New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
Litigation
An ALM Publication
WWW.NYLJ.COM
MONDAY, NOVEMBER 3, 2014

Should Old **Subpoena Compliance** Rules Apply in the **Digital Age**?

BY DOUGLAS DAVISON, PETER VIGELAND AND THOMAS KESSLER

For many years, the U.S. Securities and Exchange Commission (SEC) and other administrative agencies have routinely issued subpoenas to employers requesting any and all documents in an employer's possession, custody or control sent or received by particular employees within a specified date range. By their expansive terms, these subpoenas often require employers to produce their employees' personal or private communications, such as personal emails sent to spouses or significant others, text messages sent to friends and family, and records of personal Internet use on company computers. Issued without judicial authorization, these subpoenas can be based upon mere suspicion or official curiosity.[1]

This broad license given to administrative agencies stems from two sources: first, expansive Congressional grants of authority in statutes; second, court cases from the past century granting government agencies wide berth under the Fourth Amendment.[2] For example, Congress has authorized the SEC to subpoena documents upon a determination that the documents may be "relevant or material to [an] inquiry."[3] And the federal courts, adhering to a standard that has remained largely unchanged since 1946, recognize only a vague reasonableness limitation under the Fourth Amendment on the exercise of administrative subpoena authority.[4] For the employer receiving the subpoena, the subpoena only need be "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[5] This reasonableness standard "cannot be reduced to formula," because "relevancy and adequacy or excess in the breadth of the subpoena are matters variable in relation to the nature, purposes and scope of the inquiry."[6]

This weak reasonableness limitation is relaxed further by the federal courts' deployment of the third-party records doctrine, first articulated by the Supreme Court in 1976.[7] This doctrine provides that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,"[8] and is not entitled to notice of a subpoena requesting such information from third parties.[9] Federal courts often find that communica-

DOUGLAS DAVISON *is a partner at Wilmer Cutler Pickering Hale and Dorr in Washington, D.C. and vice-chair of the firm's securities department.* PETER VIGELAND *is a partner and* THOMAS KESSLER *is an associate in the New York office.*

tions sent or received by an employee using an employer's network are voluntarily provided to the employer, such that the communications are not entitled to any expectation of privacy.[10] As a result of the third-party records doctrine, employees often lack the opportunity and grounds to challenge subpoenas requiring the production by their employers of their personal communications sent or received over their employer's network.

An employer's capacity to produce more types of an employee's personal communications to the government has been greatly enhanced by technology over the last decade:

> All email that is sent or received through [company owned proprietary email accounts] is stored in the server and can be viewed later … . In order for an employer to monitor an employee's personal, web-based email, such as Yahoo, Hotmail, or Gmail, the employers have to exert a little more effort. New technology allows employers to monitor web-based email messages and chat conversations, record keystrokes, and take screenshots of what appears on an employee's screen. To use this new technology, employers must install additional software or hardware directly onto an employee's computer.[11]

In addition, an increasing number employees are using the same mobile devices (such as laptops, smartphones and tablets) for personal and business purposes. While employers historically issued company-owned mobile devices to their employees to enable remote access to company computers, employees are now using company devices to engage in personal computing that involves a host of private activities and content,[12] such that employees have little or no basis to protect personal communications.[13] Additionally, a growing number of employers have implemented "bring your own device" (BYOD) policies, allowing employees to use their personal mobile devices to create, store and transmit work-related data.[14] BYOD turns an employee's personal mobile device into something used for both personal and work-related activities.[15] Certain courts have indicated that an employer's "carefully crafted electronic use policy could eradicate, or at least considerably [diminish], an employee's reasonable expectation of privacy"[16] in the personal use of employer-issued or BYOD electronic devices such as laptops and cell phones.[17]

But help is on the way. Recent decisions by the courts have expressed concern that, in the modern age of ubiquitous electronic communications (all of which are to some extent voluntarily disclosed to third parties), rigid adherence to the third-party records doctrine could erode the privacy guarantees of the Fourth Amendment by enabling the government to subpoena and aggregate voluminous personal information from third parties with only a minimal showing of relevance or need. In the digital age, these recent decisions suggest that it is time to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.

In *United States v. Jones*,[18] the Supreme Court unanimously held in 2012 that the attachment of a global positioning system (GPS) to a car for a period of four weeks amounted to a search under the Fourth Amendment. Justice Sonia Sotomayor, in her concurrence, and Justice Samuel Alito, in his concurrence joined by three other justices, ventured beyond the particular issue presented in the case and discussed the need to rethink expectations of privacy in the digital age. The five justices who concurred in *Jones* stressed that the modern advances of technology have removed one of the main impediments to intrusive government surveillance—namely, the difficulty and cost of traditional investigative techniques.[19] Both concurrences observed the ease with which surveillance can now be conducted and the ease by which the government can now mine and synthesize that data.[20] These factors caused Sotomayor to question the continued viability of the third-party records doctrine in the digital age:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks … . But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[21]

An employer's capacity to produce more types of an **employee's personal communications** to the government has been greatly enhanced by technology over the last decade.

