Crossing Borders in the Digital Age

By Douglas Whitney

Although it may seem counter-intuitive, the digital revolution has made international travel substantially more perilous for clients and lawyers alike. Thanks to cell phones, we now travel with more private and confidential information than could have been imagined even a decade ago. As the Supreme Court recently observed, "it is no exaggeration to say that many of the more than 90 percent of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[1] And for lawyers and clients, cell phones and laptops also often contain vast amounts of confidential data and communications protected by the attorney-client privilege.

In *Riley v. California*, 134 S. Ct. 2473 (2014), the Court confronted this new technological reality in which today's smart phone is "now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy" and issued a game-changing opinion in terms of its Fourth Amendment jurisprudence.[2] In *Riley*, Chief Justice Roberts, writing for eight members of the Court, concluded that the smart phone required a fundamental re-examination of longstanding Fourth Amendment doctrines (in that case, the search incident to arrest exception) because "[w]ith all they contain and all they may reveal, [smart phones] hold for many Americans 'the privacies of life,'" which are not "any less worthy of protection" simply because technology "allows an individual to carry such information in his hand."[3]

It remains to be seen, however, what exactly *Riley* means for travelers crossing U.S. borders carrying electronic devices. Pursuant to a somewhat antiquated jurisprudence known as the "border exception" to the Fourth Amendment, which was originally developed to allow the government to protect the "territorial integrity" of the United States by searching incoming individuals and parcels for contraband, the U.S. Customs and Border Patrol (CBP) now routinely searches tens of thousands of these electronic devices each year without a warrant or probable cause.[4] CBP conducts these warrantless searches pursuant to its "plenary authority" to conduct searches and inspections of "persons and merchandise crossing our nation's borders."[5] In other words, by exiting or entering this country, every traveler is effectively agreeing to allow CBP to rummage freely through every piece of private and confidential information contained on any electronic device they are carrying, even if CBP does not have any reasonable suspicion (or any suspicion at all) that the device contains contraband or relates to any illegal activity.

In this digital age, in which information contained on our electronic devices is at once so revealing and fully accessible without regard to location or national borders, is this really the right answer? And, if so (or in the meantime), what do lawyers need to do to discharge their ethical obligations to maintain client confidences and privilege? Courts, privacy advocates, and lawyers are all grappling with these pressing questions.

Until March of this year, no United States Court of Appeals had been asked to reconcile the "border exception" with the Supreme Court's recent decision in *Riley*. In *United States v. Vergara*, the Eleventh Circuit was presented with the apparent conflict between the two. Unfortunately, its reconciliation efforts were less than inspiring. In a relatively cursory opinion, the two-judge majority simply stated that "[b]order searches have long been excepted from warrant and probable cause requirements, and the holding of *Riley* does not change this rule."[6] But in a lengthy and compelling dissent, Judge Jill Pryor argued that technological advances and the Court's decision in *Riley* required reevaluation of the border search exception because "cell phones are fundamentally different from any object traditionally subject to government search at the border."[7] Accordingly, Judge Pryor would have held that, absent other potentially applicable warrant exceptions such as exigent circumstances, a warrant and probable cause should be required to search an electronic device at the border.

Surely the Eleventh Circuit's decision in *Vergara* will not be the last word on this issue. There are a number of other Fourth Amendment challenges pending before district courts, and the ACLU and the Electronic Frontier Foundation also filed a lawsuit in September challenging the CBP's authority to conduct warrantless and suspicionless searches of electronic devices.[8] It is likely that the issue will be taken up by other courts of appeals soon, and eventually by the Supreme Court in the next several terms as it continues to grapple with the ramifications of the digital age in various Fourth Amendment contexts.

In the meantime, in January, CBP issued revised (but still quite disconcerting) guidelines for searches of electronic devices along the border. The new CBP guidelines restrict agents' ability to conduct "advanced searches" on electronic devices – i.e., those that require use of an external device. Now, such searches may not be conducted unless CBP has reasonable suspicion of unlawful conduct or a national security concern.[9] But CBP remains free to conduct "basic" or non-advanced searches for any or no reason at all. The current guidelines also direct searching officers "encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine" to coordinate with CBP counsel and employ a "Filter Team composed of legal and operational representatives" to examine such data, but it is not clear how and when this provision may be enforced.[10]

While this revised guidance does provide clarity regarding CBP's procedures, it falls far short of adequately protecting the privacy of incoming and outgoing travelers. For, as Chief Justice Roberts observed in *Riley*, transparency may be nice, but "the Founders did not fight a revolution to gain the right to government agency protocols."[11]

As it now stands, CBP maintains virtually unfettered discretion to search electronic devices, which is particularly concerning for lawyers, who have an ethical duty to protect their client's confidential and privileged information. In a formal opinion issued in 2017, the Association of the Bar of the City of New York took this issue on, concluding that the "reasonable steps" a lawyer must take to preserve client confidences depend on the nature of the confidences, the potential harm to the client, the attorney's need to have access to the information while traveling, and the efforts taken by the attorney to protect the information before and during any encounter with CBP. While suggesting that lawyers consider removing confidential and privileged information from the devices they are traveling with, or travel only with burner devices that contain no such information, the opinion stopped short of concluding that such steps need be employed in every case.[12]

But, in this digital age, is it really possible – or should it be necessary – to travel without access to confidential and privileged information on electronic devices? Hopefully, courts will soon rein in the authority of CBP in this regard. In the meantime, however, clients and lawyers must be cognizant of the possibility that their electronic devices can be freely rummaged through by CBP any time they cross the border. •

Douglas E. Whitney is the principal at Douglas Whitney Law Offices LLC, where he represents individuals and companies in government investigations and civil and criminal litigation. He previously served as Deputy General Counsel and Chief Litigation Counsel at a Fortune 500 company, a partner in the white collar group at McDermott Will & Emery, and a federal public defender. He can be reached at Doug.Whitney@dwlollc.com.

Endnotes:

[1]*Riley v. California*, 134 S. Ct. 2473, 2490 (2014).

[2]*Riley*, 134 S. Ct. at 2484.

[3]*Id.* at 2494-95 (quoting *Boyd v. United States*, 116 U. S. 616, 630 (1886)).

[4]While it is true that, on a percentage basis, searches of electronic device searches remain very rare, CBP searched 60% more electronic devices in 2017 than in 2016, and it is certainly reasonable to expect this trend to continue. See CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (January 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

[5]CBP DIRECTIVE NO. 3340-049A (Jan. 4, 2018), at 5.1.4 (https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf).

[6]2018 U.S. App. Lexis 6413 (11th Cir. Mar. 18, 2018).

[7]*Id.* at *14.

[8]*Alasaad v. Nielsen*, 17-cv-11730-DJC (D. Mass.).

[9]CBP DIRECTIVE NO. 3340-049A, at 5.1.4.

[10]*Id.* at 5.2.1.2.

[11]*Riley*, 134 S. Ct. at 2494-95

[12]Association of the City Bar of New York Committee on Professional Ethics Formal Opinion 2017-5, http://s3.amazonaws.com/documents.nycbar.org/files/2017-5_Border_Search_Opinion_PROETHICS_7.24.17.pdf.