

Lead Report

Privacy

Appellate E-Communication Privacy Rulings Lend Impetus to Push for Reforms to ECPA

Recent appellate rulings that have challenged and rejected the constitutionality of the Electronic Communications Privacy Act—to the extent that it gives law enforcement access to data about private digital communications without a warrant—are providing additional motivation for lawmakers to update the 25-year-old statute.

The Stored Communications Act, 18 U.S.C. § 2703—part of the Electronic Communications Privacy Act—sets standards for law enforcement access to, and communications services' disclosure of, electronic communications. The law incorporates a complicated matrix of privacy protections for electronic communications, based on the age of communications, where they are located, and who has seen them.

Lawmakers attempted to update the 1986 statute in 2000, but the terrorist attacks on Sept. 11 sidelined that effort in favor of expanded electronic surveillance capabilities under the Patriot Act. Since then, the uptake of new technologies—such as cloud computing and behavioral tracking for marketing purposes—has made the ECPA appear even more shopworn.

Finally, recent constitutional rulings—especially the Sixth Circuit's *United States v. Warshak*, No. 08-3997 (6th Cir. Dec. 14, 2010)(15 ECLR 1925, 12/22/10)—supply an added element to the policy reform discussion: not only do these rulings suggest the need for reform, they create constitutional limits on what lawmakers can write into any new electronic privacy statute.

Warshak held that if the SCA permits law enforcement to obtain the contents of stored e-mail without a warrant, then it is unconstitutional. If law enforcement needs a warrant to obtain the contents of all reasonably private communications, then other open ECPA questions may not need to be answered.

Some of those questions—also explored in BNA's *At a Glance: ECPA's Unresolved Questions* and *Recent ECPA Litigation Highlights Uncertain Digital Privacy Protections*—include:

- Is webmail held by an “electronic communications service” or a “remote computing service?”
- Does opening of e-mail destroy its status as a ECS-held “backup?”
- Is location data merely account information for which law enforcement need only request a court order, or does it have a more private character that makes it start to look like content information?
- Are documents and other communications, including cloud computing storage networks or messages on social networks, held by an electronic communications service or a remote computing service?

At a Glance: ECPA's Unresolved Questions

Courts have struggled to apply the Electronic Communications Privacy Act—with its segmented data types and prioritization of service providers—to communications services that did not exist when the statute was enacted in 1986.

Fourth Amendment issues aside, key legal questions under the law include:

- When does a private e-mail server qualify as “a facility through which an electronic communication service is provided” *Devine v. Kapasi*, No. 09-6164 (N.D. Ill. June 7, 2010)(15 ECLR 988, 6/23/10)(holding that a private e-mail server was not an e-communications “facility,” after identifying a split on the issue)?
- Who has the authority to consent to the disclosure of stored communications after *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008)(13 ECLR 861, 6/25/08)?
- Can webmail qualify for protection under the 18 U.S.C. § 2703(a) warrant requirement, discussed in *Jennings v. Jennings*, No. 4711 (S.C. Ct. App. July 14, 2010)(15 ECLR 1257, 8/11/10)?
- Does the warrant requirement for messages in “electronic storage” expire when messages are opened, discussed in *United States v. Weaver*, No. 09-3006 (C.D. Ill. July 15, 2009)(14 ECLR 1050, 7/29/09)?
- Is stored e-mail that is synched with another machine or device—and simultaneously deleted—stored for “backup protection” and thus shielded by the warrant standard, discussed in *KLA-Tencor Corp. v. Murphy*, No. 09-1922 (N.D. Cal. May 11, 2010)(15 ECLR 803, 5/19/10)?
- Are messages and other documents stored on social networks and cloud computing services protected under the act, discussed in *Crispin v. Audigier Inc.*, No. 09-9509 (C.D. Cal. May 26, 2010)(15 ECLR 907, 6/9/10)?
- Is location information merely account-type data that can be obtained via an administrative or trial subpoena, discussed in *In re Application of United States of America for Order Directing Provider of Electronic Communication Service to Disclose Records to Government*, No. 08-4277 (3d Cir. Sept. 7, 2010)?

The adoption of a single, probable cause standard for law enforcement access to stored communications could solve all these problems, e-commerce attorneys told BNA in a series of recent interviews. Each practi-

tioner is a part of the Digital Due Process coalition, which has also made that recommendation (analysis of the group's *Recommended Principles for ECPA Reforms* in this story).

