Bloomberg Law Reports®

March 15, 2012

Technology Law

Privacy & Information Law

The Incredible Shrinking Expectation of Online Privacy


Contributed by Stephen M. Juris and Jacob W. Mermelstein, Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer, P.C.

In 1985, in what would turn out to be an incredibly prescient article, a tech-savvy graduate student at Yale warned that the traditional legal framework governing privacy was not well-equipped to deal with recent developments in computer technology, including the increasing use of "electronic mail."[1] The inverse relationship between technology and privacy had been lamented for more than a century. In 1890, for instance, Louis Brandeis and Samuel Warren warned that recent inventions such as "instantaneous photographs" and "numerous mechanical devices" had threatened to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[2] The article's insight, however, was that the advent of new technologies like the Internet presented a unique threat to privacy that was different in kind from the "mechanical devices" of the past. First, vast quantities of private information would become accessible from third-party sources, without any tangible physical intrusion. Second, advances in computing technology would make it technologically feasible to mine countless bits of identifying information - each relatively innocuous - and assemble them into a portrait as revealing as a paper-bound diary.

Today, with the ever-expanding use of e-mail, cloud computing, and social networks by businesses and individuals alike, the most intimate details of our lives and work are increasingly stored online, and thereby entrusted to the custody of third parties. Unfortunately, although our digital footprint has never been more expansive, the legal framework governing the privacy of that information remains sorely outdated, incomplete, and poorly understood.

The Stored Communications Act

There is no comprehensive federal legislation protecting the privacy of electronic information. Rather, an *ad hoc* patchwork of statutes apply, depending on the type and age of the information in question, the type of user, and the type of entity storing or transmitting the information.[3] For e-mail or other electronic user data stored by entities like Google, Hotmail, Yahoo!, Twitter, Facebook, LinkedIn, or their equivalents, the principal federal statute regulating users' privacy is the Stored Communications Act ("SCA"), a part of the Electronic Communications Privacy Act of 1986.[4]

Congress's stated goal in enacting the SCA was to "update and clarify" existing privacy protections in light of "dramatic changes in new computer and telecommunications technologies," including the relatively recent adoption of "large-scale electronic mail operations" and the use of offsite data banks for "sophisticated data processing."[5] At the time, a chief concern was that e-mail and other electronic data might not be adequately protected under existing Fourth Amendment jurisprudence because the information had been revealed to a third party (*i.e.*, the e-mail service provider or remote storage facility).[6] Through the SCA, Congress attempted to create a statutory "zone of

privacy" safeguarding electronic subscribers and protecting them from having their personal information wrongfully used or publicly disclosed.[7]

Though well-intentioned, this statutory scheme has been almost universally criticized as a "dense and confusing" mess.[8] At its most basic level, the statute forbids voluntary disclosure of certain information when privately stored by service providers, and sets forth the procedural steps that the government must take in order to compel disclosure of that information. It also sets forth criminal and civil penalties for unauthorized access to protected information. Unfortunately, a significant number of unanswered questions remain concerning the application of the SCA in light of the profound changes in technological and social practices that have occurred since it was passed more than twenty-five years ago. Moreover, even where the SCA is clear, it is often out of step with modern expectations of privacy and its application is inconsistent with the Fourth Amendment - an ironic turn of events given its original purpose.

– Uncertainty Caused by Obsolete Terminology

To understand the SCA and recognize its limitations, perhaps the single most important point to note is that it applies only to two types of entities: an Electronic Communication Service ("ECS"), defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications," and a Remote Computing Service ("RCS"), defined as "provision to the public of computer storage or processing services by means of an electronic communications system."[9] Unfortunately, even under the most expansive reading, it is not possible to shoehorn the full range of modern Internet technologies into these two categories, which were conceived of in an era when VHS players were a fixture of living rooms, the fax machine was considered cutting-edge technology, and the web browser had not yet been invented.

