New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
Litigation
An ALM Publication
WWW.NYLJ.COM
TUESDAY, JANUARY 17, 2012

Do Privacy Rights In Electronic Communications Exist?

BY HECTOR GONZALEZ, JAMES McGUIRE AND REBECCA S. KAHAN

IN AN ERA of increasing disclosures of information that once was thought to be private, determining when a personal communication will be shielded from disclosure is often difficult. Both common law and the Fourth Amendment protect the right to privacy. Individuals asserting a constitutional protection must generally demonstrate "a subjective expectation of privacy…that society accepts as reasonable."[1] Individuals asserting a common law claim must make a similar showing.[2] Courts have made clear that there is no reasonable expectation of privacy in communications to large audiences, such as posts on social media websites.[3]

However, as people use new technology and devices to communicate, seemingly private disclosures are leaving electronic trails that are visible to others, forcing courts to address whether the tracks are discoverable and where the bounds of privacy lie. Recent cases addressing how these electronic trails affect an individual's expectation of privacy indicate two generally relevant considerations: (i) social norms and (ii) the existence of written policies that address the disclosure of stored information.

No Bright-Line Rule

The Supreme Court has declined to answer directly the question of when a reasonable expectation of privacy exists in electronic communications. In *City of Ontario, California v. Quon et al.*,[4] the Court was asked to consider whether an employer can search text messages sent through an employer-issued device. Quon, a police officer who had sent text messages through a police department phone, argued that he had a reasonable expectation of privacy in the communications that protected the text messages from being the subject of a search. The city of Ontario argued that it had reviewed the messages in connection with a legitimate investigation of the use of technology by its employees.

The Court agreed with the city of Ontario and upheld the search on the ground that it "was reasonable even assuming Quon had a reasonable expectation of privacy."[5] Thus, the Court did not need to address the issue of whether the author of the text messages had a reasonable expectation of privacy in their contents. The majority nevertheless stated that the Court "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment."[6] In its discussion, the majority indicated that there would likely be two relevant factors: evolving social norms and pre-existing policies concerning the communications.[7] Although the decision thus does not purport to set a bright-line rule, Justice Antonin Scalia stated in his concurrence[8] that it gives a "heavy-handed hint" of the relevant considerations. Justice Scalia went on to criticize the majority opinion, noting that "in saying why it is not saying more, the Court says much more than it should."[9]

Usage Records Are Not Private

Without a formal test, courts are forced to grapple on a case-by-case basis with issues related to the reasonable expectation of privacy concerning communications that are stored and transmitted by a third party.

Recently, a district court upheld the issuance of a subpoena pursuant to the Stored Communications Act (SCA)[10] for information maintained by Twitter. In connection with an ongoing investigation of Wikileaks, the government sought, and a magistrate judge granted, an order that required Twitter to turn over certain information about account holders who had posted various Tweets.[11] The government sought, among other things, the account information provided by the account holders when they registered their accounts, as well as records related to their use of Twitter, including the associated IP addresses. Petitioners, certain Twitter users who were the subject of the order, moved to vacate the order. They argued, in part, that the disclosure of IP address information violated their Fourth Amendment rights. Specifically, they maintained that the order authorized a search, and that they had a reasonable expectation of privacy because the search would reveal information that was not revealed through the normal use of Twitter.

The court disagreed, finding that there was no reasonable expectation of privacy in the IP address-related information. It analyzed the nature of communications on the Internet, and the related disclosures made by Twitter, disclosures that all users are required by Twitter to acknowledge. Specifically, the court recognized that:

(i) Service providers frequently maintain records of IP addresses that access their website;

(ii) Twitter requires all users to disclose their IP address information;

(iii) All users must sign a privacy policy prior to using Twitter; and

(iv) The privacy policy discloses that Twitter collects certain information that can be disclosed, among other reasons, if disclosure is necessary to comply with the law.

