr. Gal presented that receipt, along with his U.S. passport, to an immigration officer in a glass-walled booth. The immigration officer reviewed Dr. Gal's passport and Global Entry receipt, and instructed him to go to Customs Area B, an area adjacent to the baggage claim at SFO. The immigration officer kept Dr. Gal's passport, sending him to Customs Area B without it.

At Customs Area B, Dr. Gal was interrogated by three CBP officers. Dr. Gal understood one of those officers, whose name was Bowman, to be the supervisor of the other two officers. All three officers were armed with holstered handguns. Two of the officers were dressed in tactical military fatigues and the supervisor was dressed in a blue uniform. All wore armored vests.

The CBP officers asked Dr. Gal numerous questions about his travel plans, his work at Apple, his employment history, and his electronic devices. The officers also asked Dr. Gal detailed questions about his work at Mozilla and travel to Canada, indicating an awareness and interest in Dr. Gal's public stance on online privacy—which constitutes speech that Dr. Gal has a First Amendment right to engage in. The questions Dr. Gal was asked were not limited to his identity, citizenship, or customs-related matters. Throughout the interrogation. Dr. Gal repeatedly requested that the officers explain why he was being asked questions. The officers refused to answer.

Dr. Gal was travelling with an Apple iPhone XS and an Apple MacBook Pro. Both devices were issued to him by Apple for software-development purposes. The laptop bears a sticker reading "PROPERTY OF APPLE. PROPRIETARY." The phone has a sticker with a serial number but not Apple's name; its lockscreen displays the legend "Confidential and Proprietary," and includes a number to call if the device is found. Apple development devices have specialized software, hardware, and other features that distinguish them from consumer devices. As an Apple employee, Dr. Gal is bound by non-disclosure agreements requiring him to maintain the secrecy of Apple proprietary information. In addition, he is obligated to maintain careful possession and control of his Apple-issued development devices; to avoid the dissemination of information concerning these devices or the Apple projects to which they related; and to strictly limit access to those devices by other persons. Dr. Gal takes his obligations under these agreements very seriously.

CBP officers searched Dr. Gal's wallet and all his luggage, and asked questions about everything they found. When they discovered Dr. Gal's Apple-issued electronic devices, the officers first asked Dr. Gal to pull up his itinerary on his mobile phone, and then to hand the unlocked

[2] The "TTRT" mark on Dr. Gal's Global Entry kiosk receipt may refer to the so-called "Tactical Terrorism Response Teams" deployed at United States Points of Entry and consisting of CBP Officers ostensibly trained in "counterterrorism response." *See* https://www.dhs.gov/news/2017/05/03/written-testimony-cbp-ice-plcy-house-committee-homeland-security-task-force-denying. Neither the immigration agents nor the CBP officers ever offered any justification—because none exists—for why Dr. Gal's receipt was marked with a "TTRT" designation.

device over to CBP. Dr. Gal responded that he would email them the itinerary, but that he would need to speak with a lawyer and his employer before giving CBP officers full access to his mobile phone.

CBP officers ordered Dr. Gal to turn over his passcode to his mobile phone and password to his laptop, and repeatedly threatened Dr. Gal that they would keep his devices if he did not unlock them. Dr. Gal advised the CBP officers that both his mobile phone and his laptop contained proprietary and highly confidential information about Apple technology. Dr. Gal again requested the opportunity to consult with his employer or an attorney prior to providing passwords to his devices because he had signed a non-disclosure agreement laying out strict legal obligations for those devices.

Critically, Dr. Gal never refused to provide the passcodes to access the electronic devices in his possession, he only asked that he be allowed to consult with an attorney to ensure that he would not violate non-disclosure agreements with his employer. In the interactions with CBP officers, Dr. Gal repeated many times that he would comply with any legal requirement, but that he needed to consult with an attorney to understand his rights before he could do so.

CBP officers refused to allow Dr. Gal access to an attorney or the ability to contact his employer. CBP officers told Dr. Gal that he had no right to an attorney. After Dr. Gal made clear that he would not unlock his devices without first consulting with his employer and an attorney, a CBP officer stated that Dr. Gal was legally required to supply his passwords in response to their request. The CBP agent told Dr. Gal to "look up 18 U.S.C. § 111," which states that any person who "forcibly assaults, resists, opposes, impedes, intimidates, or interferes with" a federal officer in the performance of official duties is committing a federal crime. One of the officers later wrote "18 U.S.C. 111" on a piece of paper and handed it to Dr. Gal. This threat of criminal prosecution had no basis in fact or law.

