January/February 2019 ▪ Volume 24 ▪ Issue 1

PRIVACY—WHEREFORE ART THOU? THE THIRD CIRCUIT DENIES 4TH AMENDMENT RIGHT

by Melinda F. Levitt

Melinda F. Levitt (mlevitt@foley.com) is a Partner in the Washington, D.C. office of Foley & Lardner LLP.

Let's face it—over the last 20 years or so, we have come to embrace, celebrate, and depend completely on electronic communications. What is more, we keep reaching out to grasp onto yet more ways to communicate, be it through Alexa (who just may be listening in on everything we do), our appliances, or whatever else is the internet-of-things gadget *du jour*. We love the ease, the fun, and the ability to run our lives from these contraptions. Without them we are lost.

But we also gave up something when we turned our lives over to these mechanisms. We lost our privacy. In fact, we gave it away—freely, if perhaps unwittingly. With each email, text, purchase, tweet, phone call, survey response, and picture posted, we leave an electronic trail leading right back to . . . *us*. Information about us can be found on our actual apparatuses, embedded in our messages, housed with our internet service provider, or floating somewhere in "the cloud." We don't actually know what information we have sent out there into the cyber world, how long it exists, or who can actually find that information and read it, decipher it, and use it against us. Some of us have started to worry about it too. "Isn't this information mine?" "Don't I have a say in what happens to it?" "Can't I stop others from seeing it?"

The Europeans have been addressing these issues for some time now, both at the individual national-level and on a European Community-wide basis. In May of last year, a whole new set of EC-wide rules and regulations went into force—the General Data Protection Regulation or, as it is more commonly known, the GDPR. A great deal has been written about the GDPR and all of its complexities and intricacies. But at its core, it was designed to do something that people forgot that they crave—it is designed to protect their privacy. As the EU Commission stated last year in a filing to the U.S. Supreme Court, the EC regards "protection of personal data [as] a fundamental right" and the GDPR reflects the EU's interest to protect that right.[1]

Thus, under the GDPR, individuals - that is, actual human beings - are given certain rights and controls over their so-called "personal data" . . . not only the content of their electronic messages but their very email addresses and any other information that may reveal who they are, where they live or work, what they purchase, or how they can be contacted via

telephone, mobile phone, text, etc. In addition, individuals *must be* notified if some other person or entity is collecting their information and sharing it with someone else—and the individual is granted the right of review of that data, the right to correct it, the right to demand that the information be erased, and the right to demand to be forgotten.[2] Granted, there are some exceptions to the rights and obligations outlined in the GDPR, such as when the collection and transfer of the personal data is "necessary for compliance with a legal obligation." GDPR, Art. 6(1)(c). However, it likely will be years before the EC Data Protection authorities and the European courts will be able to provide any meaningful guidance about when and under what circumstances these exceptions apply.

The bottom line is this: In Europe, privacy rights over personal data is regarded as a fundamental right of the individual. What about here in the United States? Well . . . well . . . well, we are thinking about it.

Shortly after the GDPR went into effect, California adopted the California Consumer Privacy Act 2018, but that statute is of more limited scope and has yet to be tested. Intel recently published proposed draft privacy legislation and is inviting public comment on its draft.[3] It also is possible that the new Congress may take up privacy rights issues and even, finally, amended the woefully outdated Stored Communications Act, which was adopted in 1986. But, as of now, we live in a hazy fog of privacy uncertainty.

That uncertainty was reinforced recently by the Third Circuit Court of Appeals in its September 20, 2018 decision in *Walker v. Coffey*, 905 F.3d 138, 358 Ed. Law Rep. 780, 2018 I.E.R. Cas. (BNA) 340348 (3d Cir. 2018). There, Walker, an employee of Pennsylvania State University, brought suit against the state prosecutor and a special agent employed by the state attorney general for using an invalid subpoena to induce her employer into collecting and producing her work emails. The emails were sought as part of a criminal investigation into Walker and her husband's activities.

Initially, defendants simply asked the University for Walker's work emails. However, University officials balked and asked for "something formal, a subpoena." *Id.* at 142. Defendants "complied" with that request by obtaining a blank subpoena form from the local courthouse but filled out only part of it before submitting it to the University. Defendants later conceded that by leaving out required information—including relatively innocuous information such as the date and place of document production—the subpoena was incomplete and unenforceable. *Id.* Despite this infirmity, the University's general counsel accepted the subpoena and ordered that Walker's work email be collected and handed over to the law enforcement officials. Walker, of course, was not informed of these developments.