The district court then concluded that "[i]f Twitter decided to record or retain [the IP addresses], any privacy concerns were the consequence of private action, not government

HECTOR GONZALEZ *and* JAMES M. McGUIRE *are partners in the white collar and securities litigation group at Dechert in New York.* REBECCA S. KAHAN *is an associate at the firm.*

action. The mere recording of IP address information by Twitter and subsequent access by the government cannot by itself violate the Fourth Amendment."[12]

The analysis did not, however, end there. The court next considered whether, even if a reasonable expectation of privacy had existed, the petitioners had relinquished their claims of privacy through disclosure to a third party.[13] The Supreme Court has long held that, where an individual discloses information as a necessary condition of using a service, no reasonable expectation of privacy exists in the disclosed information.[14] Because "[p]etitioners relied on Internet technology to access Twitter, indicating an intention to relinquish control of whatever information would be necessary to complete their communication," the so-called third-party doctrine applied. The court went on to conclude that "[t]he fact that a particular user may not see or know which IP address he is using at a particular moment does not create a reasonable expectation of privacy in the information. If the user is communicating over the Internet, intermediary computers and the destination computer must know the IP address as a condition of that communication. Under the Fourth Amendment, that fact renders unreasonable any expectation of privacy in the IP address."[15]

Content May Be Private

Although no reasonable expectation of privacy exists in information that is transmitted to a service provider when making a communication, the contents of that message may be private. Whether the content of the message is private likely will depend on who else has access to the communication.

In *United States v. Warshak*, the court considered whether an individual's Fourth Amendment rights were violated when the government compelled his internet service provider to turn over the contents of his e-mails.[16] In addressing whether the expectation of privacy in the content of an e-mail is an expectation that society is prepared to accept as reasonable, the court noted that two factors are critical.

> First, the very fact that information is being passed through a communications network is a paramount Fourth Amendment consideration.... Second, the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.[17]

The court observed that the mere fact that a third party can access the contents of a communication does not extinguish the expectation of privacy[18] and "h[e]ld that a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'"[19]

If others have access to the content of the communication, however, a reasonable expectation of privacy may not exist. In *SEC v. Reserve Mgmt Co. Inc.*,[20] the court was asked to determine whether a reasonable expectation of privacy existed in e-mails that were transmitted over a company server. The sender of certain e-mails asserted that e-mails sent from his employer-issued e-mail address to his wife were shielded from disclosure pursuant to the spousal privilege.

For the privilege to apply, however, the communications cannot have been made in the presence of a third party.[21] In the context of electronic communications, determining the privilege's applicability requires the court to "consider whether [the author of the communication] was on actual or constructive notice that these communications could be 'read[] or otherwise monitored by third parties.'"[22]

To make this determination, the court applied the four-factor test set out in *In re Asia Global Crossing, Ltd.*:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[23]

The e-mail policies of the company provided, among other things, that: (i) employees were not to use e-mail for personal use; (ii) the employer reserved the right to access and inspect an employee's computer and e-mail; and (iii) e-mails and other documents maintained on company computers were subject to review and disclosure to third parties.[24] Based on those policies, the court concluded that the husband did not have a reasonable expectation of privacy in his communications and, therefore, the communications were not shielded from disclosure.[25]

Although the communications in *Reserve Mgmt.* were not protected, at least one court has found that an employee did have a reasonable expectation of privacy in e-mails sent from a personal e-mail address on an employer issued device, even though images of those e-mails were maintained on the device. In *Stengart v. Loving Care Agency Inc.*, an employee, Stengart, used her work-issued laptop to send e-mails to her attorney through a personal, password-protected e-mail account.[26] After Stengart was terminated, Loving Care, her previous employer, searched her laptop and recovered certain communications to and from her attorney that were made on her personal e-mail account. Stengart argued that the communications were protected, and Loving Care argued that Stengart had waived any relevant privileges because she did not have a reasonable expectation that the e-mails would remain private.

