New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 249—NO. 004
MONDAY, JANUARY 7, 2013

WHITE-COLLAR CRIME

Expert Analysis

Privacy and Technology: Balancing Competing Interests

By **Elkan Abramowitz**

And **Barry A. Bohrer**

The law regarding the Fourth Amendment's application to digital evidence continues to evolve as each branch of government tries to keep pace with society's increased reliance on technology. Americans increasingly use laptops and tablets, email, and cell phones to transact both personal and professional business while on-the-go, and the information stored on these devices more frequently is sought in the investigation of crimes. In the face of rapid advancements in technology, legislators and the courts work to frame the limits of government access while balancing competing societal privacy expectations. This article looks at circumstances under which the government can obtain digital information.

Emails

In most cases, the government does not need a warrant based on probable cause to look at an individual's emails. Case law from the 1970s establishes that a person has no expectation of privacy and, therefore, no Fourth Amendment protection of information shared with a third party.[1] With many emails, webmail providers such as Google, Yahoo, or Microsoft may function as this third party, arguably eviscerating any legitimate privacy concerns. It is unclear, however, how the decades-old third-party doctrine of the Fourth Amendment applies to modern technologies.

In 1986, Congress passed the Electronic Communications Privacy Act in an effort to moderate government surveillance of wired and electronic communications. The law prohibits third parties that provide electronic communication services, such as cell phone service or data storage providers, from voluntarily disclosing customer communications or records.[2] However, the statute permits the government to subpoena the contents of such communications if they are more than 180 days old, without prior notice to the customer. Communications that are not 180 days old can be obtained through the issuance of a warrant based on probable cause.[3]

As recently recognized by Senator Patrick Leahy (D-Vt), "[t]hree decades after the enactment of the ECPA, Americans face even greater threats to their digital privacy, as we witness the explosion of new technologies and the expansion of the Government's surveillance powers."[4] On Nov. 29, 2012, the U.S. Senate Judiciary Committee responded to this concern in an Executive Business Meeting during which it considered legislation to update the ECPA. Proposed amendments to the statute would expand vthe protection it provides by extending the warrant requirement to apply to all contents of wire or electronic communications sought by the government regardless of age. In addition, the amendments would require the government to provide notice and a copy of the warrant to a subscriber or customer whose communications have been obtained at least three days after receipt of the information from an electronic services provider.[5]

Legislators and the courts work to frame the limits of government access while balancing competing societal privacy expectations.

Although the legislation has received bipartisan support and was approved out of the committee, its ultimate fate

ELKAN ABRAMOWITZ *is a member of Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer. He is a former chief of the criminal division in the U.S. Attorney's Office for the Southern District of New York.* BARRY A. BOHRER *is also a member of Morvillo Abramowitz and was formerly chief appellate attorney and chief of the major crimes unit in the Southern District U.S. Attorney's Office.* GRETCHAN R. OHLIG, *an attorney, assisted in the preparation of this article.*

lies in the hands of Congress where it may face some resistance. Senator Chuck Grassley (R-Iowa), the Senate Judiciary Committee's ranking minority member, expressed concern that the law does not adequately balance privacy with public safety and that the extended warrant requirement may inhibit certain government investigations.[6] Many others, however, believe updates to the ECPA are long overdue. "[The amendment]…requires government investigators to do for online communications what they already do in the offline world: Get a warrant before reading postal letters or searching our homes."[7]

Cell Phones

In response to a recent congressional inquiry, cell phone service providers reported that last year they responded to approximately 1.3 million demands for customer information such as caller location and text messages.[8] The variety of data provided by these companies poses continuing issues regarding the proper balance of law enforcement and privacy interests. As noted by one scholar, neither the ECPA nor the Constitution "take into account what the modern cellphone has—your location[] [and] the content of communications that are easily readable, including Facebook posts, chats, [and] texts."[9]

Tracking Records. Cell phone towers and the Global Positioning System features of many cell phones serve as trackers and can inform authorities as to the location of a phone and, sometimes, its owner. Although the Supreme Court has held that the installation of a GPS tracking device on a suspect's vehicle by police constituted a search under the Fourth Amendment,[10] the law is less clear with respect to tracking data from cell phones.

Unlike situations in which the government seeks the contents of a communication, like that contained in emails, in these cases the government seeks only "a record or other information pertaining to a subscriber to or customer of" an electronic communications provider. Section 2703(d) of the ECPA provides that the government can obtain a court order for the release of such information upon a showing of "specific and articulable facts showing that there are reasonable grounds to believe that [the records sought] are relevant and material to an ongoing criminal investigation."[11]

The U.S. Court of Appeals for the Third Circuit is the only federal appeals court to consider the legality of cell phone tracking under this provision.[12] In its 2010 decision, the court noted that although Section 2703(d) permits the release of such information upon a showing of reasonable relevance, another provision of the ECPA, Section 2703(c)(1)(A), also gives a magistrate judge "the option to require a warrant showing probable cause." Accordingly, the court found that a magistrate judge properly can refuse cell phone tracking requests based on the lesser standard after providing "fact findings and…a full explanation that balances the [g]overnment's need (not merely desire) for the information with the privacy interests of cell phone users."