In another recent case from 2010, *United States v. Warshak*,[22] the U.S. Court of Appeals for the Sixth Circuit, holding that an individual has a reasonable expectation of privacy in emails stored with an Internet service provider (ISP), barred the government from compelling production of certain documents from an ISP absent a warrant or some exception to the warrant requirement. The court observed that although "a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account, we doubt that will be the case in most situations … . [T]he mere ability of a third-party intermediary [such as an ISP] to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy … . Nor is the right of access [decisive as to the reasonableness of an expectation of privacy]."[23] The Sixth Circuit stressed the quantity and quality of information stored in a personal email account:

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.[24]

While the need to rethink reasonable expectations of privacy in the digital age seems obvious, fashioning new rules interpreting the Fourth Amendment is a daunting task. Indeed, while Alito's concurrence in *Jones* discusses the need to rethink privacy in the digital age, it makes no effort to delineate new rules establishing the point at which the GPS monitoring became unreasonable. Instead, Alito's concurrence simply concludes that "[w]e need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[25]

Despite the unquestionable difficulties in fashioning new Fourth Amendment standards, a few new approaches can be advanced in the context of administrative subpoenas issued to employers for employee communications. First and foremost, it seems as if the third-party records doctrine should not bar all claims of a reasonable expectation of privacy in personal communications sent over an employer's network, even where an employer's policies provide for the monitoring and interception of such communications. In evaluating whether an expectation of privacy in emails sent over an employer's network is reasonable under the Fourth Amendment, the federal courts should analyze the privacy expectations in the context of a modern, technologically advanced world and shift its analysis to what society expects to remain private.[26] Recognizing that an employee has a reasonable expectation of privacy in certain

personal communications "voluntarily disclosed" to an employer would provide employees with a constitutional basis to challenge administrative subpoenas from the government which demand production of those communications from their employers.

Second, the courts may want to consider requiring, in certain circumstances, that notice be provided to employees whose personal emails and texts are being collected. Merely recognizing that a reasonable expectation of privacy may exist for personal emails sent over the employer's network would not sufficiently protect an employee's privacy interests if the employee remains ignorant of their imminent production.[27] To be sure, an employee's interest in receiving notice of a subpoena's request must be balanced against important public interests in maintaining the secrecy and efficacy of administrative investigations. To address these countervailing concerns, the courts might allow delayed notice to the employee upon a showing by the administrative agency that prior notice could jeopardize the investigation. Permitting delayed notice to employees in such circumstances would allow administrative agencies to maintain the secrecy and efficacy of their investigations and avoid tipping-off targets while at the same time providing some protection to the employee's reasonable expectations of privacy.

Third, the federal courts could grant permissive intervention to employees under Rule 24(b) of the Federal Rules of Civil Procedure to challenge the reasonableness of administrative subpoenas requesting production of their personal communications from their employers. The courts could require that the employee bear the initial burden of proving through in camera inspection that the subpoena's request would require the production of personal communications for which the employee has a reasonable expectation of privacy.[28] Upon such a showing, the court could allow the employee to challenge the reasonableness of the subpoena's request. The court could then balance the employee's privacy interest with the communications' relevance to the agency's investigation. Where communications are clearly personal or private in nature, the courts could require the government to make some showing of need before compelling the production of the subject emails and texts.[29] Alternatively, if the scope of the subpoena is so broad as to require the production of myriad personal and private communications, the courts could consider imposing ex ante limiting provisions to screen out those communications from production.

•••••••••••••●●●•••••••••••••

1. See *SEC v. Brigadoon Scotch Distrib.*, 480 F.2d 1047, 1053 (2d Cir. 1973) (noting that "even if the agency request is motivated by 'nothing more than official curiosity,' the subpoena is enforceable because agencies have a legitimate interest in seeing that the law and the public interest are maintained … .") (quoting *United States v. Morton Salt*, 338 U.S. 632, 652 (1950)).

2. See, e.g., *Oklahoma Press Publishing v. Walling*, 327 U.S. 186, 208 (1946); *SEC v. Jerry T. O'Brien*, 467 U.S. 735, 743 (1984).

3. 15 U.S.C. §78u(b).

4. See *Oklahoma Press*, 327 U.S. at 208 ("[T]he fair distillation [of the court's prior cases], in so far as they apply merely to the production of corporate records and papers in response to a subpoena … seems to be that … the Fourth [Amendment], if applicable, at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant. The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable."). While *Oklahoma Press* equivocated about whether the Fourth Amendment's reasonableness limitation was applicable to administrative subpoenas, subsequent Supreme Court cases have treated this issue as settled. E.g., *See v. City of Seattle*, 387 U.S. 541, 544 (1967).