At that point, three armed CBP officers had detained Dr. Gal, interrogated him about every aspect of his travel and his possessions, and threatened him with criminal prosecution. In those interactions, Dr. Gal felt that he was not free to leave, and CBP officers retained his passport throughout the questioning. Dr. Gal informed the CBP agents that he would not be able to answer any more questions without being permitted to speak with an attorney. Dr. Gal did not answer any further questions from the CBP officers.

CBP officers eventually allowed Dr. Gal to leave with his devices but a CBP officer took Dr. Gal's Global Entry card and told him his privileges would be revoked. CBP officers informed Dr.

Gal that he would lose his Global Entry status as a result of his "refusal to comply with a search."[3] Before he was permitted to leave the airport, an officer provided Dr. Gal with a slip of paper with handwritten text reading "Port 2801," "Supervisor Bowman," and the phone number, "[redacted]"

2. CBP's Attempted Search of Dr. Gal's Devices Violated the Fourth Amendment.

CBP must ensure that its officers comply with the U.S. Constitution. Even at the border, the search of an electronic device is governed by the Fourth Amendment. To satisfy Ninth Circuit and Supreme Court law concerning electronic searches, any such search should be based on a warrant and be limited in scope to information relevant to the agency's legitimate purpose in conducting the search. The attempted unconstitutional search of Dr. Gal's devices illustrates that CBP's policies do not in fact include the requirements necessary to safeguard the constitutional rights of people at the border.

Dr. Gal returned to the United States on November 29, 2018 from a business trip, carrying a mobile phone and a laptop. Amongst Americans, the use of mobile electronic devices is pervasive. Nearly every American adult owns a cell phone of some kind.[4] With their immense capacity, modern smartphones can hold the equivalent of "millions of pages of text, thousands of pictures, or hundreds of videos." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). Moreover, the availability of cloud-based storage, email, and social-media services can vastly increase the functional capacity of a device and sensitive information accessible on it. Much information that courts have recognized as intensely private can be contained on people's mobile devices, including internet browsing history,[5] medical records,[6] historical cell-phone location data,[7] email,[8] privileged communications,[9] and

[3] Dr. Gal never refused to comply with any search, he only requested that he be permitted to consult with an attorney before handing over the passcodes to his electronic devices.
[4] Pew Research Ctr., Mobile Fact Sheet (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.
[5] *See Riley*, 134 S. Ct. at 2490 ("An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").
[6] *See Ferguson v. Charleston*, 532 U.S. 67, 78 (2001) (expectation of privacy in diagnostic test results).
[7] *See Riley*, 134 S. Ct. at 2490 ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").
[8] *See United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) ("[E]mail requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve.").
[9] *See Jaffee v. Redmond*, 518 U.S. 1, 15 (1996) (psychotherapist-patient privilege); Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) (attorney-client privilege); *Blau v. United States*, 340 U.S. 332, 333 (1951) (marital communications privilege).

associational information.[10] As a result, the search of electronic devices constitutes a significant intrusion on an individual's Fourth Amendment privacy interest, and searches of electronic devices require a warrant, even if the search was conducted incident to a lawful arrest. *See Riley*, 134 S. Ct. 2473.

This same principle applies at the border. As in other contexts, "[t]he ultimate touchstone of the Fourth Amendment is reasonableness." *See Riley v. California*, 134 S. Ct. 2473, 2482 (2014); *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985). Whether a search is reasonable and exempted from the warrant requirement is determined by balancing a person's privacy interest against the government's interests. *See Riley*, 134 S. Ct. at 2484. As noted above, the Supreme Court has held that there is an extraordinarily high privacy interest in the contents of an electronic device. *Id.* at 2489–91. CBP's interest in searching electronic devices is lower than its interest in searching luggage for contraband or dangerous items. *See U.S. v. Ramsey*, 431 U.S. 606, 616 (1977). No customs-based rationale justifies the search of sensitive private correspondence wholly unrelated to concerns about contraband, *see Ramsey,* 431 U.S. at 624, or the search of cloud-based data that cannot be said to move *across the border*. CBP's suspicionless searches of digital devices, like the one CBP attempted to conduct of Mr. Gal's devices, are unconstitutional.

