Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 31, ISSUE 11 / OCTOBER 31, 2013

EXPERT ANALYSIS

Email and Telephone Communications: What Privacy Protections Remain?

By Janet Stiven, Esq.
Dykema

Recent publication of formerly "top secret" government memoranda and Foreign Intelligence Surveillance Court opinions regarding the U.S. government's alleged bulk collection of email and telephone content, Internet usage data and metadata has resulted in renewed public debate about the scope of current laws and privacy protections.[1]

Today, there is no question that the federal government collects and analyzes bulk telephone and Internet content and metadata from individuals in the name of national security; however, public debate continues about these activities. At issue is whether U.S. citizens and businesses still have a reasonable expectation of privacy with respect to their email and telephone communications.[2]

This commentary highlights some of the U.S. laws that protect the privacy of email and phone communications and related data and how they may be used by the government to intercept and access such communications and data.

An examination of the current laws reveals a complex and confusing framework of statutes, regulations, case law and executive orders that affect the protection and privacy of email and telephone communications. Much of the confusion surrounding the laws involving surveillance of electronic communications arises from the fact that the laws were adopted over a period of many years, in a piecemeal fashion, and have not been adapted to reflect continuing changes in communication technology.

REASONABLE EXPECTATIONS OF PRIVACY

The Fourth Amendment of the U.S. Constitution protects citizens against unreasonable search and seizure and sets forth a reasonable expectation of privacy. Pursuant to the Fourth Amendment, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[3]

The U.S. Supreme Court explored the boundaries of the Fourth Amendment privacy protections for modern communications in *Katz v. United States*, 389 U.S. 347, 352 (1967). In that case, the high court was asked to determine the extent of the Fourth Amendment's protections related to telephone communications. The Supreme Court's holding in *Katz* has since been cited for the broad proposition that there is an expectation of privacy in the content of a telephone call. Consequently, the acquisition of such communications may result in a "search" or "seizure" within the meaning of the Fourth Amendment, depending on the circumstances.[4]

At issue is whether U.S. citizens and businesses still have a reasonable expectation of privacy with respect to their email and telephone communications.

EXCEPTIONS TO FOURTH AMENDMENT PROTECTIONS

Fourth Amendment case law continued to evolve after the *Katz* decision, with exceptions being asserted to the Fourth Amendment's privacy protections, such as the third-party and public exposure exceptions.

The "third-party doctrine" says that persons have no legitimate expectation of privacy when they share information with others. This doctrine has been used as a basis to find some electronic communications unprotected by the Fourth Amendment if they involve disclosures to third parties.[5]

For example, in *Smith v. Maryland*, the U.S. Supreme Court held that a list of telephone numbers a person dialed did not warrant Fourth Amendment protection. The court reasoned that there could not be any expectation that the numbers that telephone users dialed were protected secrets because people know that numerical information is relayed to a telephone company.[6]

The "public exposure" exception, as the name suggests, provides that persons have no legitimate expectation of privacy related to information shared in public places. For example, the Supreme Court held that attaching a radio beeper to a container stored in an automobile and then following the automobile on the public streets and highways did not constitute a search under the Fourth Amendment because there is no reasonable expectation of privacy in movements from one public place to another.[7]

OTHER FEDERAL PRIVACY LAWS

In addition to Fourth Amendment privacy protections, a number of other laws affect the privacy of email and telephone communications. They are briefly summarized below.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 provides privacy protections for domestic electronic communications. The law prohibits the unauthorized interception of any wire, oral or electronic communication, which is defined as the acquisition of the "contents" of the communication. It also prohibits the use and disclosure of the contents of such a communication if it was unlawfully intercepted. For purposes of these prohibitions, "contents" is defined as "information concerning the substance, purport or meaning of the communication."[8]

The Foreign Intelligence Surveillance Act of 1978 establishes rules for the U.S. government's surveillance of agents of a foreign power without a search warrant. So long as the target of an investigation is a "foreign power" or an agent of a foreign power, government surveillance based upon probable cause is allowed.[9]

The Electronic Communications Privacy Act of 1986 was adopted, in part, to update wiretap laws to reflect then-current technologies.[10] The ECPA consists of three titles:

- Title I, commonly known as the Wiretap Act, prohibits the unauthorized interception of wire, oral or electronic communications.
- Title II, commonly known as the Stored Communications Act, governs the privacy of, and restricts access to, stored electronic communications and records of communication service providers.
- Title III, the Pen Register Act, creates a procedure for governmental installation and use of pen registers as well as trap-and-trace devices. It also prohibits the installation or use of these devices except for law enforcement and foreign intelligence investigations.[11]

In 1994, Congress further expanded the protections of the ECPA by enacting the Communications Assistance for Law Enforcement Act, Pub. L. No. 107-56, 115 Stat. 272, to address privacy protections related to cordless telephones and radio transmissions.