5. *City of Seattle*, 387 U.S. at 544 (quoted with approval in *Donovan v. Lone Steer*, 464 U.S. 408, 415 (1984); *Bowsher v. Merck & Co.*, 460 U.S. 824, 858 (1983)). In addition, the Supreme Court has held that in an enforcement proceeding, an administrative agency must demonstrate "good faith" in issuing the subpoena. "Good faith" requires a showing that (1) the investigation is conducted pursuant to a legitimate purpose, (2) the information requested under the subpoena is relevant to that purpose, (3) the agency does not already have the information it is seeking with the subpoena, and (4) the agency has followed the necessary administrative steps in issuing the subpoena. *United States v. Powell*, 379 U.S. 48, 57-58 (1964).

6. *Oklahoma Press*, 327 U.S. at 209.

7. See *United States v. Miller*, 425 U.S. 435, 443 (1976).

8. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

9. *SEC v. Jerry T. O'Brien*, 467 U.S. 735, 743 (1984).

10. See, e.g., *Smyth v. Pillsbury*, 914 F. Supp. 97, 101 (E.D. Pa. 1996) ("[W]e do not find a reasonable expectation of privacy in email communications voluntarily made by an employee to his supervisor over the company email system notwithstanding any assurances that such communications would not be intercepted by management. Once [the employee] communicated [the information] to a second person (his supervisor) over an email system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."); *Garrity v. John Hancock Mut. Life Ins.*, No. CIV.A. 00–12143–RWZ, 2002 WL 974676, at *1-2 (D. Mass. May 7, 2002) (finding that emails sent over company intranet system were not private).

11. Meir S. Hornung, "Think Before You Type: A Look at Email Privacy in the Workplace," 11 Fordham J. Corp. & Fin. L. 115, 125-26 (2005).

12. See David Navetta, "The Security, Privacy and Legal Implications of BYOD (Bring Your Own Device)," InfoLawGroup, March 28, 2012, http://www.infolawgroup.com/2012/03/articles/byod/the-security-privacy-and-legal-implications-of-byod-bring-your-own-device (last visited Oct. 8, 2014).

13. See, e.g., *Mintz v. Mark Bartelstein & Associates*, 885 F. Supp. 2d 987, 998-1000 (C.D. Cal. 2012) (holding that an employee had only a limited expectation of privacy in his personal data on a device that he personally owned because the employee also used the device for work, the employer paid for the phone service, and the employee had signed a data policy acknowledging that he had no expectation of privacy in the phone's data); *Shefts v. Petrakis*, 758 F. Supp. 2d 620 (C.D. Ill. 2010) (holding that an employer's communication policy providing for the monitoring and interception of its employees' communications was sufficient to eradicate an employee's expectation of privacy in text messages sent over the employer's network from the employee's personally-owned BlackBerry device).

14. Gary G. Mathiason et al., "The 'Bring Your Own Device' to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions," The Littler Report, May 10, 2012, http://www.littler.com/files/press/pdf/TheLittlerReport-TheBringYourOwnDeviceToWorkMovement.pdf (last visited Oct. 8, 2014).

15. Id.

16. Robert D. Brownstone et al., "Privacy of Email and Text Messages—Case Law Sprinting to Catch Up to Modern Technology," Bloomberg Law Reports—Privacy & Information (March 2011), available at http://www.fenwick.com/Fenwick-Documents/fenwick_west_brownstone_ghassemi-vanni_cho_article.pdf (last visited Oct. 8, 2014).

17. *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010) (noting that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated"); *In re Reserve Fund Securities and Derivative Litigation*, 275 F.R.D. 154, 163-64 (S.D.N.Y. 2011) (holding that a company's email policy was sufficient to eradicate an employee's expectation of privacy in personal emails that he sent to his wife over the company's email system using a company computer, and that the employee therefore could not invoke the marital privilege in response to an SEC subpoena requesting production of those emails).

18. 132 S. Ct. 945 (2012).

19. See id. at 956 (Sotomayor, J., concurring) ("[B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.' … The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to a democratic society.'") (internal citations omitted); id. at 963-64 (Alito, J., concurring) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.").

20. Id. at 955-56 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. 'Disclosed in [GPS] data … will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.' The government can store such records and efficiently mine them for information years into the future.") (internal citations omitted); id. at 964 (Alito, J., concurring) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving.").

21. Id. at 957 (Sotomayor, J., concurring) (internal citations omitted).

22. 631 F.3d 266, 288 (6th Cir. 2010).

23. Id. at 286-87 (internal citations omitted).

24. Id. at 284.

25. 132 S. Ct. at 964.

26. Abraham Tabaie, "Protecting Privacy Expectations and Personal Documents in SEC Investigations," 81 S. Cal. L. Rev. 781, 822 (2008).

27. Id. at 816 ("[A] third party, like a corporation holding a director's personal documents, has no interest in fighting a subpoena for those documents because if the company fully cooperates, it could resolve an incident with minimum penalties or sanctions.").

28. Id. at 814.

29. Id. at 815.