Since this decision, several magistrate judges have rejected applications for cell phone tracking under the ECPA on the grounds that intermittent cell phone tracking is unconstitutional.[13] Legislation requiring the police to obtain a warrant before demanding location records from cell phone providers has been circulated in Congress and some individual states, but no such law has been ratified.

Text Messages. The rules that apply to emails under the ECPA also apply to text messages—the government needs only a subpoena to obtain those messages more than 180 days old from cell phone service providers, but a warrant is required for more recent texts. The ECPA plays no part, however, in cases where the government seizes a cell phone pursuant to arrest or encounters a cell phone during a warrantless search of a crime scene.

Although the Supreme Court has held that the installation of a GPS tracking device on a suspect's vehicle by police constituted a search under the Fourth Amendment, the law is less clear with respect to tracking data from cell phones.

State courts are split over whether a warrant is required to review the contents of a cell phone in these instances and the Supreme Court declined to rule on the issue when it had the opportunity.[14] Many courts have found a cell phone to be a "container" subject to search after arrest, while others believe it is more akin to a face-to-face conversation, characterizing text messages as "raw, unvarnished and immediate, revealing the most intimate thoughts and emotions."[15]

Border Searches

As the authors previously have noted,[16] another area in which the Fourth Amendment and technology intersect is international travel. The government's increased focus on border security has resulted in heightened searches of all travelers who leave and enter the United States, including business travelers who frequently carry a variety of electronic devices containing extensive personal and business information. Typically, the government would have to obtain a subpoena or warrant in order to examine these items. These rules do not apply at international borders, however.

Pursuant to U.S. Customs and Border Protection (CBP) policy, issued in August 2009, a customs officer is permitted to search, analyze and review information contained in electronic devices "with or without individualized suspicion." The search is to be conducted in the presence of the traveler unless specific law enforcement or security considerations make it inappropriate.[17] Further, because the search may require more time than allowed while the traveler waits at the

border, customs officials are permitted to "detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search." In these instances, the traveler is given a receipt detailing the items kept.[18] The policy also states that the search is to be completed "as expeditiously as possible," which is ordinarily within five days.[19]

A number of court cases have examined border agents' power to search such devices. Typically, the issue is litigated within the context of a child pornography prosecution. Two recent cases have put the government on the defensive, however. In these cases, plaintiffs have sued the government civilly, arguing that they were detained and searched at the border because of their politics in violation of not only the Fourth Amendment, but also the First Amendment right to speech.

In the Eastern District of New York, Pascal Abidor, a U.S. citizen studying Islamic studies at McGill University in Montreal, Canada, who was detained when entering the country and had his laptop searched and seized, has sued to challenge the CBP policies, along with the National Association of Criminal Defense Lawyers and the National Press Photographers Association. Plaintiffs state, "With each passing day, Americans conduct most of their lives electronically, storing their most intimate details on their personal electronic devices, which have become extensions of people's minds and receptacles for their thoughts and memories. This case challenges the government's claimed authority to search Americans' most private details without any reasonable suspicion of wrongdoing."

The government has moved to dismiss the action, arguing that the plaintiffs lack standing and that, in any event, the challenged policies do not violate the Constitution. Specifically, the government notes that plaintiffs cannot demonstrate that they are in danger of sustaining an injury as a result of the policies in light of the fact that border searches of electronic devices are "extremely rare." It cites statistics to support this argument, asserting that although approximately 590 million people crossed the border into the United States between Oct. 1, 2008, and June 2, 2010, only 6,500 people were subject to searches of their electronic devices.[20] Plaintiffs respond that "[t]his statistic does not undercut the reasonableness of plaintiffs' fear of suspicionless searches in the future. Plaintiffs allege that the…policies authorize *suspicionless* searches, not that electronic device searches are *random*."[21]

Earlier in 2012, a U.S. District Court in the District of Massachusetts considered a similar case in *House v. Napolitano*.[22] In that case, David House, who was associated with an organization that raised funds to support Bradley Manning, the military analyst accused of leaking military and diplomatic documents through WikiLeaks, alleged that federal agents' search of his electronic devices at the border and the 49-day seizure of the same without reasonable suspicion violated his Fourth and First Amendment rights.