Courts are in agreement that Internet Service Providers ("ISPs") like Verizon or Comcast fall into one or both of these two categories, as do e-mail providers like AOL, Google's Gmail, or Microsoft's Hotmail. Video-sharing sites like YouTube and social networking sites like Twitter and Facebook have also been found to be functioning as an ECS or RCS, so long as videos, messages, "wall-posts," and the like are not accessible to the world at large.[10] However, the status of other service providers remains unclear. For instance, every one of the major search engines (Google, Yahoo!, Bing) routinely collects identifying information, including the specific search queries that a user enters, a list of websites accessed, and the IP address utilized, and often stores that information for a period of months or even years. These search engine logs have been described as a "virtual honeypot" for law enforcement because they are often exceedingly revealing.[11] And in many respects, the privacy interests implicated by such queries are even more significant than the privacy interests asserted - and litigated - in connection with law enforcement officials' efforts to obtain library records.[12] However, the level of privacy protection afforded here is uncertain because a search engine doesn't fit neatly into the RCS or ECS categories. Legislative history suggests that if Internet search engines had been in operation at the time, the statute likely would have included them in its scope. At least some commentators have suggested that a search engine should be considered a covered entity. However, the government has repeatedly advocated for a strict construction of the SCA, arguing that search engine logs are not covered because neither category (ECS or RCS) is a precise fit under the SCA's plain language.[13]

While search engines like Google present the most notable categorization quandary, a similar problem is presented by any online service that compiles logs of user information based on data entered into forms on a website.[14] Recently, Google announced a new, "unified" privacy policy under which it intends to aggregate private information from its users' search queries with data it has gathered from the use of other services it operates, such as YouTube, Google+, or even a user's actual location as recorded by a Google Maps application on a GPS-enabled mobile device. While Google's public disclosure is laudable, such a comprehensive amalgamation of data is likely to prove irresistible to both law enforcement and civil litigants. The scale of the information being compiled by Google, and its centrality to the ways in which the modern computer user relies on the Internet, only highlights the need for greater clarity.

Limitations on Privacy Protection

Assuming that an entity is properly characterized as an ECS or RCS, the statute presents a barrier for both government entities and private parties seeking to obtain stored electronic information, although for the government that barrier is often not very high. For private parties, the SCA absolutely bars the service provider from disclosing the "content" of an e-mail or other stored communication.[15] However, if only "non-content" information is sought, discovery may be requested directly from the ECS or RCS provider. Thus, for example, the SCA would not automatically bar issuance of a third-party subpoena to a service provider for records showing that a defendant was sending a text message at the time of a car crash, or for the e-mail addresses of the individuals with whom a litigant was frequently corresponding. However, the actual content of those texts or e-mail messages could not be obtained from the service provider without the consent of the account holder. Disregard of this principle can be costly: service providers routinely move to quash private civil subpoenas and courts have imposed sanctions or even civil penalties for a litigant's attempt to improperly secure "content" directly from an ECS or RCS.[16] Of course, a civil litigant may still attempt to obtain the "content" of a communication through ordinary discovery requests directed to the account holder.

For the government, the pertinent question isn't what information may be obtained, but rather what legal process is necessary in order to compel disclosure. A search warrant, issued upon probable cause, is required for only the most sensitive data. However, lesser process is sufficient where the government seeks "non-content" information such as connection logs, the credit card that was used to pay for services, a subscriber's name or physical address, or even a list of websites that he or she accessed. To compel disclosure of such "non-content" data, the government may simply use an administrative subpoena, or a specialized

court order pursuant to 18 U.S.C. § 2703(d), which a court will issue upon a showing that the communication is "relevant and material to an ongoing criminal investigation." Regardless of the type of data sought, there also is no guarantee that a subscriber will receive advance notice of the government's request.[17]