Moreover, even if a search were authorized by a warrant or predicated on sufficient suspicion at its inception, it must still be reasonably limited in scope. Prior to the Supreme Court's decision in *Riley,* the Ninth Circuit Court of Appeals recognized that the scope of a digital search must be reasonable, holding that reasonable suspicion was required for a "comprehensive and intrusive" search of a laptop seized at the border because of the degree to which a thorough search infringed upon privacy interests—which interests outweighed the government's interest in such searches. *United States v. Cotterman*, 709 F.3d 952, 966–68 (9th Cir. 2013)[11]; *cf. U.S. v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1170–72 (9th Cir. 2010) (concluding government agents had failed to comply with a warrant by reviewing digital information outside its scope).

---

[10] *Riley*, 134 S. Ct. at 2490 ("Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news . . . ."); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958)
("[C]ompelled disclosure of affiliation with groups engaged in advocacy may constitute . . . a restraint on freedom of association . . . .").

[11] It is the invasiveness of a digital device search, not the manual or forensic method by which it is conducted, that is key to the analysis of reasonableness. The *Cotterman* court emphasized this, noting that the "key factor triggering the requirement of reasonable suspicion" was the "comprehensive and intrusive nature of the forensic examination." 709 F.3d at 962. *Cotterman* did not conclude that manual searches are reasonable no matter how far they invade the privacy and dignity interests of a person. In addition, because *Cotterman* predates *Riley*, the Court's assumption that a "cursory" search would be permissible even without suspicion is not the final word on the lawfulness of such searches, particularly now that cursory searches of many electronic devices can provide access to troves of content that is easily accessible through built-in search tools.

Though a directive that constitutes CBP's national policy concerning electronic searches includes some instructions for officers encountering certain sensitive information (including legal information and medical records), it contains neither a prohibition on searches lacking probable cause nor any procedures designed to limit the scope of authorized searches to that needed to further any legitimate purpose. *See* U.S. Customs and Border Protection, *Border Search of Electronic Devices*, Directive No. 3340-049A, § 5.1.2 (January 4, 2018) (hereinafter the "Directive").[12] Nor does the Directive comply with the Ninth Circuit's decision requiring reasonable suspicion for forensic searches of electronic devices seized at the border. *See Cotterman*, 709 F.3d at 968. As a result, CBP officers acting pursuant to the Directive are free to rifle through sensitive personal information contained on electronic devices with no suspicion and no limitations on the scope of their search.

The attempted search of Dr. Gal's company-issued phone and laptop is particularly concerning given the vast amount of highly proprietary information and trade secret information contained on the devices. The federal government would be required to demonstrate to a court's satisfaction that it could meet a stringent legal standard in order to force Apple to disclose the developer versions of software and hardware that were contained on Dr. Gal's devices. Yet the Directive appears to offer the federal government an end-run around those standards by permitting CBP to search, and even copy, the contents of Dr. Gal's devices without any probable cause. The Directive also fails to permit an individual like Dr. Gal, who is subject to his own legal obligations and requirements, the opportunity to consult with his employer or an attorney before providing access to the contents of his devices. These concerns are corroborated by the Office of Inspector General's recent report confirming that CBP officers who engaged in device searches did not properly document the searches and did not always delete travelers' information copied during advanced searches (the "December 2018 OIG Report").[13] Finally, even under the terms of the Directive, the CBP officers did not properly "protect [confidential] information from unauthorized disclosure" as the Directive requires. *See* Directive § 5.2.3.

