AN A.S. PRATT PUBLICATION
APRIL 2020
VOL. 6 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 | NUMBER 3 | APRIL 2020

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [6] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [67] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2020–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Can Border Agents Search Your Phone? An Update

By J. Alexander Lawrence and Sara Stearns*

The authors of this article explain the current state of the law on border searches of electronic devices.

A federal court in Massachusetts recently issued a ruling that may curtail the expanding practice of government agents searching electronic devices at the U.S. border. In recent years, instances of Customs and Border Patrol ("CBP") and Immigration and Customs Enforcement ("ICE") agents searching international travelers' electronic devices as they enter the United States have been on the rise. While the actual figures are likely higher, the number of electronic device searches at the border has reportedly risen from 5,100 in 2012 to over 40,000 in 2019.

BORDER SEARCHES: THE CURRENT STATE OF THE LAW

The Fourth Amendment generally requires law enforcement officers to obtain a warrant based on probable cause before conducting a search or seizure. But there are several exceptions to the warrant requirement, including the border search exception, which allows border agents to conduct routine examinations and seizures of persons and property crossing into the country in order prevent the entry of unauthorized persons or contraband.[1]

Courts in the U.S. Courts of Appeals for the Fourth and Ninth Circuits have held (and both CBP and ICE policies currently require) that border agents must have reasonable suspicion before conducting a forensic search of an electronic device.[2] Reasonable suspicion requires "a particularized and objective basis for suspecting the particular person stopped of criminal activity"[3] and is a lower standard than probable cause. The CBP and ICE policies refer to a forensic search as an "advanced search," and define it as "any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to the device, but to review, copy and/or analyze its contents."

---

* J. Alexander Lawrence is a partner at Morrison & Foerster LLP advising clients on all aspects of complex commercial litigation in federal and state trial and appellate courts and in arbitration. Sara Stearns is a litigation associate at the firm. Resident in the firm's Tokyo office, the authors may be contacted at alawrence@mofo.com and sstearns@mofo.com, respectively.

[1] *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

[2] *See United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018); *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013).

[3] *United States v. Cortez*, 449 U.S. 411, 417-418 (1981).

Nonetheless, under the current policies, when CBP and ICE agents conduct a non-forensic search of an electronic device (referred to in the policies as a "basic search"), no reasonable suspicion or other justification is required. The government agencies take the position that even without cause the border search exception permits these basic searches. While perhaps not as extensive as an advanced search, a basic search is still quite invasive, as agents can view any information on the device, including emails, texts, social media posts, and photos.

ALASAAD v. NIELSEN

In May 2018, a group of U.S. citizens and a lawful permanent resident sued the Department of Homeland Security, CBP, and ICE to challenge the constitutionality of the border search policies. Each plaintiff had been subjected at least once to a "basic search" of his or her electronic device where the officer did not have reasonable suspicion for the search. In the course of these basic searches, border agents obtained an array of sensitive information, including privileged attorney-client communications, information related to a plaintiff's journalism work, a plaintiff's work product as a NASA employee, social media posts, and photos of a plaintiff and her daughters without their religiously required attire (which, when viewed by male border agents, violated her religious beliefs).

The plaintiffs argued that the searches violated the Fourth Amendment. The court agreed. The court found that because electronic devices like cell phones and laptops contain such a breadth of sensitive personal information, even a basic search of an electronic device resulted in a significant invasion of privacy. After balancing the government's interest in border protection against individual privacy interests, the court decided that giving the government unfettered access to the contents of electronic devices was not justifiable under the border search exception. The court held that border agents must have reasonable suspicion before conducting any non-cursory search of an electronic device.[4]

Moreover, the court went out of its way to specify that for a search to be justified under the border search exception, "the reasonable suspicion that is required for the currently defined basic search and advanced search is a showing of specific and articulable facts, considered with reasonable inferences drawn from those facts, that the electronic devices contain contraband."[5] The contraband element significantly narrows border agents' authority to search electronic devices and may help prevent fishing expeditions.

---

[4] Memorandum and Order, *Alasaad v. Nielsen*, No. 1:17-cv-11730-DJC (D. Mass Nov. 12, 2019). A cursory search, which falls within the border search exception and does not require a heightened showing of cause, includes "a brief look reserved to determining whether a device is owned by the person carrying it across the border, confirming that it is operational and that it contains data." *Id.* at 30.

[5] *Id.* at 35.

IMPLICATIONS AND TRENDS

The government has appealed the case, and how the court of appeals will rule on the Fourth Amendment issue remains to be seen. Additionally, because the court declined to enter a nationwide injunction at this stage in the litigation, the current limits on border agents' search authority are unclear.

Nevertheless, the decision in *Alasaad* reflects a growing trend toward recognizing electronic device searches as fundamentally different from searches of other belongings and toward limiting the government's authority to search electronic devices. In the opinion, the court relied heavily on the U.S. Supreme Court's decision in *Riley v. California*, which held that searching the contents of an arrestee's cell phone did not fall within the warrant exception for searches incident to arrest.[6] The opinion is also consistent with the Supreme Court's recent decision in *Carpenter v. United States*, which held that the government generally must obtain a warrant to access cell phone location information and noted that "[w]hen confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."[7]

While the decision may ultimately usher in new CBP and ICE policies affording greater protections at the U.S. border, the risk of having your device searched at another country's borders will remain.

There are many things you can do to protect sensitive information when crossing an international 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.
- 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.
- 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.

[6] 573 U.S. 373 (2014).
[7] 138 S. Ct. 2206, 2221-2222 (2018).