May 4, 2017

John Roth
Inspector General
Office of Inspector General/Mail Stop #0305
Department of Homeland Security
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

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 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

Dear Inspector General Roth:

We write on behalf of Aaron Gach, a U.S. citizen and artist, who recently returned to the United States from Belgium, where he had participated in an art exhibition. This letter documents concerns about U.S. Customs and Border Protection (CBP) policies and practices raised by CBP's search of a U.S. citizen's smartphone at the border. Specifically, the purpose of this correspondence is to document (1) the facts concerning the questioning of Mr. Gach and the search of his smartphone, (2) that CBP's policies allow invasive searches of electronic devices in

violation of the Fourth Amendment and federal appeals court precedent, (3) that CBP's policies lack protections for First Amendment rights by allowing questioning and device searches focused on, and possibly on the basis of, a traveler's expressive activities, and (4) that CBP officers, in at least this instance, failed to follow CBP's policies and failed to accurately communicate those policies to Mr. Gach.

1. CBP's Questioning of Mr. Gach and Search of His Smartphone at the San Francisco International Airport

Mr. Gach, an accomplished artist, is currently a professor at California College of the Arts, and was recently the Granada Artist-in-Residence at the University of California at Davis Department of Theatre and Dance. His work addresses public space, social politics, and community issues. In addition to producing national and international projects, he has taught courses in Public Art, Street Media, Art & Magic, and 4D Art at the University of California at Santa Cruz, Stanford University, and the San Francisco Art Institute.

On February 23, 2017, Mr. Gach returned to the United States from Belgium. He arrived at San Francisco International Airport (SFO). He had traveled to Belgium to participate in an art exhibition, at which he presented three different interactive art pieces designed to evoke themes including incarceration, government control, and political dissent.

After Mr. Gach presented his passport during immigration processing at SFO, a CBP officer told him to step aside for additional screening in a closed set of offices adjacent to the primary screening area. During this screening, two CBP officers extensively interrogated Mr. Gach about his travels and background. CBP officers asked Mr. Gach to prove he was an artist and asked detailed questions about his work, including where he travelled and how often he travelled to exhibitions. CBP officers also pressed Mr. Gach for information about the Belgium exhibition's curators. CBP officers asked many of their questions repeatedly.

During this questioning, CBP officers turned their focus to Mr. Gach's smartphone, an iPhone SE. The officers asked to search Mr. Gach's phone with the stated purpose of verifying his verbal answers to their questions. In response, Mr. Gach asked to see written policies authorizing the requested search. CBP officers did not immediately provide Mr. Gach with this information. In addition, CBP officers refused to identify any specific information they were searching for, when asked by Mr. Gach.

Officers told Mr. Gach his phone would be detained for an "indeterminate" amount of time if he chose not to enter the passcode and submit to a search. The officers also told Mr. Gach that CBP had downloaded information from the phones of other travelers who had refused to unlock their devices. When CBP officers asked Mr. Gach why he did not want to submit his phone for a search, Mr. Gach replied that he believes strongly in the U.S. Constitution and in his right to privacy.

CBP officers continued to demand that Mr. Gach produce his cell phone for a search. Mr. Gach repeatedly answered that he wanted to see the written justification for such a search. Eventually, officers produced a "tear sheet" for Mr. Gach while they conducted a search of his

luggage in his presence. However, the "tear sheet" merely stated that CBP is authorized to search to "determine identity and citizenship of all persons seeking entry into the United States, determine the admissibility of foreign nationals, and deter the entry of possible terrorists, terrorist weapons, controlled substances, and a wide variety of other prohibited and restricted items." At no point did the officers explain why, in their view, a search of Mr. Gach's phone would assist in determining his identity and citizenship (which CBP officers did not themselves question). Nor did they offer any explanation of how information about his work as an artist or the curators with whom he has worked had any connection to terrorists, terrorist weapons, controlled substances, or other prohibited and restricted items.

