Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 17, NUMBER 3 >>> MARCH 2017

United States

Can Border Agents Search Your Phone?



By Miriam Wugmeister, J. Alexander Lawrence and Rhiannon Batchelder

There have been numerous reports from individuals entering the U.S. of border agents searching their phones and laptop computers. Many of those individuals are U.S. citizens. Although these events have been in the news recently and appear to be on the rise, this practice is not new. According to CNN, quoting a U.S. customs agency spokesman, border agents searched 4,444 cellphones and 320 other electronic devices in 2015. In 2016, searches of electronic devices at the U.S. borders rose to 23,877, according to the same source. In countries such as China and Russia, border agents have been searching phones and laptops for years, and many companies have developed policies to provide guidance to employees traveling to those countries. Companies are now struggling with how to advise and craft policies for employees traveling to and from the U.S. with electronic devices that may contain sensitive data.

Miriam Wugmeister, a partner at Morrison & Foerster LLP's New York City office, is a member of the firm's Global Privacy and Data Security practice.

J. Alexander Lawrence is a partner at Morrison & Foerster in New York and co-chair of its E-Discovery Task Force.

Rhiannon Batchelder is a litigation associate at Morrison Foerster in New York.

Border Searches: The Constitutional Framework

Courts have held that, under U.S. law, Customs and Border Patrol (CBP) and Immigration and Customs Enforcement (ICE) agents may ask to search electronic devices at the border and may request individuals to disclose their password so they can conduct the search. These courts have held that a border agent may conduct a manual search of any electronic device without a warrant and without reasonable suspicion. *United States v. Cotterman*, 709 F.3d 952, 963 (9th Cir. 2013). A more intrusive, forensic examination of electronic devices requires that the boarder agent have reasonable suspicion of criminal activity. *Id.* at 968. "Reasonable suspicion" means "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *Id.* (quoting *United States v. Cortez*, 449 U.S. 411, 417-18 (1981)). In the absence of reasonable suspicion, a border agent may still ask for the password and scroll through the contents of the device.

Border agents do not have unfettered authority in this area. For instance, a federal district court recently suppressed evidence found during a search of a laptop at the border after border agents made an exact copy of the laptop's hard drive and searched it with forensic programs. *United States v. Kim*, 103 F. Supp. 3d 32, 52 (D.D.C. 2015). The court held that there had not been reasonable suspicion that the defendant was engaged in ongoing or imminent criminal activity at the time of the border search. Therefore, the search was illegal under the Fourth Amendment. *Id.* at 59.

The precise limits on the authority of border agents in this area remain an open question; the Supreme Court has not yet weighed in on this issue.

When traveling internationally, consider taking only a clean smartphone or laptop computer.

The Department of Homeland Security Guidelines

In a Privacy Impact Assessment for border searches of electronic devices, the Department of Homeland Security addressed procedures for when a device may contain privileged material. U.S. Department of Homeland Security, *Privacy Impact Assessment for the Border Searches of Electronic Devices*, Aug., 2009, at 11, 13.

With respect to searches conducted by CBP, the Assessment states:

> [w]here an electronic device is to be detained or seized by CBP, a CBP Supervisor must approve of the detention or seizure, and the CBP Officer must provide a completed CF 6051D or S, respectively, to the traveler. Where a traveler claims that the contents of the electronic device contain attorney-client or other privileged material, the CBP Officer must consult with the local Associate/Assistant Chief Counsel or U.S. Attorney's Office before conducting the examination. *Id.* at 11.

With respect to searches conducted by ICE, the Assessment states:

> a traveler's claim of privilege or statement to an ICE Special Agent that something is personal or business-related does not preclude the search. ICE policy and certain laws, such as the Privacy Act and the Trade Secrets Act, requires the special handling of some types of sensitive information including attorney-client privileged information, proprietary business information, and medical information. Special Agents violating these laws and policies are subject to administrative discipline and criminal prosecution. Further, when a Special Agent suspects that the content of electronic devices includes attorney-client privileged material that may be relevant to the laws enforced by ICE, ICE policy requires the Special Agents to contact the local ICE Chief Counsel's office or the local U.S. Attorney's Office before continuing a search. *Id.* at 13.

Therefore, to avail themselves of these DHS protections, individuals should notify border agents of the potential privileged or business-sensitive nature of the data on their electronic devices.

Practical Tips: Protecting Sensitive Data at the Border

There are many things you can do to protect sensitive information at the border, below are a few:

- When traveling internationally, consider taking only a clean smartphone or laptop computer. If there is no sensitive data on the electronic device, there is no risk that such data will be exposed to border officials.

o If all sensitive data cannot be wiped from electronic device prior to international travel, only take the information needed and remove all unnecessary sensitive data.

o Inventory all sensitive data contained on any electronic devices that will be taken across the border. That way, if it is accessed, you will know exactly what information was impacted.

- Fully power down all electronic devices prior to passing through customs. Encryption software is most effective when devices are powered down.

- If a request for a search is made, inform CBP or ICE officials if there is privileged or business sensitive data on your devices.

  WDPR ISSN 1473-3579