Moreover, the attempted search of Dr. Gal's phone under the Directive was not an isolated incident. In recent years, government searches of electronic devices under this Directive have skyrocketed: such searches increased substantially in 2016 to nearly 19,000 devices, and DHS has estimated that 2,200 devices were searched by CBP in February 2017 alone.[14] The December 2018 OIG Report noted serious deficiencies in the documentation maintained by CBP officers regarding

[12] *Available at* https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.
[13] Dep't of Homeland Security, Office of Inspector General, CBP's Searches of Electronic Devices at Ports of Entry, OIG-19-10 to 11 (Dec. 2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-12/OIG-19-10-Nov18.pdf.
[14] Cynthia McFadden, E.D. Cauchi, William M. Arkin, and Kevin Monahan, *American Citizens: U.S. Border Officers Can Search Your Cellphone*, NBC News, Mar. 13, 2017, http://www.nbcnews.com/news/us-news/traveling-while-brown-u-s-border-officers-can-search-your-n732746.

electronic device searches, making it nearly impossible to quantify searches and identify departures from the Directive.[15] To the extent these searches are conducted without a warrant or probable cause, or are not limited in scope to the information needed to further CBP's legitimate interests, they are unconstitutional.

3. <u>CBP Policies and CBP Officers' Interrogation of Dr. Gal and Attempted Search of His Smartphone and Laptop Violated Dr. Gal's First Amendment Rights.</u>

We are also deeply concerned about the impact of CBP's interrogation and attempted device search on Dr. Gal's First Amendment rights, and the lack of protection for such rights in CBP's Directive or other policies. Dr. Gal is a politically-active technologist, and extensive information about his political commitments and technical work is available to the public. CBP's suspicionless detention, interrogation, and search of Dr. Gal appears motivated by hostility to his First Amendment-protected activities. In other words, it appears that CBP singled out Dr. Gal for questioning and search based on Dr. Gal's political viewpoints.

There was no basis for Dr. Gal to be detained and interrogated by "TTRT" officers with special training in "counterterrorism response." Dr. Gal entered the United States as a holder of Global Entry status, available only to "low-risk" individuals. And Dr. Gal has been an entrepreneur, technologist, and public figure for decades. Designating Dr. Gal for interrogation by "TTRT" indicates that Dr. Gal was targeted because of his exercise of his First Amendment rights in expressing viewpoints that may be disfavored by the federal government.

Moreover, there was no reason for any CBP officers—TTRT or otherwise—to detain and interrogate Dr. Gal or his devices. Notably, CBP officers did not confiscate and retain Dr. Gal's devices, which they were authorized to do under the Directive and presumably would have done if they truly felt that they possessed a basis for detaining Dr. Gal or keeping his devices. *See* Directive, § 5.3.3. Instead, CBP officers proceeded to demand that Dr. Gal provide immediate, unlimited access to his devices. And when he continued to request access to counsel, CBP officers issued baseless threats of criminal prosecution. Again, the lack of any plausible reason to detain and interrogate Dr. Gal suggests that he was targeted based on his First-Amendment protected expression of political viewpoints.

CBP officers also focused their interrogation on Dr. Gal's First Amendment-protected political speech and activism. The CBP officers asked detailed questions about Dr. Gal's work for Mozilla, his interaction with co-workers years ago in Canada, and whether any records (e.g., emails or other communications) from that time were still accessible on his devices. As Mozilla's Chief

[15] December 2018 OIG Report at OIG-19-10.

Technology Officer, he frequently spoke at industry conferences and was interviewed by the media. As a result, and due to his active Twitter presence, his views on privacy and surveillance, and his political leanings, were well known. Dr. Gal's statements on privacy-protective technology and his associations during that time represent First Amendment-protected activity. There was no legitimate reason for the CBP officers to ask about these subjects, because they bear no relationship to Dr. Gal's entitlement to enter the country (he is a U.S. citizen) or any customs rationale.

The attempted search of Dr. Gal's device also threatens his exercise of his First Amendment rights. At the time of CBP's search, Dr. Gal's smartphone included contact information about his family and associates, correspondence with other persons, and other information about his and their views, which can be understood as critical of government action, policies and personnel. In the closely related context of customs searches of incoming international mail, the U.S. Supreme Court recognized that First Amendment-protected speech might be chilled by such searches and notably declined to invalidate that search regime only because regulations existed "flatly prohibit[ing], under all circumstances" customs officials from reading correspondence without a search warrant. *United States v. Ramsey*, 431 U.S. 606, 623 (1977). Here, the Directive fails to place any limitations on the government's search and review of First Amendment protected-speech and associational information accessible on an electronic device during a border search, even though, in light of the quantity and quality of information at issue, the chill on First Amendment rights may be even greater than searches of papers or mail. Thus, the government's attempted search of expressive and associational information on Dr. Gal's devices without any limit as to scope violated Dr. Gal's First Amendment rights. *See Alasaad v. Nielsen*, No. 17-CV-11730-DJC, 2018 WL 2170323, at *24 (D. Mass. May 9, 2018) (holding that a device search at the border, in light of the "limitless search authorizations" in CBP policies, could violate the First Amendment).