POST–9/11 CHANGES TO PRIVACY

The 9/11 terrorist attacks led to significant changes in U.S. privacy laws and the U.S. government's right to collect data in the interest of national security. The USA Patriot Act of 2001 was adopted shortly after 9/11.[12] Since that time, it has been amended to expand its scope to provide the U.S. government with a basis to monitor and access oral, wire and electronic communications of individuals and businesses for a variety of reasons, so long as a foreign intelligence investigation is "a significant purpose" of the investigation.[13] Until recently, the Foreign Intelligence Surveillance Court, the secret court that is authorized to approve surveillance orders, has provided few published opinions about the permitted scope of the government's surveillance and access to email and telephone communications.

In 2004, Congress further expanded the use of such collected data by allowing for inter-agency sharing when it passed the Intelligence Reform and Terrorism Prevention Act, and it added a new category for monitoring purposes to include any non-U.S. person who engages in or prepares for international terrorism.[14] This abolished the need for a nexus between the non-U.S. person and a foreign power or terrorist group. Today, if the U.S. attorney general designates someone as a potential terrorist threat, that person may have the contents of his or her wire or electronic communications monitored, so long as proper authorization is obtained.

HOW THESE OTHER PROTECTIONS APPLY

Although cases construing the Fourth Amendment provide a basis for asserting privacy protections related to certain email and telephone communications, cases construing the ECPA and the Patriot Act privacy protections for email and telephone communications are less clear.[15]

The Wiretap Act, which prohibits the intentional interception of any oral, wire or electronic communication, applies to any person, even law enforcement. Under the law, there are important differences among oral, wire and electronic communications. An oral communication is an utterance made under the expectation that it is not being intercepted. So, a reasonable expectation of privacy depends upon the context of the utterance at the time it is made.

However, with wire and electronic communications, there is an automatic expectation of privacy under the statute. Wire communications are defined as an "aural transfer" (containing a human voice) made through a communications service that uses wires, cables or similar connections operating in interstate or foreign commerce. A telephone call would thus be a covered wire communication. An electronic communication is broadly defined as the transfer of any form of data by electronic or optical systems affecting interstate or foreign commerce, not made by wire. In addition, email is a covered electronic communication under the Wiretap Act.

The Wiretap Act prevents the interception of the contents of a communication. The term "contents" is defined under the Wiretap Act as "[a]ny information concerning the substance, purport, or meaning of [the] communication."[16] The term "contents" has the same definition under the Stored Communications Act as it does under the Wiretap Act; however, the statutes have different timing components. The Wiretap Act only covers the acquisition of data at or near the time the messages are transmitted. Stored emails or telephone records, which are not intercepted while made but are retrieved later, are covered under the Stored Communications Act. The SCA generally prohibits any entity that provides an electronic communication service, or ECS, to the public from disclosing the contents of communications in storage to any entity, including the government, unless certain conditions are satisfied.

CONTENT VS. METADATA

Cases addressing privacy issues arising from Fourth Amendment protections related to telephone and email communications focus on whether there is a reasonable expectation of privacy. An analysis of the Fourth Amendment privacy protections available to email and telephone

The Wiretap Act, which prohibits the intentional interception of any oral, wire or electronic communication, applies to any person, even law enforcement.

communications requires consideration of the methods and information related to each of these types of communications.

Email communications contain information about the email and Internet protocol addresses of the sender and recipient, in addition to the subject and content of the message. Telephone communications (both landline and cellular telephone communications) involve the actual communication in addition to metadata or information about the telephone numbers of the caller and the receiver as well as the date, time and length of the call. Cellular telephone communications also include geolocation information.