In addition, officers expressly refused to conduct a search of Mr. Gach's phone in his presence. CBP officers stated that their search would be "manual" rather than forensic but offered no further information about the scope of their proposed search.

Ultimately, Mr. Gach was forced to choose between unlocking his phone and handing it over for a search out of his line of sight or relinquishing his phone for an "indeterminate" amount of time. Mr. Gach did not consent to the search, but feeling as though he had no meaningful choice, Mr. Gach entered his passcode and handed his unlocked smartphone to the officers. Mr. Gach did not provide the officers with his passcode. The CBP officers removed his phone to an area in the room behind a dividing wall and outside of Mr. Gach's view for a period of approximately 5 to 10 minutes. After completing their examination of Mr. Gach's smartphone, officers released him with the phone, his passport, and other belongings.

2. CBP's Policies Authorize Unconstitutional Searches of Electronic Devices, Including the Search of Mr. Gach's Smartphone.

CBP, like every government agency, is obligated to 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 precedent concerning electronic searches, any such search should be based on a warrant or, at a minimum, probable cause, and be limited in scope to that information relevant to the agency's legitimate purpose in conducting the search. However, as the unconstitutional search of Mr. Gach's phone illustrates, CBP's policies do not in fact include the requirements necessary to guarantee the constitutionality of a device search.

Mr. Gach returned to the United States with, among other devices, an iPhone SE. Amongst Americans, the use of mobile, or portable, electronic devices is pervasive. Nearly every American adult owns a cell phone of some kind.[1] 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 exponentially increase the functional capacity of a device and sensitive information accessible on it. Many types of information that courts have recognized as deserving of particularly stringent privacy protections

[1] Pew Research Ctr., Mobile Fact Sheet (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.

can be contained on people's mobile devices, including internet browsing history,[2] medical records,[3] historical cell phone location data,[4] email,[5] privileged communications,[6] and associational information.[7] As a result, the Court determined that a search of an electronic device constitutes a significant intrusion on an individual's Fourth Amendment privacy interest, and held that searching an electronic device required a warrant even when the search was conducted incident to a lawful arrest.

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. On the other side of the scale, 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 conducted of Mr. Gach's phone, 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

---

[2] *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.").

[3] *See* Ferguson v. Charleston, 532 U.S. 67, 78 (2001) (expectation of privacy in diagnostic test results).

[4] *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.").

[5] *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.").

[6] *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).

[7] 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 . . . .").

Cir. 2013)[8]; *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).

Though CBP's Directive 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 Containing Information*, Directive No. 3340-049, § 5.1.2 (Aug. 20, 2009) (hereinafter "Directive No. 3340-049" or "Directive").[9] Nor does this Directive, CBP's apparent national policy on electronic searches, acknowledge 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 the wealth of sensitive personal information contained on electronic devices without any apparent suspicion of wrongdoing or any limitations to narrow the scope of their search. In fact, Mr. Gach worries about the potentially sweeping nature of the search conducted by CBP officers, and whether officers limited their search or examined a wide range of his sensitive information accessible via apps and stored in the cloud.

Moreover, the search of Mr. Gach'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.[10] 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. CBP Policies and CBP Officers' Questioning of Mr. Gach and Search of His Smartphone Raises First Amendment Concerns.

We are also deeply concerned about the impact of CBP's questioning and smartphone search on Mr. Gach's First Amendment rights, and the lack of protection for such rights in CBP's Directive or other policies.

---

[8] 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 cloud-based content stored on remote servers.

[9] *Available at* https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.

[10] 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.

First, the focus of the CBP officers' questions raises concerns about whether CBP targeted Mr. Gach for further questioning and search because of his First Amendment-protected activist art and advocacy, which would be a violation of his First Amendment rights. During their questioning, the CBP officers asked Mr. Gach what kind of art he creates. CBP officials also asked for the names, phone numbers, and email addresses of the Belgium exhibition's curators and other participants and attendees. They asked how often Mr. Gach travels for art and where he travels. The CBP officers' intensive questioning about Mr. Gach's art was inappropriate in and of itself and lends credence to the inference that his detention and subsequent search of his smartphone were improperly motivated by his constitutionally-protected expression.

