



Can They Search Your iPad or iPhone at the Border?

By Christopher B. Hopkins

Are you considering a trip to Europe this summer? Or perhaps a weekend in the Bahamas or an international business trip? Certainly you will bring your smartphone, tablet, or laptop to stay connected, if not entertained. Depending on the length and nature of your trip, you will likely access emails, documents, personal accounts, or even your office server. Imagine, upon your return, that the border agent wants to access your electronic devices. Let's pose a short quiz:

Can border patrol search your devices, apps, and files when you return to the U.S.? Can the government go further and perform a forensic examination, peering into deleted spaces and password protected files?

- (a) No, I have Fourth Amendment protection and the government cannot search me without a warrant;
- (b) Somewhat, the government can do a cursory review but cannot undertake forensic searches of my devices without a warrant;
- (c) Yes, the government can perform a cursory review and, upon reasonable suspicion, undertake a forensic examination of my devices;
- (d) Yes, the government has a broad exception to the Fourth Amendment at the border and can undertake a full search of my devices.

The answer rests somewhere between answers (c) - (d). Travelers arriving in the U.S. should prepare their electronic devices for cursory as well as potential forensic examination.

If that answer comes as a surprise to you as a lawyer, imagine the surprise of Howard Cotterman, who returned from a routine family vacation to Mexico and had his cameras and laptops opened at the border. No incriminating evidence was initially found although there were password protected files on one laptop.

However, Mr. Cotterman had a fifteen year old conviction which triggered a "hit" on the border patrol's system. It was reported that he had been convicted of child pornography and a concern was raised that his frequent trips to Mexico might be evidence of child sex tourism (for what it is worth, while he was a registered sex offender, the specific conviction was incorrectly reported to border patrol). The government performed a several-day long forensic scan of the laptop and overcame the password protection, ultimately finding illegal child pornography in the deleted and protected spaces. There were no indications that the illegal content had anything to do with his trip to Mexico.

Mr. Cotterman, individually, deserves little sympathy since the evidence lead a jury to convict him of abusive, criminal behavior upon a minor over a period of years. That said, in the context of Fourth Amendment privacy, it is often the (accused or actual) reprobates of society who set the stage for legal challenges which establish how far into our privacy the government may intrude (*see also* bit.ly/USvJonescase). To that extent, and for a clear understanding of the searchability of your digital content during international travel, this case is important.

Generally speaking, the Fourth Amendment protects us from unreasonable searches of our person and "papers" – digital or otherwise – and, inside United States, the government will generally need to obtain a warrant. There is, however, an exception for "border searches" since the sovereign has a profound interest to prevent entry of unwanted persons and effects. "Border searches" are generally deemed reasonable simply by virtue of the fact that they occur at the border.

According to *U.S. v. Cotterman* (9th Cir. March 30, 2011) ("*Cotterman I*"), however, the panel held that searches of electronic devices were different and should be reviewed on an *ad hoc* basis applying a reasonableness standard. In other words, *Cotterman I* held that not all border searches were inherently reasonable.

Within a year, that opinion was vacated and the Ninth Circuit *en banc* released *Cotterman II* on March 8, 2013. The majority held that a cursory examination of devices was always permitted and that the forensic search of Mr. Cotterman's laptop was reasonable under the circumstances; the forensic search required a heightened standard since electronic devices, which retain content even after erasure, carries with them a "significant expectation of privacy."

The concurring judges, meanwhile, agreed with the result (no Fourth Amendment violation) but held that the "majority ignores the reality [of a "border search"] by erecting a new rule requiring reasonable suspicion for extended searches of electronic devices." The concurrence found that electronic devices were not entitled to special consideration and, instead, concluded that border searches were *per se* reasonable.

The dissent, meanwhile, blasted the majority for eroding the long-standing precedent of liberal border searches and outrightly begged for intervention, writing, "... I sincerely hope the Supreme Court will grant certiorari and reverse the holding in this case... for the sake of our national security."

Some recommendations for international travelers:

- (1) prepare to be searched upon arriving in a foreign country;
- (2) *Cotterman* says little about whether the government may access your files and accounts on the internet via apps or browsers which pre-fill your account information -- including cloud or other remote storage;
- (3) if you have convictions or your name appears on travel restriction lists, you may be more likely selected for greater search;
- (4) copied movies and music may be an issue; and
- (5) be wary of office / shared devices, since you have no control over what might lurk in deleted spaces or unaccessed parts of the machine.

Christopher B. Hopkins is a shareholder with Akerman Senterfitt. An email to christopher.hopkins@akerman.com with your comments will not invade his dignity or privacy.

CLE Content Now Available 24/7

Click on the Bar's CLE webpage

<http://www.palmbeachbar.org/continuing.php>
to view list of seminars available either on CD's
or for immediate download to your MP3 device.