Searches of Electronic Devices: Recent Developments and Judges' Ethical Responsibilities

By Keith R. Fisher

Judges frequently carry with them a variety of electronic devices on which confidential or privileged information might be stored. They should be aware of certain recent developments involving searches by government agents of electronic devices and understand the pertinent canons of judicial conduct.

Background

Early into the Obama Administration, the U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE)—both agencies within the Department of Homeland Security (DHS)—adopted policies[1] to search, sometimes seize, and review the content of electronic devices at U.S. border crossings. Since the inception of the program, the numbers of these searches have steadily increased from approximately 8,500 in 2015; 19,000 in 2016; and 30,000 in 2017. To put these numbers into context, however, even this dramatic increase accounts for only 0.007 percent of the 397 million travelers (including both U.S. and foreign nationals) who crossed the border during the 12-month period ending September 30, 2017.[2] Over 80 percent of devices searched reportedly belonged to foreigners or legal permanent residents.[3]

---

[1] *See, e.g.,* U.S. Customs & Border Patrol, Border Search of Electronic Devices Containing Information, Directive No. 3340-049 (Aug. 20, 2009), *available at* https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf; U.S. Immigration and Customs Enforcement, ICE Policy System, Border Searches of Electronic Devices, Directive No. 7-6.1 (Aug. 18, 2009), *available at* https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

[2] *See* Nick Miroff, *U.S. Customs Agents Are Searching More Cellphones – Including Those Belonging to Americans*, WASH. POST, Jan. 5, 2018, *available at* https://www.washingtonpost.com/world/national-security/us-customs-agents-are-searching-more-cellphones--including-those-belonging-to-americans/2018/01/05/0a236202-f247-11e7-b3bf-ab90a706e175_story.html?utm_term=.350aad80597f

[3] *See* Alicia A. Caldwell & Laura Meckler, *Border Agents' Searches of Travelers' Phones Skyrocketed, Agency Says; Customs and Border Protection Unveils New Policy for Searching and Seizing Electronic Devices,* WALL. ST. J., Jan. 5, 2018, *available at* https://www.wsj.com/articles/border-agents-searches-of-travelers-phones-skyrocketed-agency-says-1515179058.

Also noteworthy are some 2017 reports that the Transportation Security Administration (TSA) is implementing heightened screening procedures with respect to electronic devices for purely *domestic* flights.[4]

On the one hand, these searches and seizures are carried out without a warrant or any individualized suspicion—much less probable cause—that a traveler has done anything wrong. On the other hand, these searches have been instituted to vindicate national security concerns. Thence arises the delicate constitutional question of balancing that governmental interest against individual rights. Some federal court decisions have permitted routine border searches of travelers' computers and other electronic devices as an exception to the Fourth Amendment prohibition against warrantless searches without probable cause.[5] Nevertheless, as the Ninth Circuit concluded, en banc, an intrusive forensic search of a computer hard drive is not "routine" and therefore requires reasonable suspicion to be constitutionally permissible. [6]

Electronic devices belonging to lawyers and judges raise additional concerns—namely, the confidentiality of information contained in documents stored electronically, including information that is protected by one or more recognized evidentiary privileges. This article will summarize some recent developments and then consider a judge's obligations under the canons of judicial conduct.

Recent Revisions to CBP Policy

On January 4, 2018, CBP issued a revised policy[7] governing border searches of electronic devices. As it affects issues of privilege, the new policy provides:

- When examining data on a device, CBP officers are now required by section 5.1.2 of the new policy to avoid accessing data stored remotely (*e.g.*, in the Cloud) when they conduct device searches. To accomplish this, that section provides that the officers will either request that the traveler disable connectivity to any network (*e.g.*, by placing the device in airplane mode), orthey will themselves disable network connectivity where warranted by national security, law enforcement, officer safety, or other operational considerations.
- If a device is encrypted, section 5.3.1 of the revised policy requires travelers to unlock or decrypt their electronic devices and/or provide their device passwords to border agents.
- CBP officers must now consult with the CBP Associate/Assistant Chief Counsel's Office before searching devices allegedly containing privileged or work product protected information.[8]
- CBP officers and lawyers are now required to seek clarification from the individual assertingthe privilege as to the specific files, attorney or client names, or other particulars that may assist the agency in identifying the privileged information, and requires CBP to segregate the privileged materials from the other materials on the device and ensure the privileged materials arehandled