Even with respect to data stored by an ECS or RCS, the statute suffers from significant shortcomings. For example, the SCA only requires the government to obtain a warrant when it seeks new e-mails (those "in electronic storage" in an ECS for less than 180 days), while older e-mails may be obtained via a less onerous process. This 180-day cutoff is a vestige of a long-outdated technology in which e-mails that remained on a server for a lengthy period were considered abandoned. It makes little sense today. Further paring the SCA's privacy protections, some (but not all) courts have held that an e-mail ceases to be held in "electronic storage" whenever it has been accessed or read, and thus is discoverable by the government even *prior* to 180 days with a mere subpoena or court order.[18] Moreover, even if the government fails to comply with the strictures of the SCA, a defendant's remedies are limited. Unless the error amounts to a Constitutional violation, the improperly obtained data will not be suppressed.

The SCA's statutory scheme is also outdated in a different respect. As technology progresses, the line between data stored locally and remotely is increasingly blurred. With the rising popularity of always-on broadband connections and "thin-client" computing, in which inexpensive, low-power computers or mobile devices rely on web-based applications and "cloud" data, it is often of little significance whether a particular piece of data is physically stored on a computer's local hard drive or on a distant server. Indeed, in many cases a user may not even know whether certain data is stored locally or remotely. Thus, a privacy scheme that ties the level of protection to the location where data is stored, or to the identity of the company storing a user's private data, appears increasingly outmoded.

Looking Beyond the Stored Communications Act

The limitations and weaknesses in privacy protection provided by the SCA have caused litigants and courts to look anew at the Fourth Amendment. In an important 2010 decision, *United States v. Warshak*, the Sixth Circuit held that the Fourth Amendment bars the government from accessing e-mails without a warrant, even though the SCA purports to allow access under a less stringent standard.[19] The court rejected the government's contention that any reasonable expectation of privacy was precluded by the ISP's contractual right to access the defendant's e-mails, noting that the mere possibility of access was insufficient to defeat a reasonable expectation of privacy - particularly given the extensive use and revealing nature of stored e-mails. The *Warshak* decision reflects just how far technology and social practices have evolved from the era in which the SCA was passed. Whereas the SCA was enacted to be *more* protective than the Fourth Amendment, the opposite is more often true in practice. Whether that ruling signals the start of a trend remains unclear. However, the Supreme Court's recent GPS-tracking decision in *United States v. Jones* provided some promising signals. Although Justice Scalia's opinion for the majority focused on the narrow issue of whether a physical intrusion had occurred, Justice Scalia also acknowledged that "it may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy."[20] In an important concurring opinion, Justice Sotomayor went further, offering a preview of her stance on the inevitable digital privacy issues to come:

> [I]t 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. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.

Justice Sotomayor added: "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] While the SCA's outmoded terminology and other structural limitations often provide limited privacy protection, or none at all, many of the most serious concerns would be mitigated if the Supreme Court ultimately follows Justice Sotomayor's lead in taking a broad view of users' expectation of privacy in online interactions.

Separately, efforts to enact more modern and comprehensive legislation seem to be gaining momentum. In February, the White House released a detailed report with recommendations for new federal consumer privacy legislation, including a "Consumer Privacy Bill of Rights."[22] The White House also simultaneously announced that multiple companies, including Google, Yahoo!, Microsoft, and AOL, had voluntarily committed to add "Do Not Track" technology to most major web browsers in order to make it easier for users to opt out of some online data-gathering. Although the framework has been lauded by many privacy advocates as a step in the right direction, the use of the term "Bill of Rights" is somewhat of a misnomer. The proposal would apply only to private parties, and it would not in any way limit the government's ability to search and seize electronic information without a warrant. For the time being, the Fourth Amendment in the (actual) Bill of Rights will have to suffice.

Stephen M. Juris is a partner at Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer, P.C. in New York City, where he focuses principally on white collar defense and governmental investigations, regulatory enforcement matters, and complex commercial litigation. Jacob Mermelstein is an associate with the firm and a former editor of the Harvard Journal of Law & Technology. *For more information on this topic, please contact Stephen Juris at SJuris@maglaw.com. For further information about Morvillo Abramowitz, please visit www.maglaw.com.*

[1] Larry Hunter, *Public Image*, 44 Whole Earth Review 32 (Jan. 1985).

