Employee Relations
LAW JOURNAL

When Cell Phones Cross Borders: Protecting Employees' Sensitive Data from Suspicionless Cell Phone Searches at International Airports

Jayce Born, Andrew Tutt, R. Stanton Jones, Stephen K. Wirth, Sam Callahan, and Graham W. White

The authors explain that employers must understand that, at any international airport or other border crossing, border agents can seize and search their employees' cell phones without a warrant.

The ubiquity and sophistication of smartphones has created a more mobile work force ("mobile" – get it?). Employees can Zoom with their colleagues during a pandemic, they can take a call re-routed from their office phone while in transit to a client meeting, and, even if they might not want to, they can reply to emails while on vacation abroad. In fact, many employers now provide smart phones to employees for company business, or have adopted bring-your-own-device policies so that employees can integrate work email or other applications onto their personal devices.

There are certainly benefits to an increasingly connected and cross-border work force (a topic for another time and another article), but the next time an employee travels abroad for work or for pleasure, you may want to keep one major drawback in mind: today, at any international airport or other border crossing, border agents can seize and search travelers' cell phones without a warrant.

The authors, attorneys with Arnold & Porter Kaye Scholer LLP, may be contacted at *jayce.born@arnoldporter.com*, *andrew.tutt@arnoldporter.com*, *stanton.jones@arnoldporter.com*, *stephen.wirth@arnoldporter.com*, *sam.callahan@arnoldporter.com*, and *graham.white@arnoldporter.com*, respectively. George Anibowei, the plaintiff in the lawsuit pending before the U.S. Court of Appeals for the Fifth Circuit that is discussed in this article, is represented by Arnold & Porter and the Texas Civil Rights Project.

CBP POLICY

Current U.S. Customs and Border Protection ("CBP") policy permits its officers to conduct what CBP calls "basic" searches of cell phones for any reason or no reason at all.[1] And a basic search is by no means basic.

Under CBP's current policy, officers can ask travelers to unlock their phones and present them for inspection, and officers can then access and review all content and communications contained within the device. If a traveler refuses to provide the password, CBP can detain the device for an undetermined amount of time (the detention should not "ordinarily" exceed five days). And in practicality, refusing to provide the passcode likely will lead to a prolonged detention of the traveler, as well.

What is more, CBP's policy also authorizes agents to conduct "advanced" or "forensic" searches when officers have reasonable suspicion of illegal activity or a "national security concern." In an advanced search, an officer connects external equipment to the phone to review, copy, and analyze its contents. How long CBP may keep the data copied from the phone, and who they can share it with, depends on an elaborate data-retention policy that considers both the passage of time and the content of the data. Neither a basic or advanced search, nor the continued retention of any data collected during an advanced search, requires officers to obtain a warrant.

FIFTH CIRCUIT CASE

While the policy is concerning on its face, its practical effects are even more so, as demonstrated by *Anibowei v. Morgan*,[2] a case currently pending before the U.S. Court of Appeals for the Fifth Circuit.

George Anibowei is a Dallas, Texas, attorney who represents clients adverse to the U.S. government in legal proceedings. About four years ago, on October 10, 2016, border agents at the Dallas-Fort Worth airport seized Mr. Anibowei's cell phone as he returned home from a trip to Canada. Acting without a warrant, the agents searched the cell phone and copied the data on it. Since then, border agents have searched Mr. Anibowei's cell phone four more times, each time without a warrant. These searches not only exposed every intimate detail of Mr. Anibowei's private life, they also exposed attorney-client privileged information to government agents.

To justify these warrantless searches, CBP invokes the border-search exception to the Fourth Amendment's warrant requirement. This exception permits border agents to warrantlessly search physical containers to prevent contraband from crossing the border and to assist in the collection of customs duties.

But, as Mr. Anibowei argues in his appeal, neither the U.S. Supreme Court nor the Fifth Circuit has ever extended the border search exception to searches of the data on cell phones. And for good reason. Smartphones are so different from other effects routinely carried on one's person that, as the Supreme Court held in *Riley v. California*,[3] courts cannot reflexively "extend" traditional warrant exceptions to them. Cell phone searches are dragnet searches of a person's entire life – they can lay bare every private communication, every photo, and (due to GPS tracking data) every place a person has recently been, in a single search. For Mr. Anibowei, they also laid bare his client's confidential and privileged information. And for many others carrying a smartphone with access to their work email, they can lay bare sensitive, confidential, or proprietary business information.

Mr. Anibowei filed his suit nearly three and a half years ago, and his case is just now on appeal.

If Mr. Anibowei succeeds in enjoining CBP's policy, then future international travelers will not have to spend years challenging warrantless searches that exposed, and in some cases retained, their most private personal and professional information.

If he does not, employers will need to evaluate how they want employees to handle business data when traveling internationally.

CONCLUSION

If having access to work data on a smartphone is necessary while traveling, employers should, at a minimum, ensure all devices utilize strong encryption methods and that employees power down their devices before reaching the airport. For employees with routine access to particularly sensitive and confidential data, employers should consider what data those employees need to access during travel. Border agents cannot access data that does not exist, so consider having employees delete non-essential data before traveling.

Employees can also upload data to the cloud before traveling, and then re-download it at their destination: CBP's policy only allows border agents to access content on the device, not remote data like that in the cloud (but it is worth noting that Immigration and Customs Enforcement has a similar policy to CBP's but with no similar remote-access limitation). You may also want employees to clear, log out of, and/or delete their cloud applications and browsers, as agents may be able to see cached content – content stored from the last time the application or browser was accessed.

If employees are simply traveling internationally for pleasure, on the other hand, employers may want to bring meaning back to the automatic "out-of-office" reply by requiring employees to leave their work phones at home or remove work applications from their personal devices before hitting the road for vacation: no more checking work email from the beach.

NOTES

1. *https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf*.

2. *Anibowei v. Morgan*, No. 20-10059 (5th Cir.).

3. *Riley v. California*, 573 U.S. 373, 386 (2014).