BUSINESS CRIMES BULLETIN

JULY 2018

Balancing Fourth Amendment Expectations in the Electronic Era

By Jonathan S. Feld, Dante Stella and Christina Brunty

As rapid technological changes in the 21st century continue to expand the types and volume of private electronic information, the Fourth Amendment's privacy protections are evolving. Originally, "Fourth Amendment jurisprudence was tied to common-law trespass" and provided protections against searches of property. *See*, *United States v. Jones*, 565 U.S. 400, 405 (2012). For the past 50 years, however, modern Fourth Amendment jurisprudence has focused on protecting "people, not places." The critical question in Fourth Amendment cases is whether a person has a "reasonable expectation of privacy in the information or event." *Katz v. United States*, 389 U.S. 347, 360 (1967).

Carpenter v. United States and *United States v. Microsoft*, illustrate the difficulty of applying the Fourth Amendment's "expectation of privacy" standard to digital records. Both cases arose from the Stored Communications Act, 18 U.S.C. 2701, *et seq.* (SCA) , which established statutory procedures for the government to obtain customer data from electronic data providers. The *Microsoft* case involved a challenge to a request for email data that Microsoft stored outside of the United States and was resolved by the newly-enacted Clarifying Lawful Overseas Use of Data Act (CLOUD) Act in March 2018. The *Carpenter* case, which concerned subpoenaed electronic cell records, was decided on June 22, 2018 by the Supreme Court. *See*, *Carpenter v. United States*, No. 16-402.

The Stored Communications Act

Enacted over 30 years ago, the SCA protects the privacy of communications held by *service providers*. It provides the government three avenues for obtaining disclosure of customer communications or records from electronic communication service providers and remote computing service providers: 1) administrative subpoenas; 2) Section 2703(d) orders; and 3)

Section 2703 warrants. *Carpenter* involves the use of a Section 2703(d) order, while *Microsoft* concerned a Section 2703 warrant.

To obtain a Section 2703(d) order, the government must show "reasonable grounds to believe that" the records are "relevant and material to an ongoing criminal investigation." 18 U.S.C. §2703 (d). It allows the government to obtain basic subscriber information, the contents of records stored by an electronic communication service for more than 180 days, and the contents of records stored by a remote computing service, as well as "other information pertaining to a subscriber." 18 U.S.C. §2703(a), (b)(1)(B)(i)-(ii), (c)(1). However, the government must provide prior notice to the subscriber or seek to delay notice by up to 90 days. 18 U.S.C. §2703(b)(1)(B). In contrast, under a Section 2703 warrant, which requires a higher probable cause showing, the government can obtain the same records *plus* the contents of records stored for 180 days or less, 18 U.S.C. §2703(a), without the provider's having to provide prior notice to a subscriber, 18 U.S.C. §2703(b)(1)(A).

Carpenter: Does the Fourth Amendment Apply?

In *Carpenter v. United States*, the Court addressed what expectations of privacy, if any, individuals have in cell tower location records under the Fourth Amendment. The government, to aid an armed robbery investigation, obtained a Section 2703(d) order, using the lower standard of "reasonable grounds," for Carpenter's cell-site location information that confirmed Carpenter's presence in the vicinity of the robberies. When challenged, the Court of Appeals for the Sixth Circuit held the government did not violate the Fourth Amendment because Carpenter "lack[ed] any property interest in the cell-site records created and maintained by [the cell provider]" and voluntarily conveyed the information to the cell provider. *United States v. Carpenter*, 819 F.3d 880, 888 (6th Cir. 2016).

In a 119 page, 5-4 opinion, with four separate dissents, the court recognized that the "digital data — personal location information maintained by a third party — does not fit neatly under existing precedents." Slip Op., *Carpenter*, 16-402, at 7. The Court ruled that the petitioner did have an expectation of privacy in personal location data contained in the cell-site location information (CSLI). Therefore, the government's taking of this information was a "search" subject to Fourth Amendment protections. *Id.* at 17. The Third Party Doctrine, as the Court explained, did not apply due to the "unique nature of cell phone location records." *Id.* at 11.