[2] Louis Brandeis and Samuel Warren, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890).

[3] *See, e.g.,* Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030; Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. § 1801 *et seq.*; Cable Communications Policy Act of 1984, 47 U.S.C. § 521 *et seq.*; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506; Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039; Communications Act of 1934, 47 U.S.C. § 222; Privacy Act of 1974, 5 U.S.C. § 552a; Wiretap Act, 18 U.S.C. §§ 2510-2522; Pen Register and Trap and Trace Devices Statute, 18 U.S.C. §§ 3121-27.

[4] The SCA is codified as 18 U.S.C. §§ 2701 to 2712.

[5] S. Rep. No. 99–541, at 2-3 & n.2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556-57.

[6] *Id.* at 2-3 (citing *United States v. Miller*, 425 U.S. 435 (1976)).

[7] *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 610 (E.D. Va. 2008).

[8] 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, 1208 (2004).

[9] 18 U.S.C. § 2510(15); 18 U.S.C. § 2711(2).

[10] *See, e.g.*, *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010); *cf. Pietrylo v. Hillstone Rest. Group*, No. 06–5754 (FSH), 29 IER Cases 1438 (D.N.J. Sept. 25, 2009) (upholding jury verdict in favor of plaintiff in civil suit alleging improper retrieval of information from private MySpace page).

[11] Omer Tene, What Google Knows: Privacy and Internet Search Engines, 2008 Utah L. Rev. 1433, 1435 (2008).

[12] Library records and records of book purchases have historically been granted heightened protection because of their revealing nature. *See, e.g.*, *United States v. Rumely*, 345 U.S. 41, 57-58 (1953) (Douglas, J., concurring); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1053 (Colo. 2002) ("[T]he First Amendment embraces the individual's right to purchase and read whatever books she wishes to, without fear that the government will take steps to discover which books she buys, reads, or intends to read."); *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 573 (W.D. Wis. 2007) (quashing government subpoena seeking the identities of Amazon.com book buyers).

[13] Tene, *supra*, at 1477 (concluding that Google likely an RCS with respect to web searches); *Gonzales v. Google,* Case No. 5:06-mc-80006-JW (N.D. Cal. Feb. 24, 2006) *(*Reply Memorandum of U.S. in Support of Motion to Compel) (contending that Google is neither an RCS nor ECS).

[14] *See Crowley v. Cyberspace Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (dismissing SCA claim against Amazon.com because company was not an ECS); *In re Jetblue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 308 (E.D.N.Y. 2005) ("[B]usinesses offering their traditional products and services online through a website are not providing an 'electronic communication service'") (citation omitted); *see generally* Kerr, *supra*, at 1230 (arguing that Ebay probably not an RCS, but recognizing ambiguity in SCA).

[15] *Viacom Int'l Inc. v. Youtube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) ("An ISP is statutorily prohibited from complying with a private party's subpoena for the content of emails, because the SCA's prohibition on voluntary disclosure "contains no exception for . . . civil discovery requests.").

[16] *See, e.g.*, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004) (reversing dismissal of SCA claim against party that served ECS with unlawful subpoena for e-mail contents).

[17] Where a search warrant is used, no advance notice is ever required. Where a less onerous procedure is followed, advance notice is required in some instances, but may be delayed where such notification would risk an "adverse result." *See* 18 U.S.C. §§ 2703(b)(1)(A), 2705(a).

[18] *Compare Theofel*, 359 F.3d at 1075-77, *with United States v. Weaver*, 636 F. Supp. 2d 769, 771-73 (C.D. Ill. 2009).

[19] *United States v. Warshak*, 631 F.3d 266, 284-88 (6th Cir. 2010).

[20] *United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945, 954 2012 BL 14420 (2012).

[21] *Id.* at 957.

[22] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012).