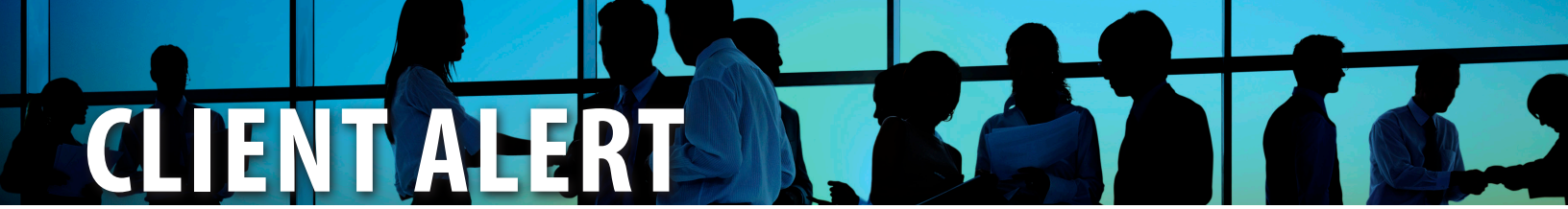

DATA PRIVACY AND CYBERSECURITY

IF YOU DON'T NEED IT, DON'T PACK IT: BORDER SEARCHES OF MOBILE DEVICES

by Sara H. Jodka

Currently there are a number of pending cases concerning the issue of whether Border searches can include a search of someone's cellphone. On March 15, 2018, a divided 11th Circuit Court, upheld the conviction of a Florida man wherein a warrantless Border search of his cellphone uncovered child pornography. In upholding the conviction, the court held that such searches, which do not require a warrant or even any probable cause, do not violate the Fourth Amendment's prohibition against illegal searches and seizures.

We are including this as a client alert because this is *relevant for any person traveling* across the United States Border. And while the case at issue concerned images of minors in compromising positions, the availability of such searches is an issue for anyone traveling with a mobile device that contains confidential, proprietary or trade secret information; intellectual property; financial/banking information; patient-client privileged information or information subject to HIPAA/HITECH; information protected by the attorney-client or work product privilege, etc.

In The United States of America v. Hernando Javier Vergara, Case No. 8:16-cr-00021-JDW-MAP-1 (11th Cir. Mar. 15, 2018), Hernando Javier Vergara, was returning home to Tampa, Florida following a cruise to Mexico. He was subjected to a search of his luggage by a U.S. Customs and Border Protection officer. The luggage search included a search of Vergara's cell phones. He had three in his possession, and he was asked to turn one of the phone on and provide access. The officer located a video of two topless female minors. Vergara was then summoned by the Department of Homeland Security to provide all three phone for forensic analysis. That analysis revealed more than 100 images and videos that were deemed child pornography.

Vergara was indicted by a grand jury for "knowingly transport[ing] in and affecting interstate and foreign commerce one or more visual depictions, the production of which involved the use of a minor engaging in sexually explicit conduct and such visual depictions were of such conduct"; and, that he "knowingly possess[ed] numerous matters that had been shipped and transported using any means and facility of interstate and foreign commerce, including by computer, which matters contained visual depictions of minors engaging in sexually explicit conduct and the production of which involved."

Vergara tried to suppress the evidence obtained from the phone searches because it was obtained without a warrant, but his efforts failed and the evidence was admitted. This helped lead to his conviction and sentencing to ninety-six months in prison and, upon release, lifetime supervision.

On appeal, the 11th Circuit, upheld the conviction finding that the search-incident-to-arrest exception to the warrant requirement did not apply to Border searches of cell phones. Instead, the court found that, since the cell phones occurred at the Border, not as searches incident to arrest, neither a warrant nor probable cause was required because, at most, border searches require reasonable suspicion, which was a point Vergara did not argue.

The court included a reminder from the United States Supreme Court's Riley v. California, Case No. 13-132 (2013) decision wherein the Court held that: "The Supreme Court has consistently held that border searches are not subject to the probable cause and warrant requirements of the Fourth Amendment."

This is just one of many similar cases. In September 2017, eleven people sued the Department of Homeland Security after their phones and laptops were search at United States airports at the northern border. The group alleged that their First and Fourth Amendment rights were violated when United States agents searched, and in some cases confiscated, their devices without a warrant.

In June of 2017, the acting commissioner for Customs and Border Protection, wrote a letter to lawmakers informing them that agents are not permitted to look at data stored solely in the "cloud." With that, it seems agents would be limited to data stored directly on the device, including photos, text messages, call histories and contacts, but it appears less clear whether they are permitted to search cloud-based apps installing on a device, which would include social media accounts and email.

On January 4, 2018, U.S. Customer and Border Protection (CBP) issued a Directive (CBP Directive No. 3340-04K A) titled "Border Search of Electronic Devices" that provides that border searches of electronic devices are limited to "only the information that is resident upon the device," and officers are prohibited from intentionally using the device to access information that is solely stored remotely. To avoid access to information stored remotely, officers will either request that the traveler disable network connectivity or, where warranted by national security, law enforcement, officer safety, or other operational considerations, the officers themselves will disable network connectivity. Thus, there is a "basic" search, which may be conducted without suspicion, and an "advanced" search, which requires officers to have reasonable suspicion of activity in violation of the laws CBP enforces or administers.

Interesting for certain professionals with confidentiality obligations, when an individual asserts the attorney–client privilege or the attorney work product doctrine, the officer is supposed to seek clarification—in writing, if practicable—from the individual asserting privilege to assist CBP in identifying the privileged information. This type of detail, however, does not appear to apply to other types of confidential information, such as trade secrets, business information, or medical records.

Takeaways

We have not heard the end of this debate. This issue is likely to be one that goes up to the Supreme Court and, even when it does, it is unclear

whether the issue of whether reasonable suspicious is required since it was not a point argued in *Vergara*. The Ninth Circuit Court of Appeals agreed with the government's position that "reasonable suspicion is not needed for customs officials to search a laptop or other electronic device at the international border". United States v. Arnold, 2008 WL 1776525 at *4 (9th Cir. 2008)).

Here are some best practices:

1. Those traveling abroad should be extremely careful and cognizant of *all* information they travel with, including what is accessible via a laptop or device.

2. The same logic that applies to physical packing for traveling should apply to packing electronically-accessible information. Don't over pack. If you don't need it, don't pack it. This goes as far as, if you don't need the device, do not take it at all.

3. Understand the contents on your device, how they are stored, and how they are accessed.

4. For information you may want to access later, transfer it to the cloud, ensure strong password protection, and disable the connection.

5. Carry a burner phone that allows you to make calls and ensure you have relevant numbers programed into the phone.

6. If you have programs or applications open that access the cloud, which includes social networks, log-out and close them, and put the device in airplane mode.

7. Delete all programs, applications, and delete all data and information you do not need.

8. Transfer photos and videos to a cloud account and remove them from the device.

9. If you get selected, you can either cooperate to allow the search to go easily or you can be prepared to sit and wait. If you choose the latter, be prepared to have your device confiscated and returned to you at a later time, if at all.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of data privacy and cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.