Is the Third-Party Doctrine Controlling?

One of the most significant issues in *Carpenter* was whether the CSLI was "voluntarily shared." Under the Third-Party Doctrine, if individuals voluntarily provide information to third parties, they relinquish their legitimate reasonable expectation of privacy. More than 40 years ago, the Supreme Court established the Third-Party Doctrine in *United States v. Miller*, 425 U.S. 435 (1976), explaining the absence of a Fourth Amendment protection for subpoenaed bank records because the defendant had voluntarily conveyed his checks and deposit slips to his bank. Similarly, in *Smith v. Maryland*, 442 U.S. 735 (1979), the Court again applied the Third-Party Doctrine, holding

that an individual had no Fourth Amendment interest in dialed telephone numbers because that information was "voluntarily" given to the telephone company.

The question in *Carpenter* remained how the Third-Party Doctrine applies in this new technological context. The government stressed that the legal analysis under the *Miller* case remains applicable despite the new technology, because the records were the carrier's "business information," not Carpenter's personal records. Oral Arg. Tr.*, Carpenter*, at 40 (Nov. 29, 2017). In opposition, Carpenter argued that the *Miller* and *Smith* decisions are outdated and distinguishable because cell location records are more "sensitive personal information" and are not voluntarily disclosed. *Id.* at 4. Such records, Carpenter argued, are private and cannot be disclosed by service providers without prior customer authorization. *Id.* at 11.

The concern in *Carpenter* was that if the Third-Party Doctrine allows the government to skirt Fourth Amendment and statutory probable cause warrants to obtain cell-site location information under the SCA, there will be no limit on the electronic information that can be obtained. In its brief in opposition, the government disagreed that the Third-Party Doctrine would "permit unregulated" government collection of emails; rather, the government seemed to carve out an exception. It explained that "[e]mails [are] *routed through regular providers,* and its content, like those sealed in a letter, may remain private." Br. in Opp'n, *Carpenter*, at 12 (Sept. 25, 2017) (emphasis added). Citing a case from 140 years ago, *Ex Parte Jackson*, 96 U.S. 727 (1878), the government wrote that reliance on a third party "to deliver communications" does not destroy an "expectation of privacy in the content." Br. in Opp'n at 37.

This position is potentially inconsistent with the government's stance that the sensitivity of contents is not determinative. *Id.* at 38. The government could argue that the Third-Party Doctrine would apply to emails or messages sent through online apps which, like cell records, are transmitted with a third party provider, even though the customer has "no choice" but to store the information with the provider. In other situations, the customer may store older emails and other content with a third party other than the routing company, such as a PST file of "old" email stored with Amazon even though it was "routed" by Gmail. It remains unanswered whether this data would remain private under the SCA. But *Carpenter* suggests there may be a limit to how much email *metadata* law enforcement authorities can obtain without a probable-cause warrant. Email generates its own location information, that information is stored long-term, and email is an integral part of modern communications.

The Court also rejected the application of Third-Party Doctrine to the cell records on the grounds that they are "business records." Slip. Op. at 15. Chief Justice Roberts said that in "mechanically applying" the Third-Party Doctrine to this case, the government did not appreciate the nature of the CSLI; application of the Third-Party Doctrine would have been a "significant extension." *Id.* There is a "world of difference" between the cell-site records and the bank records in *Miller* and pen register records of *Smith*. *Id.* The Court explained that its prior decisions considered the "nature of the particular documents sought." *Id.* at 16. The Court rejected the government's position that information had been "shared" or voluntarily conveyed to a third party, the telephone company, resulting in a loss of privacy. Slip. Op. at 17.