Second, the search of Mr. Gach's device also implicates his First Amendment freedoms. At the time of CBP's search, Mr. Gach's smartphone included contact information about his family and associates, correspondence with other persons, and information about his artistic work which can be understood as critical of government action. 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 examination of expressive and associational information on Mr. Gach's smartphone without any limit as to scope raises serious First Amendment concerns.

Given the dearth of rules limiting CBP officers' discretion to inspect and read information contained on or accessible from electronic devices, travelers such as Mr. Gach may justifiably choose not to use their phone to communicate about controversial issues, take photos of artistic works, or maintain a list of professional contacts. In other words, the mere prospect that CBP officers may read information available on digital devices exerts a significant chilling effect on the expression of First Amendment rights.

4. <u>CBP Officers Acted Improperly in Violating CBP's Own Directive and in Providing Inaccurate Information to Mr. Gach About the Directive.</u>

Beyond the concerns stated about the lack of constitutional safeguards in the Directive, we are additionally concerned that CBP officers did not actually comply with the Directive or accurately describe it to Mr. Gach. The Directive states that "[s]earches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit the individual to remain present." Directive No. 3340-049, at § 5.1.2. Moreover, the Directive provides that individuals may be permitted to witness the search itself (above and beyond being present in the room) unless that would "reveal law enforcement techniques or potentially compromise other operational considerations." *Id.* However, despite the

lack of apparent applicability of any of these exceptions (for one, a "manual" search on its own is not a novel technique and would not reveal specialized operational details), CBP officers expressly refused Mr. Gach's request to be present for the search and conducted the search out of his view. Mr. Gach does not know the scope of what officers examined or even whether, contrary to their assertions, they connected his device to forensic equipment. As a result, officers conducting the search denied Mr. Gach even the minimal protections provided by the Directive and have heightened his concern that the search was sweeping in scope.

In addition, the CBP officers provided Mr. Gach with inaccurate information about the Directive and the potential consequences of his decision to refuse a device search. CBP officers told him that if he refused to consent to a search, his phone would be retained for an "indeterminate" period. However, the Directive establishes clear timelines and rules for the retention of electronic devices and information therein. *See* Directive No. 3340-049, at §§ 5.3.1-1.2. Subject to extensions, the Directive states devices should ordinarily be detained for no more than five days. *Id.* at § 5.3.1. The Directive also requires supervisory approval to detain a device or information from a device after a subject is released. *Id.* at § 5.3.1.1. CBP's statements were inconsistent with CBP's own policies and contributed to the coercive environment that led Mr. Gach to involuntarily unlock his device.

***

We ask for prompt acknowledgement of this letter and an investigation into whether CBP's questioning and search of Mr. Gach 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. conducting searches of electronic devices in the absence of safeguards and guidance designed to ensure such searches are targeted at information that would assist in determining admissibility or discovering contraband;
3. conducting searches of electronic devices outside of the view of the person whose device is being searched;
4. singling out persons for secondary screening and searches of electronic devices based on First Amendment-protected expression or associations;
5. examining or retaining information found on electronic devices that is protected by the First Amendment; or
6. 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.

Thank you for your time and careful attention.

Sincerely,

Matt Cagle
Technology and Civil Liberties Policy Attorney
ACLU of Northern California

Chris Conley
Technology and Civil Liberties Policy Attorney
ACLU of Northern California

Esha Bhandari
Staff Attorney
Speech, Privacy, and Technology Project
American Civil Liberties Union Foundation

Nathan Freed Wessler
Staff Attorney
Speech, Privacy, and Technology Project
American Civil Liberties Union Foundation

Hugh Handeyside
Staff Attorney
National Security Project
American Civil Liberties Union Foundation