---

4 *See, e.g.*, Russ Thomas, *TSA implements new screening procedures in Montana*, KPAX.com, Dec. 14, 2017, *available at* http://bit.ly/2sMepaI; Joel Hruska, *TSA Will Now Screen All Electronics "Larger Than a Cell Phone,"* EXTREME TECH, July 26, 2017, *available at* http://bit.ly/2sG2Fq4.

5 *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 960–61 (9th Cir. 2013) (en banc); Abidor v. Napolitano, 990 F. Supp. 2d 260, 277–82 (E.D.N.Y. 2013).

6 *Cotterman*, 709 F.3d at 960–68.

7 U.S. Customs & Border Patrol, Border Search of Electronic Devices, Directive No. 3340-049A (Jan. 4, 2018), *available at* https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/cbp-directive-3340-049a-border-search-electronic-media.pdf (superseding Directive No. 3340-049).

8 Section 5.2.1 of the prior policy required such consultation only when (A) the devices contained materials that appeared to be "legal in nature" or that were claimed to be protected by the privilege or work product *and* (B) the border officer suspected that the material "may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP."

appropriately, all through the use of a filter team consisting of legal and operational representatives of the agency.

- Any privileged materials that are copied by CBP must be destroyed at the end of the review process, unless the materials indicate an imminent threat to homeland security, or copies of the materials are needed to comply with a litigation hold or other requirement of law.
- The new policy distinguishes a "basic search" of an electronic device, which may be conducted with or without suspicion, from an "advanced search" (defined as one in which an officer connects the device to external equipment to review, copy, and/or analyze its contents), which may only be conducted if there is reasonable suspicion of unlawful activity or a national security concern.[9]
- Note that CBP's revised policy (section 2.7) expressly does not apply to searches by ICE, even when CBP transfers devices to ICE for a search.

As of this writing, ICE has not revised its own policy, so its prior policy remains in force. ICE's policy authorizes searches of electronic devices with or without individualized suspicion. Unlike CBP's revised policy, however, ICE's does not contain enhanced protection or consultation procedures for information claimed to be privileged or confidential and does not prohibit Cloud searches.

Pertinent Ethical Obligations

Judges should consider whether consenting to a device search by a CBP or ICE agent is compatible with their professional responsibilities. Obviously, the first step is for a judge facing such a search to advise the border agent of the existence of any privileged material on the device in question.

Part-time judges are also bound by the Code of Judicial Conduct.[10] To the extent that they are also practicing lawyers, however, they should be aware of pertinent obligations under applicable rules of professional conduct as well.[11] (Though full-time judges are usually members of the bar, they may not practice law (MCJC Rule 3.10), so the latter set of rules are largely inapplicable to them).

Model Code of Judicial Conduct

Compliance with Law. Rule 1.1 requires judges to comply with the "law." The purpose of the provision is central to the MCJC – avoiding the appearance of impropriety and to avoid diminishing public confidence in the judiciary. Assuming, *arguendo*, that border searches of personal electronic devices are authorized by existing federal statutes,[12] there can be no civil disobedience by a judge of CBP and ICE policies.

---

9 Although not explicit in the new policy, this particular requirement may be a reaction to federal court decisions such as *Cotterman*, holding that an intrusive "forensic search" of a computer hard drive is not "routine" and requires reasonable suspicion to be constitutionally permissible.

10 References in this article will be to the ABA Model Code of Judicial Conduct ("MCJC"). Judges should consult the version adopted in their respective states.