There is a split among federal courts regarding whether there a reasonable expectation of privacy in electronic communications.[17]

In considering the expectation of privacy in email and telephone communications, courts have distinguished the "content" from the "metadata" associated with the communication:

- Some courts have held that metadata associated with telephone calls, text messages and email are not "contents" and thus would not trigger ECPA privacy protections.[18]
- At least one court has held that geolocation data stored on cellphones is not part of the content of communication, but is simply an automatically generated set of data, much like a telephone number.[19]
- Some courts regularly permit law enforcement agencies to obtain cellphone location data, but others have adopted the "mosaic theory" to hold that there is a reasonable expectation of privacy in cellphone geolocation information.[20]
- Email subject lines have been considered to be the content of an email.[21]

In considering the expectation of privacy in email and telephone communications, courts have distinguished the "content" from the "metadata" associated with the communication.

Metadata are information relating to electronic communications that are generated by electronic communication devices and ECS providers. Metadata include information about the time and duration of an electronic communication, the electronic device used in the communication, the addresses or numbers contacted and geolocation information. There is a growing concern that metadata may be more revealing than the content of electronic communications, because metadata may be more easily analyzed electronically than the content of communications — the analysis of which may require translation and some human analysis.

Generally, metadata that are automatically tracked or stored in making a phone call or in sending an email will not be considered content. But any user-generated content related to the actual message he or she intended to communicate (such as a subject line, the body of an email, a text or spoken words on the phone) is typically protected from interception.[22]

BROAD ACCESS BY THE FEDERAL GOVERNMENT

Unlike private parties, whose rights to intercept and access email and telephone communications are restricted, the Stored Communications Act allows the government to access email, voicemail and related data under certain circumstances.

Three definitions are important to the application of the compelled-disclosure provisions of the SCA: electronic storage, electronic communication service and remote computing service, or RCS.

Electronic storage is "any temporary, intermediate storage of a wire or electronic communication ... and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." An ECS is intended for "data transmissions and electronic mail," and an RCS is intended for outsourced computer processing and data storage. The law provides different privacy protections to each of these services, so it is important to determine the applicable classification of service.[23]

If a computing service meets the definition of an ECS, then the government's obligations concerning compelled disclosure vary depending on how long the email has been in the provider's electronic storage. A search warrant is required if the contents of wire or electronic communications have been in ECS storage for 180 days or less. Any court with jurisdiction over the offense may issue such a warrant. For content of wire or electronic communications in ECS storage for more than 180 days, the government can access the content of such communications without prior notice to the customer if it obtains a warrant, uses an administrative subpoena or obtains a court order under Section 2703(d) of the Stored Communications Act.

For contents of wire or electronic communications stored by an RCS, the government may require the RCS provider to disclose such content pursuant to the same statutory means that apply to ECS providers. The government, however, has a more expanded right to compel disclosure of contents of wire and electronic communications in an RCS than those stored with an ECS. It also has greater access to ECS and RCS records concerning the customer than the contents of the wire and electronic communications. The government may access such communications and customer records by simply asserting "reasonable grounds to believe" that the content and records are "relevant and material to an ongoing criminal investigation."

Privacy protections under an ECS and RCS afford limited protection to personal information about the user, such as his or her name and physical email or IP addresses. An ECS or RCS provider can disclose this information to both governmental and non-governmental entities upon receipt of an administrative subpoena. Although this personal identifiable information may be revealed in certain situations, courts have typically protected communications and data stored with ECS and RCS providers from compelled disclosure to parties in a civil case. However, the Stored Communications Act may not necessarily protect the contents of electronic communications from direct requests to a party during civil litigation.[24]

When it comes to requiring the government to show evidence before conducting a search, the SCA applies a lower burden for the government to satisfy in obtaining court orders compelling *ex parte* production of documents when the documents are electronic and stored on a third-party's server. Also, the definition of electronic storage for ECS providers is more limited than what most people would expect, since it applies only to temporary storage incident to the transmittal of the communication or for backup purposes. This means that there may be limited privacy protections afforded to email under the SCA.

Under the Patriot Act, the U.S. government monitors email and telephone communications and uses "data mining" techniques that involve collecting personal information from a variety of databases to analyze large amounts of telephone and email metadata to find links and patterns in behavior.[25] The purpose of this data mining is not necessarily limited to identifying potential acts of terrorism; some data mining involves fraud detection and immigration analysis.[26] There has been continued debate as to whether the aggregation and mining of such data are appropriate. Intelligence agencies are authorized under the FISA and the Patriot Act to obtain broad electronic surveillance orders from the Foreign Intelligence Surveillance Court.