District Court Judge Denise Casper rejected the government's motion to dismiss, finding that House had asserted a plausible Fourth Amendment claim with respect to the duration of the seizure of House's laptop and a USB device, stating that "even if the initial seizure of a laptop and other electronic devices at the border requires no reasonable suspicion…[t]he duration of the seizure must be 'reasonably related in scope to the circumstances which justified it initially.'" The court similarly declined to dismiss House's First Amendment claims. The case is now in the midst of fact discovery that is scheduled to end in March 2013. The outcomes in both *Abidor* and *House* are highly anticipated.

Conclusion

The resolution of issues related to the Fourth Amendment's application to digital evidence is complicated by the constantly evolving nature of technology and the devices used by Americans to store personal and business information. The few examples cited in this article demonstrate that legislative and judicial lawmakers are unlikely to find a one-size-fits-all solution.

•••••••••••●●•••••••••••

1. See, e.g., *Smith v. Maryland*, 442 U.S. 735 (1979) (no reasonable expectation of privacy of pin register numbers provided to third-party phone company); *United States v. Miller,* 425 U.S. 435 (1976) (a depositor has no reasonable expectation of privacy with respect to checks and deposit slips sent to and circulated within third-party financial institutions).

2. 18 U.S.C. §2702.

3. 18 U.S.C. §2703(a)-(b).

4. Testimony of Senator Patrick Leahy before the U.S. Committee on the Judiciary, Executive Business Meeting (Nov. 29, 2012) (available at: http://www.judiciary.senate.gov/hearings/testimony.cfm?id=a4bac863917e3bf68f986f7431839d3c&wit_id=a4bac863917e3bf68f986f7431839d3c-0-1).

5. H.R.2471, Title II—Electronic Communications Privacy, Section 203 (available at: http://www.gpo.gov/fdsys/pkg/BILLS-112hr2471rs/pdf/BILLS-112hr2471rs.pdf).

6. Grassley proposed a counter-amendment offering an exemption in child kidnapping cases, which was rejected by the committee. A number of committee members noted that criminal and antiterrorism laws related to search warrants already include exceptions for emergencies where time is of the essence. Webcase of Executive Business Meeting located at: http://www.judiciary.senate.gov/hearings/hearing.cfm?id=a4bac863917e3bf68f986f7431839d3c).

7. Statement of Gregory T. Nojeim, Director of Center for Democracy & Technology's Project on Freedom, Security and Technology (Nov. 29, 2012) (available at www.cdt.org).

8. Eric Lichtblau, "Wireless Firms are Flooded by Requests to Aid Surveillance," *The New York Times* (July 8, 2012).

9. Somini Sengupta, "Courts Divided Over Searches of Cellphones," *The New York Times* (Nov. 25, 2012).

10. *United States v. Jones*, 132 S. Ct. 945 (2012)

11. 18 U.S.C. §2703(d). The government can seek more limited customer information, such as name, address, telephone number, length of service, and means of payment by subpoena. Id. §2703(c)(2).

12. *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010).

13. Jeremy H. Rothstein, "Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest," 81 Fordham Law Review 489, 505-506 (Oct. 2012).

14. *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010) (ruling on narrow issue of reasonableness of search and declining to rule on application of Fourth Amendment to pagers and text messages).

15. Sengupta, "Courts Divided Over Searches of Cellphones." See also, Decision, *Rhode Island v. Patino*, P1-10-1155A (Superior Court, Sept. 4, 2012) (police officer had no right to read messages on "beeping" cell phone on kitchen counter without a search warrant after responding to the home on a 911 call about an unconscious child) (available at: http://dl.dropbox.com/u/96984918/State%20v%20%20Patino-%20FINAL.pdf); *State v. Roden*, 169 Wash. App. 59 (2012) (privacy laws not violated where cops used suspected drug dealer's cell phone to respond to text messages from and locate and arrest a customer).

16. Elkan Abramowitz and Barry A. Bohrer, "Expansion of Border Searches to Laptops, Electronic Items," *New York Law Journal* (May 6, 2008).

17. U.S. Customs and Border Protection Directive no. 3340-049 ¶¶5.1.2, 5.1.4 (Aug. 20, 2009) (available at: http://www.cbp.gov/linkhandler/cgov/travel/admissibility/elec_mbsa.ctt/elec_mbsa.pdf).

18. Id. at ¶ 5.3.1.

19. Id.

20. Defendants' Memorandum of Law in Support of Motion to Dismiss, *Abidor v. Napolitano*, No. 10CV4059, at p. 16 (Jan. 28, 2011).

21. Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss, *Abidor v. Napolitano*, No. 10CV4059, at p. 16 (March 9, 2011) (emphasis in original).

22. 2012 WL 1038816 (D.Mass. March 28, 2012).