Recent Developments in Cybersurveillance

David W. Opderbeck

New Jersey Law Journal, May 16, 2016

Over the past few months, there has been a flurry of sometimes contradictory activity concerning the government's ability to access electronic information in the course of a criminal investigation. This article highlights three recent proposals that show how the broader policy debate is playing out at the level of specific legal rules.

Changes to the Federal Rules of Criminal Procedure Concerning Search Warrants

On April 28, the Supreme Court adopted changes to F. R. Crim. Pro. 41, adding a subsection (6), to authorize a magistrate judge in any district "where activities related to a crime may have occurred" to issue a warrant "to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district." Under the amendment, such warrants can issue if "the district where the media or information is located has been concealed through technological means" or in cases involving investigations of hacking or malware transmission under the Computer Fraud and Abuse Act where the "media" are damaged computers in five or more districts.

Historically, warrants were only available for search and seizure within the district where the warrant was issued. In 1990, F. R. Crim. Pro. 41 was amended to permit a warrant for search and seizure of a person or property located outside the district "if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Fed. R. Crim. P. 41(b)(1)-(2). This principle was expanded by the PATRIOT Act in 2002 to include authority to issue a warrant for a person or property outside the district if the investigation involved domestic or international terrorism, and was further amended in 2006 to include warrants for installation of a tracking device to track the movement of person inside or outside the district. SeeFed. R. Crim. P. 41(b)(1)-(4). Finally, in 2006 the rule was amended to clarify that a warrant could be issued for property outside the district but within a U.S. territory, possession or commonwealth, on the premises of a U.S. diplomatic or consular mission in a foreign state, or in a residence leased by the U.S. and used by U.S. personnel assigned to a U.S. diplomatic or consular mission in a foreign state. Fed. R. Crim. P. 41(5).

Critics of the recent addition of subsection (6), including some tech industry giants such as Google, argued that "remote access" warrants will provide authority for nationwide or even worldwide electronic surveillance. Google's comments in this regard were typical of tech industry concerns:

The proposed change does not define what a "remote search" is or under what circumstances and conditions a remote search can be undertaken; it merely assumes such searches, whatever they may be, are constitutional and otherwise legal. It carries with it the specter of government hacking without any Congressional debate or democratic policy-making process. http://googlepublicpolicy.blogspot.com/2015/02/a-small-rule-change-that-could-give-us.html

Notwithstanding such objections, the rule change was approved by the Supreme Court, and will become effective unless disavowed by Congress before Dec. 1, under the Rules Enabling Act. See 28 U.S.C. §2074.

Burr-Feinstein Bill

On April 13, Senators Richard Burr (R-N.C.) and Diane Feinstein (D-Calif.), Chair and Vice-Chair, respectively, of the Senate Intelligence Committee, released a draft bill titled the "Compliance With Court Orders Act of 2016." This bill responds to the recent showdowns between Apple and the FBI concerning the ability to compel technology companies under the All Writs Act to assist with access to locked and encrypted devices such as iPhones. See David W. Opderbeck, "The Apple iPhone Showdown: What Is at Stake," N.J.L.J., March 7, 2016.

The bill would require any covered entities that receive court orders "for information or data" to provide the information or data "in an intelligible format" and to "provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order." Discussion Draft, Sec. 3(a)(1). The bill states that a covered entity is only responsible for providing data in an intelligible format "if such data has been made unintelligible by a feature, product, or service owned, controlled, created, or provided, by the covered entity or a by a third party on behalf of the covered entity." Id., Sec. 3(a)(2). The bill further states that it would not authorize any government officer to require or prohibit "any specific design or operating system to be adopted." Id., Sec. 3(b). However, the very next subsection of the bill requires providers of "remote computing service" or "electronic communication service" to ensure that their products or services are capable of complying with

the requirement to provide data in an intelligible format. Id., Sec. 3(d), (e). The terms "remote computing service" and "electronic communication services" are defined to have the meanings provided in the Electronic Communication Privacy Act (ECPA), 18 U.S.C. s 2510, 2711.