Ultimately, all criminal charges against Walker were dismissed. Walker, however, then brought suit against defendants under 42 U.S.C.A. § 1983—the statute that permits an individual to file suit claiming that he/she was deprived of rights by a government official—arguing that the use of an invalid subpoena to obtain her work emails violated her Fourth Amendment right to be free from unreasonable search and seizure. Defendants moved to dismiss on the grounds that they had qualified immunity because Walker had no reasonable expectation of privacy in her work emails. *Id.* at 143. The district court agreed, find-

ing that Walker could not show a clearly established, constitutionally based right to privacy in the content of her work email. And the Third Circuit affirmed.

The Third Circuit began with the "touchstone of Fourth Amendment analysis"—i.e., whether a person has a constitutionally protected reasonable expectation of privacy over the subject matter seized. That analysis requires a two-part inquiry asking first whether the person manifested a subjective expectation of privacy and whether "society is willing to recognize that expectation as reasonable." *Id.* at 145 (citations omitted). The court concluded that Walker's subjective expectations were clear and, thus, focused only on the second question—whether Walker had an objectively reasonable expectation in the content of her work email.

From there, the Third Circuit conducted a survey of Supreme Court decisions, in particular those that addressed new advances in technology over the decades. Hence, in *Katz v. U.S.*, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967), the Court recognized a reasonable expectation of privacy in the contents of a telephone call conversation made from a public telephone, but in *Smith v. Maryland*, 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979), the Court held that there is no expectation of privacy in the telephone numbers actually dialed and that obtaining that information from the telephone company does not implicate the Fourth Amendment. As the Third Circuit explained "the core holding of Smith rested upon the established rule that 'a person has no legitimate expectation to privacy in information [he/she] voluntarily turns over to third-parties.' " *Id.* at 145-46 (quoting *Smith*, 442 U.S. at 743-44).

Moving from the world of telephone calls to more modern communication methods, the Third Circuit then discussed *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 130 S. Ct. 2619, 177 L. Ed. 2d 216, 30 I.E.R. Cas. (BNA) 1345, 93 Empl. Prac. Dec. (CCH) P 43907, 159 Lab. Cas. (CCH) P 61011 (2010), where the Supreme Court essentially punted on the question of whether a police officer had a reasonable expectation to privacy in text messages sent over a city-issued pager. There, the Supreme Court determined that it was premature to "elaborate[e] too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *Quon,* 560 U.S. at 759. Instead, the Supreme Court assumed for purposes of its opinion that Quon had a legitimate privacy expectation but ultimately determined that, because his messages were searched by his employer for a valid work-related purpose, Quon's Fourth Amendment rights were not violated. *Quon,* 560 U.S. at 764-75 (search conducted by an employer for non-investigatory work-related purposes or to investigate work-related misconduct does not constitute an impermissible search and seizure).

The Third Circuit then looked at two other decisions from 2010—one from the Eleventh Circuit, *Rehberg v. Paulk*, 611 F.3d 828 (11th Cir. 2010), aff'd, 566 U.S. 356, 132 S. Ct. 1497, 182 L. Ed. 2d 593 (2012), and one from the Sixth Circuit, *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010). In the former, the Eleventh Circuit deferred from declaring a privacy right in emails based on the view that because this information was shared with third-party internet service providers (ISPs), it is questionable whether an established reasonable expectation of privacy exists in that information. *Rehbert,* 611 F.3d at 847. The Sixth Circuit, however, went the other way and held that law enforcement officials violated

Warshak's Fourth Amendment rights when it subpoenaed his ISP and obtained over 27,000 emails sent to or received by Warshak's email address. The Sixth Circuit explained that an ISP is the functional equivalent of a post office or telephone company, and "the government cannot compel a commercial ISP to turn over the contents of emails without triggering the Fourth Amendment." *Warshak,* 631 F.3d at 286.

Strangely absent from the Third Circuit's discussion was any mention of the Supreme Court's June 2018 analysis of the intersection of the Fourth Amendment and modern technology—*Carpenter v. U.S.*, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018). There, as part of an investigation into a string of robberies, the FBI obtained, without a warrant, the suspects' cell-site location information, which is data automatically transmitted from a person's cellphone to near-by cell towers. Such information is routinely retained by wireless service providers for internal business purposes, but the information can be collected and produced. The Supreme Court held that Fourth Amendment privacy rights do attach to such personal location information and that the government may not obtain that information without a warrant. Again, however, the Third Circuit ignored this opinion.