CONCLUSION

Laws that protect email and telephone content may not apply to the metadata associated with the communication. Furthermore, in the name of national security, it appears that the government may access, retain, process, analyze and disseminate intelligence from the both the content and metadata of communications it acquires, although the legal rationale for these activities remains unsettled. Because of the deep insights that can be gained by the government's ability to access email and telephone communications, further debate and clarifying legislation on the scope of Fourth Amendment and statutory protections for these communications are important.

Because of the deep insights that can be gained by the government's ability to access email and telephone communications, further debate and clarifying legislation on the scope of Fourth Amendment and statutory protections for these communications are important.

NOTES

[1] *See e.g.,* Foreign Intelligence Surveillance Court Memorandum Opinion (J. Bates) (redacted) (Sept. 25, 2012); Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) (redacted) (Nov. 30, 2011); Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) (redacted) (Oct. 3, 2011). The Foreign Intelligence Surveillance Court is the secret court responsible for overseeing the scope of the U.S. government search activities.

[2] Glenn Greenwald & Spencer Ackerman, *NSA Collected U.S. Email Records in Bulk for More Than Two Years under Obama,* THE GUARDIAN, June 27, 2013, *available at* http://www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama; James Risen & Eric Lichtblau, *Bush Secretly Lifted Some Limits on Spying in U.S. After 9/11, Officials Say,* N.Y. TIMES, Dec. 15, 2005; Siobhan Gorman, Devlin Barrett & Jennifer Valentino-DeVries, *Secret Court Faulted NSA for Collecting Domestic Data,* WALL. ST. J., Aug. 21, 2013 ("The National Security Agency violated the Constitution for three years by collecting tens of thousands of purely domestic communications without sufficient privacy protection, according to a secret national-security court ruling."); Donna Cassata, *NSA Court Order For Phone Records Of Verizon Users Is A Renewal, Dianne Feinstein Says,* HUFFINGTON POST, June 6, 2013, *available at* http://www.huffingtonpost.com/2013/06/06/nsa-court-order_n_3396848.html.

[3] U.S. Const. amend. IV.

[4] *See* FISA Court Memorandum Opinion and Order (Oct. 3, 2011), *supra* note 1, at 67. ("The government accepts the proposition that the acquisition of electronic communications can result in 'search' or 'seizure' under the Fourth Amendment.").

[5] *United States v. Miller,* 425 U.S. 435, 440 (1976) (holding that an individual has no Fourth Amendment privacy interest in information released to a third party and later conveyed by that third party to a government entity). *See also* Jacob M. Small, *Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet,* 23 GEO. MASON U. CIV. RTS. L.J. 255, 263-66 (Summer 2013).

[6] *Smith v. Maryland,* 442 U.S. 735, 743 (1976).

[7] *See* Michael T.E. Kalis, *Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance,* 13 U. PITT. J. TECH. L. & POL'Y 1, 10 (Spring 2013) (*citing United States v. Knotts,* 460 U.S. 276 (1983)).

[8] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 18 U.S.C. § 2510; *see also United States v. N.Y. Tel. Co.,* 414 U.S. 159 (1977) (holding that Title III does not cover the acquisition of metadata with pen registers).

[9] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, 50 U.S.C. § 1801.

[10] Electronic Communications Privacy Act of 1986, Public Law No. 99-508, 100 Stat. 1848, 18 U.S.C. §§ 2510–2522, 2701-2712, 3121-3126.

[11] Wiretap Act, 18 U.S.C. § 2510; Stored Communications Act, 18 U.S.C. § 2701. *See also* William Jeremy Robison, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act,* 98 GEO. L.J. 1195, 1206 (April 2010) (It is important to keep in mind that the Stored Communications Act has been in existence for more than 20 years and was drafted on the basis of technology that existed at that time and prior to the use of current cloud computing services. The fragmented email system in use at the time of the SCA's passage helps to explain common misunderstandings today about the act and its privacy protections.); Pen Register Act, 18 U.S.C. § 3121.

[12] USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

[13] USA Patriot Act, § 218, 115 Stat. 291 (amending 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)); *see also In re Sealed Case,* 310 F.3d 717 (U.S. Foreign Intelligence Surveillance Ct. Rev. 2002) (addressed the issue by concluding that "by using the word 'significant,' [the Patriot Act] eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses." The court thus did not provide any guidance into how such determinations of significance are to be made.).

[14] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638; *Id.* at § 6001.