11 For guidance on compliance with applicable rules of professional conduct, which include those governing competence, communicating with clients, confidentiality, and supervisory responsibilities, *see* a companion piece, Keith R. Fisher, *U.S. Border Searches of Electronic Devices: Recent Developments and Lawyers' Ethical Responsibilities*, BUS. L. TODAY (March 2018), *available at* https://businesslawtoday.org/2018/03/u-s-border-searches-of-electronic-devices-recent-developments-and-lawyers-ethical-responsibilities/.

12 Interestingly, the MCJC defines "law" somewhat broadly to include statutes, though not broadly enough expressly to include regulations or agency policy statements.

Avoiding Abuse of the Prestige of Judicial Office. Rule 1.3 prohibits judges from using or attempting to use the prestige of judicial office to gain personal advantage of deferential treatment of any kind. Thus a judge should avoid any conduct that might be, or be construed as, an attempt to use the cachet of judicial authority to intimidate or cajole a border official wishing to search any of the judge's electronic devices.[13]

Nonpublic Information. Perhaps the most pertinent provision of the MCJC is Rule 3.5, though its language creates some ambiguity. Like its predecessor, Canon 3(B)12, the rule prohibits *intentional* disclosure of use of "nonpublic information acquired in a judicial capacity for any purpose unrelated to the judge's judicial duties." "Nonpublic information" is a term of art specific to this Rule; initially it is defined, somewhat circularly, as "information unavailable to the public," but the definition goes on to provide a non-exclusive list of examples: "information that is sealed by statute or court order or impounded or communicated in camera, and information offered in grand jury proceedings, presentencing reports, dependency cases, or psychiatric reports." As electronic filing becomes more ubiquitous, judges are increasingly likely to have these sorts of pleadings or documents on their portable electronic devices.

One might well ask whether a border search of an electronic device qualifies as an "intentional" disclosure of nonpublic information acquired in a judicial capacity. That is certainly an open interpretive question. Given the breadth accorded the concept of "intent" in tort law and criminal law, however, it would be dicey in a disciplinary proceeding to hang one's hat on such an argument, especially where the expected retort would be that the judge knew or reasonably should have known that his or her electronic devices would potentially be subject to search when traveling abroad and that such a search would unduly risk the proscribed disclosure.

Some Concluding Observations

The following are worthy considerations for any judge anticipating cross-border travel:

- Consider whether it is necessary to bring with you any electronic device containing confidential or privileged information. (If you're going on vacation, the foolproof solution is to enjoy yourself and leave the device behind!)
- If you absolutely must bring one or more portable electronic devices along, make sure each one is thoroughly scrubbed of all privileged or confidential information. Note that merely deleting files may not be adequate to remove them completely. Alternatively, you could consider acquiring an electronic device exclusively for use during foreign travel and avoid, to the maximum extent possible, placing confidential or privileged information thereon.
- Merely encrypting privileged or confidential information on a device is no guarantee of its remaining confidential. Remember that border agents may demand that you

[13] *Cf.* In re Muller, No. 069351, Presentment (N.J. Sup. Ct. Adv. Comm. Judl. Cond. 2011), *available at* https://www.judiciary.state.nj.us/attorneys/assets/acjc/MullerPresentment.pdf, Final Order, (N.J. 2011), *available at* https://www.judiciary.state.nj.us/attorneys/assets/acjc/MullerOrder.pdf (reprimanding judge who made 9-1-1- call in connection with service of subpoena on her husband in unrelated matter for repeatedly identifying her judicial position when rebuking responding officers), available ; In re Heiple, 97-CC-1 (Ill. Cts. Comm'n 1997) (censuring state Chief Justice for avoiding speeding tickets by producing judicial identification credential rather than driver's license when stopped by police on several occasions and saying "Don't you know who I am?"), available at https://www2.illinois.gov/sites/jib/Documents/Orders%20from%20Courts%20Commission/Heiple.pdf.

provide password or other decrypting information, and failure to do so can lead to your device being seized and detained for a period of time.

- Finally, be cognizant of the location and content of all privileged and confidential information on each device you bring across the border, and be prepared when advising a federal officer of the existence of privileged or confidential information to identify for the officer specific files or categories of files, and any other information that will help the officer segregate such information.