The draft bill was immediately pilloried by technology-industry and civil-liberties advocates. For example, Kevin Bankston, director of the New America Foundation's Open Technology Institute, called it "easily the most ludicrous, dangerous, technically illiterate proposal I've ever seen." Andy Greenberg, "The Senate's Draft Encryption Bill is Ludicrous, Dangerous, Technically Illiterate," Wired Security, April 8, 2016. Critics noted that the bill's performance standard necessarily would constrain design choices, that it would effectively outlaw user-directed end-to-end encryption, and that it would require a greater level of technological assistance than the government ever sought in the All Writs Act cases. See"The Burr-Feinstein Proposal is Simply Anti-Security," Electronic Frontier Foundation Deeplinks Blog, April 8, 2016.

Proposed Amendments to ECPA

The changes to F. R. Crim. P. 41 and the Burr-Feinstein Bill are pro-law-enforcement and anti-encryption. Not all recent legislative proposals, however, fall on that side of the line. On April 27, the "Email Privacy Act" passed the House of Representatives. See H.R. 699, 114th Cong. 2d Sess. (2015-2016). The Email Privacy Act would amend the ECPA to require the government to obtain a search warrant to access stored electronic communications.

Current law makes a distinction between electronic communications in transit and in storage. For communications in transit, the Wiretap Act requires a showing of probable cause plus a showing that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. s 2518(3). Wiretap orders must expire after 30 days, although extensions are possible upon a showing of necessity. Id. s. 2518(5). For communications in storage, presently, the ECPA distinguishes between contents stored by an "electronic communication service (ECS)" and a "remote computing service (RCS)," and as to an ECS, further distinguishes whether the communications have been in storage for 180 days or more. See18 U.S.C. 2703. Finally, the ECPA allows a judge in *any* district, not only the district where the information is stored, to issue the order. Id. s. 2703(d).

Under the current ECPA, the contents of stored electronic communications (such as emails and voicemails) that have been in storage by an ECS for 180 days or less can be obtained only through a warrant. 18 U.S.C. s 2703(a). However, the government may obtain the contents of information held by an RCS "solely for the purpose of providing storage or computer processing services," or held in storage by an ECS for 180 days or more, through a court order based on "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. s. 2703(a)-(d). In other words, the law currently recognizes a lower expectation of privacy: (a) for the contents of communications held in storage by an RCS; and (b) for the contents of emails and other communications held in storage for more than 180 days by an ECS. These distinctions date back to the early days of the Internet, when users were able to download and store only a small amount of data from email servers run by their service providers. See H. Rept. 114-528 - 114th Congress (2015-2016) April 26, 2016, As Reported by the Judiciary Committee.

The Email Privacy Act would instead recognize the same expectation of privacy in all communications stored by third-party providers by requiring a warrant on probable cause before the government could obtain the contents of such communications, regardless of how long they have been in storage, and regardless of whether the provider is classified as an RCS or ECS. See Email Privacy Act, Sec. 3. This would make the statute consistent with practice in the Sixth Circuit, which has held the distinctions under the present ECPA unconstitutional under the Fourth Amendment. See *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The bill would not affect the government's ability to obtain noncontent information, such as subscriber records, through an administrative subpoena, nor would it change the ability of the owner of a communication system, such as an employer-owned email system, to disclose stored information voluntarily.

Conclusion

These three recent proposals get "into the weeds" of the larger national policy debate about encryption and Internet surveillance. They demonstrate that the larger debate implicates a host of more granular authorities involving the scope and requirements of judicially approved process for the government to obtain electronic information and for technology companies to assist with such a process. The critics may be right to worry about the jurisdictional and technological breadth of the changes to the search warrant rule and in the Burr-Feinstein Bill. However, even

if these rules are not adopted and the pro-privacy changes of the Email Privacy Act are enacted into law, significant issues will remain concerning how law enforcement can execute its mission to provide security for everyone while respecting Constitutional privacy concerns in the Internet age. The history of both Federal Rule of Criminal Procedure 41 and the ECPA show that the law in this area is constantly changing in response to new challenges and threats.