Applying the *Asia Global* test, the court disagreed with Loving Care. The court concluded that Stengart did have a reasonable expectation of privacy in her communications, focusing, in part, on the policies of Loving Care, and on the fact that Stengart's e-mail account was protected by a password. Because those policies permitted employees to use company-issued devices for personal communication, and because Stengart limited access to her personal e-mails with a password,[27] she had a reasonable expectation that her communications would remain private.[28]

As the Supreme Court recognized in *Quon*, it is nearly impossible to anticipate all of the ways in which people will communicate through electronic means. And with each type of communication that is made, investigators and litigants will try to find ways to obtain access to, and use, any traces of potentially relevant information that is left behind on servers or storage devices. As difficult as it is to anticipate the novel ways in which people will communicate, so too is it difficult to predict whether the government, employers or others will be granted access to the information, and where the line of privacy will be drawn. What is foreseeable is that each case will require a court to engage in a detailed analysis of the ways in which technology is being used, and the nature of the notices and disclosures that are given to the authors of the communications.

Finally, it also is foreseeable that these courts will proceed cautiously. As the Supreme Court stated in *Quon*, "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of technology before its role in society has become clear."[29] But there also are costs attendant to this caution. In his partial concurrence, Justice Scalia urged that "[a]pplying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice."[30] As he went on to state "'[t]he-times-they-are-a-changin' is a feeble excuse for a disregard of duty."[31] For now, to echo another Bob Dylan song, the answer to the question this article addresses is "Blowin' in the Wind."

1. *California v. Greenwood*, 486 U.S. 35, 39 (1988).
2. See, e.g., *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (S.D.N.Y. 2005) (citations omitted).
3. See, e.g., *United States v. Lifshitz*, 369 F.3d 173 (2d Cir. 2004) (citing *Guest v. Leis*, 255 F.3d 325 (6 Cir. 2001)) ("Users would logically lack legitimate expectation of privacy in materials intended for publication or public posting"); *Romano v. Steelcase Inc.*, 30 Misc. 3d 426, 434 (N.Y. Sup. Suffolk County 2010) ("Indeed, as neither Facebook nor MySpace guarantee complete privacy, Plaintiff has no legitimate reasonable expectation of privacy").
4. 130 S.Ct. 2619 (2010).
5. Id. at 2628-29.
6. Id. at 2630.
7. Id.
8. Justice Scalia concurred with the opinion in part, and concurred with the judgment.
9. Id. at 2635.
10. 18 U.S.C. §2701 et seq.
11. *In re Application of the United States for an Order Pursuant to 18 U.S.C. §2703(d)*, 2011 WL 5508991 (E.D. Va. Nov. 10, 2011).
12. Id. at *16.
13. Id. at *17.
14. See, e.g., *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979).
15. *Application of the United States*, 2011 WL 5508991 at *19.
16. 631 F 3d 266 (6th Cir. 2011).
17. Id. at 285 (citations omitted).
18. Id. at 286.
19. Id. at 288 (citations omitted).
20. *SEC v. Reserve Mgmt Co. Inc.*, 275 F.R.D. 154 (S.D.N.Y. 2011).
21. Id. at 159.
22. Id. (quoting *Asia Global*, 322 B.R. at 258-59) (revision original).
23. Id. at 160 (quoting *Asia Global*, 322 B.R. at 257).
24. Id. at 164.
25. Id.
26. 990 A.2d 650 (N.J. 2010).
27. Courts have indicated that whether or not access to a communication is limited by privacy settings, such as through the use of a password, does not control the question of whether the communication is private. See, e.g., *Patterson v. Turner Construction Co.*, 931 N.Y.S. 2d 311, 312 (1st Dept. 2011) ("The postings on plaintiff's online Facebook account, if relevant, are not shielded from discovery merely because plaintiff used the service's privacy settings to restrict access, just as relevant matter from a personal diary is discoverable" (citations omitted)).
28. 990 A.2d at 663.
29. *Quon*, 130 S.Ct. at 2629 (citations omitted).
30. Id. at 2635.
31. Id.