In any case, Walker argued to the Third Circuit that the Sixth's Circuit's analysis and reasoning in *Warshak* should be followed. However, the Third Circuit declined, explaining that there is not a "robust consensus of cases of persuasive authority" in support of the Sixth Circuit's approach and that, in fact, *Warshak,* appeared to be something of an outlier. *Walker,* 905 F.3d at 148. Moreover, the Third Circuit found a distinction between Walker's situation and Warshak - i.e., Walker's claim arose out of a search and seizure of her work emails and that "an employee's Fourth Amendment rights in the workplace are subject to additional exceptions and limitations." *Id.* In particular, the Third Circuit emphasized that while an employee may have some privacy rights in work emails vis-à-vis outsiders, those rights are very much circumscribed vis-à-vis the employer's right to examine those communications. *Id.*

In coming to its conclusion, the Third Circuit further noted that "courts have long recognized that employers, as third parties who possess common authority over the workplace, may independently consent to a search of an employee's workplace documents or communications." *Id.* That bears repeating—**employers can independently consent to a search and seizure of an employee's emails and other documents, *regardless of the employee's privacy interest to the extent that they exist,* because the employer has common authority over the workplace and its equipment.** And the Third Circuit is not alone in reaching this conclusion. Rather, in reaching its conclusion, the Third Circuit specifically followed and adopted the Ninth Circuit's decision in *U.S. v. Ziegler*, 474 F.3d 1184, 153 Lab. Cas. (CCH) P 60340 (9th Cir. 2007).

The Third Circuit's bottom line here is that: 1) Walker had no reasonable privacy interest in her work emails because they were subject to the common authority of her employer Penn State; and 2) because Penn State had the authority to consent to a search and seizure over its employee's communications, the fact that the authorities' subpoena was deficient was meaningless. *Id.* at 149-50. Thus, the search and collection of Walker's emails conducted by Penn State at the

request of law enforcement officials was not illegal and did not violate Walker's rights. The Third Circuit did note that it was "dismayed" that the law enforcement officials relied on an invalid subpoena, but it is highly doubtful that this "dismay" provided any comfort to Walker. How could it have, given that the Third Circuit essentially held that tricking Walker's employer with a bogus subpoena, and then not telling her about it, did not matter at all?

Where does all this leave us? Uneasy. Worried. Waiting for the next privacy shoe to drop. Maybe we just should know better. The Fourth Amendment is a mighty bulwark designed to protect us, but it is surmountable. Each new advance in technology represents a new challenge to finding the right privacy balance. What we do know as of now is that if we have "shared" our information with our employer or some unknown data server located somewhere or anywhere, we remain vulnerable to the grasp of unknown "others." Moving forward, remember this motto: Users beware.

ENDNOTES:

[1]*See* Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party at 1 and 8, *United States v. Microsoft Corp.,* No. 17-2 (S. Ct. Dec. 13, 2017) (hereinafter "EC Amicus Brief"). The *Microsoft* case concerned a warrant issued under the Stored Communications Act by a federal magistrate judge in New York for an individual's electronic data/documents stored on a Microsoft server in Ireland and Microsoft's refusal to comply on the grounds that the Stored Communications Act did not have extraterritorial reach. The Second Circuit subsequently agreed with Microsoft and overturned the district court decision. The U.S. government appealed the matter to the Supreme Court and oral argument was held in February 2018; however, due to new legislation that clarified the extraterritorial application of the Stored Communications Act, the appeal was deemed moot and dismissed.

[2]*See generally* GDPR, Arts. 15, 16, 17 and 21. *See also* Letter from the Office of the European Data Protection Supervisor to the EC Directorates General for Competition, Trade, Anti-Fraud, and the European Investment Bank, Oct. 22, 2018, at 6 (confirming obligation under GDPR Art. 14(1)(e) of entities to inform employees about the identities of recipients of their personal data when their personal data is collected and transferred, but noting that governmental agencies with investigatory authority do not constitute a "recipient" when collecting information within the scope of their authority.)

[3]*See* "Intel's Approach to Privacy" and draft legislation attached thereto available at https://usprivacybill.intel.com.