[15] *See* FISA Court Memorandum Opinion and Order (Oct. 3, 2011), *supra* note 1, at 68 ("While a warrant is typically required to acquire electronic communications, Section 702 of the Patriot Act provides a 'foreign intelligence exception' to the warrant requirement of the Fourth Amendment.").

[16] 18 U.S.C. § 2510(8).

[117] *Rehberg v. Paulk,* 598 F.3d 1268 (11th Cir. 2010) (email not protected) (Government issued subpoenas to Internet service provider requesting email records. Court held no Fourth Amendment violation because subpoenas covered information plaintiff had provided voluntarily to third parties and for which

he did not have a reasonable expectation of privacy.); *see contra, United States v. Warshak et al.,* 631 F.3d 266, 283 (6th Cir. 2010) (email is protected) (Government formally requested ISP preserve emails to or from defendant — copies that would not have existed absence government's preservation request. Government then subpoenaed ISP; later also served *ex parte* court. In all, government compelled ISP to reveal contents of about 27,000 emails. Court made analogy to telephone calls and letters sent via mail: "trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private."). *See also* Small, *supra* note 5, at 269, 270 (discussing whether email communications are within the scope of the third-party doctrine and therefore allow the government to approach the third party to gain access without implicating Fourth Amendment privacy protections).

[18] *See* Kalis, *supra* note 7, at 11 (Courts have relied on the third-party exception to hold that cellphone users have no expectation of privacy in their cell-site location information because the cell user voluntarily conveys this information to the service provider by using the cellphone.) (citations omitted).

[19] *In re iPhone Application Litig.,* 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012).

[20] *See* Kalis, *supra* note 18, at 8, 15-16 (The courts that allow law enforcement agencies to obtain cellphone location data usually rely on the third-party and public-exposure exceptions to the Fourth Amendment's reasonable expectation of privacy. The courts that say these exceptions do not apply have adopted the so-called "mosaic theory," which says that society recognizes as reasonable an expectation of privacy in the totality of one's movements.") (citations omitted).

[21] *Optiver Australia Pty. Ltd. v. Tibra Trading Pty. Ltd.,* No. 12-cv-80242, 2013 WL 256771 (N.D. Cal., San Jose Div. Jan. 23, 2013); *see also United States v. Maxwell,* 45 M.J. 406, 417 (C.A.A.F. 1996) ("[T]he tenor and content of e-mail conversations between appellant and his correspondent, 'Launchboy,' reveal a reasonable expectation that the conversations were private.").

[22] *See* Christopher R. Brennan, Katz Cradle: Holding On to Fourth Amendment Parity in an Age of Evolving Electronic Communication, 53 Wm. & Mary L. Rev.1797, 1812-13 (2012).

[23] 18 U.S.C. § 2710(15) and (17); 18 U.S.C. § 27711(2); *See also Warshak,* 631 F.3d 266 at 286 (*citing* Patricia L. Bellia et al., Cyberlaw: Problems of Policy and Jurisprudence in the Information Age 584 (2d ed. 2004); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It,* 72 Geo. Wash. L. Rev. 1208 (2004)).

[24] *See* Derek S. Witte, Bleeding Data in a Pool of Sharks: The Anathema of Privacy in A World of Digital Sharing and Electronic Discovery, 64 S.C. L. Rev. 717, 725 (Spring 2013).

[25] Glenn Greenwald & Spencer Ackerman, *NSA Collected U.S. Email Records In Bulk For More Than Two Years Under Obama,* The Guardian, June 27, 2013, *available at* http://www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama; Glenn Greenwald, *Verizon forced to hand over telephone data — full court ruling,* The Guardian, June 5, 2013, *available at* http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order; Stephen Rex Brown, *Verizon is giving the feds phone records for all of its US customers: report,* N.Y. Daily News, June 5, 2013, *available at* http://www.nydailynews.com/news/national/verizon-giving-feds-phone-records-customer-article-1.1364575; Homeland Security Organization, Subchapter II–Information Analysis and Infrastructure Protection, 6 U.S.C. § 121(d)(13).

[26] *See* Gov't Accountability Office, Data Mining Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain, No. GAO-05-866, at 4 (Aug. 2005), *available at* www.gao.gov/new.items/d05866.pdf.

Janet Stiven, a member of **Dykema**'s business services department, has more than 20 years of experience representing a diverse group of clients, including medical device, information technology and e-commerce companies. She often works in the cloud technology space advising clients on how to protect information. She can be reached at jstiven@dykema.com.