Given the dearth of rules limiting CBP officers' discretion to inspect and read information contained on or accessible from electronic devices, travelers faced with the kind of treatment Mr. Gal encountered might justifiably choose not to use their phone to communicate about controversial issues, communicate about political or religious beliefs, or maintain a record of associations on their mobile device. In other words, the prospect that CBP officers may read information available on digital devices exerts a significant chilling effect on the exercise of First Amendment rights.

Furthermore, singling out a traveler for invasive questioning and search on the basis of his avowed political viewpoints threatens to chill the traveling public from exercising their First Amendment rights publicly as well. Those who expect to travel internationally may self-censor what they say in public, knowing that CBP officers might target those with disfavored political viewpoints for questioning and searches at the border that go beyond immigration or customs matters.

4. **CBP Officers Retaliated by Threatening Dr. Gal with Criminal Prosecution and Revoking His Global Entry Status.**

In addition, the CBP officers provided Dr. Gal with inaccurate information about the potential consequences of his decision to refuse a device search. CBP officers told him that he was committing a federal crime under 18 U.S.C. § 111. A violation of that section of the criminal code is punishable by up to eight years in prison. *Id.* There is no basis for the CBP officer's assertion that Dr. Gal was violating 18 U.S.C. § 111; the claim appears to have been solely to intimidate Dr. Gal into providing the passcodes to his devices. In response, Dr. Gal insisted, after being accused of committing a federal felony and in the context of what appeared to be a custodial interrogation, that he be permitted to speak to a lawyer.

After Dr. Gal insisted on speaking with an attorney, CBP officers allowed him to leave. But as a purely retaliatory measure, the officers kept his Global Entry card and informed him that his Global Entry status was going to be revoked. In the words of the officer, "Your Global Entry is gone. I am keeping your card." To the extent CBP revoked Dr. Gal's Global Entry status because he sought to speak to his employer or an attorney before agreeing to a device search, this would introduce an unwritten requirement to Global Entry status that appears nowhere in the regulation: that to maintain Global Entry status, a traveler must always agree to an unrestricted and immediate device search by CBP. Dr. Gal's request to consult with his employer and an attorney was entirely appropriate and reasonable under the circumstances—indeed, once he had been accused by a federal agent of violating a federal criminal law, Dr. Gal had even more right to consult with an attorney. CBP officers should not be withdrawing Global Entry status as a result of travelers insisting that their rights be respected.

***

We ask for prompt acknowledgement of this letter and an investigation into whether CBP's interrogation and search of Dr. Gal was consistent with the First and Fourth Amendments of the U.S. Constitution as well as the CBP Directive. We also urge a comprehensive review of CBP's Directive and practices to determine whether CBP is complying with its obligations under the U.S. Constitution and any agency guidelines—with particular attention to the extent to which officers at ports of entry are:

1. conducting searches of electronic devices without a warrant or probable cause;
2. failing to properly instruct travelers on the Directive's protocols, including the consequences of refusing to comply with a demand to search an electronic device;
3. threatening persons with criminal prosecution when those persons request access to counsel before determining whether to provide passcodes to unlock an electronic device,

or access to their employer before determining whether to provide passcodes to unlock an employer-owned device;
4. singling out persons for secondary screening and searches of electronic devices based on First Amendment-protected expression or associations; and
5. examining or retaining information found on electronic devices that is protected by the First Amendment; and
6. retaliating against travelers by revoking their Global Entry status or by other means.

When these investigations are complete, we ask that we be informed of the results of any investigations.

Thank you for your time and careful attention.

Sincerely,

William S. Freeman
Jacob Snow
Vasudha Talla
ACLU Foundation of Northern California