The *Carpenter* ruling did not directly discuss emails, but emphasized the intrusive and "intimate" nature of the requested CSLI. Slip. Op. at 12. Furthermore, the majority pointed out that the logic of the *Smith* decision in 1979 did not extend to the "qualitatively different category of cell-site records." *Id.* at 11. It correctly observed that "few [in 1979] could have imagined" the "detailed and comprehensive" role of telephone cellular communications. *Id.* These statements appear to recognize the privacy of email contents with regard to the Third-Party Doctrine, although storage location will be an important factor. Nonetheless, the Court characterized its decision as a "narrow one" relating to location information. It did "not disturb" the application of *Smith* or *Miller*. Rather, it held that a SCA "order" is insufficient and a "warrant" is required to obtain CSLI.

Microsoft: Control or Location

In *United States v. Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), the Court previously had been asked to address whether data stored in foreign countries by U.S.-based companies is beyond the reach of the federal authorities. The Court of Appeals for the Second Circuit had ruled that the SCA did not extend to electronic communications stored in extraterritorial jurisdictions and, therefore, the government could not retrieve emails stored abroad. While the government argued that the focus of the SCA is on the disclosure of the documents, which occurs domestically (Oral Arg. Tr., *United States v. Microsoft*, 17-2, at 8-11 (Feb. 27, 2018)), Microsoft argued that the focus of the statute is on where the records are stored, which is internationally (*Id.* at 36). Several Justices, including Justice Ginsburg, questioned why the Court should not allow this issue to be resolved by Congress.

Passing CLOUD Clears the Day

Shortly after oral argument, Congress did just that. On March 23, 2018, it enacted the CLOUD Act, which allows authorities to bypass MLATs and gives law enforcement the ability to directly compel production of electronic data by a party storing its data abroad, as well as allowing foreign governments to access data stored in the United States.

The CLOUD Act contains four key changes. First, newly enacted 27 U.S.C. §2713 eliminates any question as to whether the common law standard of possession, custody, or control applies. The government can compel disclosure *"regardless of whether such communication, record, or other information is located within or outside of the United States"* (emphasis added). This change mooted *Microsoft.* In *a per curiam* opinion on April 17, 2018, the Supreme Court vacated and remanded the Second Circuit's judgment in favor of Microsoft with directions to dismiss as moot.

Second, under new 27 U.S.C. §2703(h)(2), the ability to reach data stored abroad can now be challenged by a motion to quash based on comity, or reciprocal recognition of the foreign country's law.

Third, the CLOUD Act immunizes service providers from any and all legal actions arising from activities undertaken in accord with the amended the SCA.

Finally, the CLOUD Act makes changes to 18 USC §§2511(2), 2520(d), 2523, 2702 and 2707(e) that define the ability of foreign governments to seek data that is stored in the United States, allowing such access through "Executive Agreements" with foreign governments that are drafted by Attorney General and Secretary of State. Executive Agreements require that a foreign government's justice system be essentially similar in its protections to that of the United States, but they do not require Senate approval.

Conclusion

The relentless march of technology generates voluminous electronic data, and a user may not understand its extent or have a choice but to generate it. As a result, in cases like *Carpenter* and *Microsoft*, courts wrestle with balancing privacy expectations with technological advancements. *Microsoft* was resolved by statutory clarification of the jurisdiction of law enforcement. *Carpenter* answered a difficult — but limited — question of whether electronic location information required a warrant under the SCA and the limitations of the Third-Party Doctrine to that data. Although the SCA, at least on its face, protects the *content* of communications stored by providers, that content is only one of many forms of data that may be collected and stored by different providers. The full scope of standards, and protections, for email and its related data will remain ambiguous until they are resolved by either: 1) legislative action, like with *Microsoft*; or 2) judicial confirmation that contents of electronic communications have Fourth Amendment protections requiring search warrants, as in *Carpenter*.

*****

Jonathan S. Feld is the Leader of Dykema's Government Investigations and Corporate Compliance team, **Dante Stella** is a Member who focuses on electronic discovery and Christina Brunty is an Associate in the Litigation Group who focuses on privacy and data protection.