Law enforcement, however, has vehemently opposed this proposal. Representatives from the Department of Justice have told lawmakers to avoid changes that would compromise critical investigations (15 ECLR 1459, 9/29/10).

Lawmakers held hearings in the 111th Congress to hear more about potential ECPA updates (15 ECLR 1459, 9/29/10), and Sen. Patrick Leahy (D-Vt.), who was the lead Senate author of ECPA and is the chairman of the Senate Judiciary Committee, has pledged to review the statute this year (16 ECLR 111, 1/19/11).

Services at the forefront of this debate—Facebook and CTIA—the Wireless Association—weighed in on potential ECPA reforms in recent BNA interviews, as well (*see comments in this story*). Facebook is part of Digital Due Process, and only produces the contents of communications in response to a warrant. CTIA has taken no position on recent location data privacy rulings, but would encourage lawmakers to reiterate services' defenses if they take up these issues.

ECPA's Intricate Communications Privacy Matrix. The ECPA contains standards for law enforcement access to the contents of electronic messages held by communications services. The procedures are exceptions to the statute's general rule, at 18 U.S.C. § 2702(a), that a person or entity providing communication service to the public shall not knowingly divulge the contents of a communication.

The statute's protections depend on whether the communications are in "electronic storage," 18 U.S.C. § 2703(a), or are held by a "remote computing service." The statute's highest showing—probable cause—is reserved for the contents of communications held in "electronic storage" and are no older than 180 days.

Law enforcement should only be able to access the contents of e-mailed communications with a warrant. All these intricate distinctions should fall away, both as a matter of constitutional law and in the statute.

PROF. SUSAN FREIHALD, UNIVERSITY OF SAN FRANCISCO
SCHOOL OF LAW

The statute defines "electronic storage," at 18 U.S.C. § 2510(17), as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

The ECPA's warrant requirement lapses after a communication has been in electronic storage for 180 days: At that point the requirements for disclosure of the contents of electronic communications merge with require-

ments for communications held by "remote computing services."

Those communications must be disclosed to a governmental entity pursuant to a warrant or court order, 18 U.S.C. § 2703(b).

Recommended Principles for ECPA Reforms

The Digital Due Process coalition has proposed four principles that they assert lawmakers should use to update the Electronic Communications Privacy Act.

- Law enforcement should obtain a warrant supported by probable cause before it can compel a service provider to disclose the contents of users' private communications and documents stored online.

- The government should obtain a search warrant supported by probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.

- Before obtaining transactional data in real time about when and with whom an individual communicates using e-mail, instant messaging, the telephone, or any other communications technology, the government should demonstrate to a court that such data is relevant to an authorized criminal investigation.

- Before obtaining transactional data about multiple unidentified users when trying to track down a suspect, the government should first demonstrate to a court that the data is needed for its criminal investigation.

The first change was initially proposed by Sens. John Ashcroft (R-Mo.) and Patrick Leahy (D-Vt.) in 1998, the group noted, and is consistent with recent appellate decisions holding that e-mails and SMS text messages are protected by the Fourth Amendment.

"This principle applies the safeguards that the law has traditionally provided for the privacy of our phone calls or the physical files we store in our homes to private communications, documents[,] and other private user content stored in or transmitted through the Internet 'cloud'—private emails, instant messages, text messages, word processing documents and spreadsheets, Internet search queries and private posts made over social networks[,]" the group said.

The other updates address the growing availability of data from mobile devices, and seek to remedy current law enforcement access to private communications without judicial review.

The statute also provides, at 18 U.S.C. § 2703(c), that a governmental entity may require service providers to disclose "a record or other information pertaining to a subscriber" through the methods outlined above.

In addition, the section states that services shall disclose limited categories of subscriber information—name, address, telephone connection records, records of session times and durations, the length of service,

network addresses, and payment methods—in response to an administrative subpoena, or a grand jury or trial subpoena.

ECPA's distinction between communications in "electronic storage" and those held by "remote computing services" was drafted in an era of widespread offsite mainframe storage, before many businesses and individuals had onsite data storage capabilities.

In recent cases, courts have been asked to apply these standards to requests for a wide variety of data (see examples in table).

The results, including some decisions holding that the warrant requirement could hinge on technicalities like e-mail opening and synching, have spurred debate that the time has come to update the statute to address the way individuals use digital communications services today.

Two-Pronged Debate. "There are two levels to this debate," Susan Freiwald, a cyberlaw professor at the University of San Francisco School of Law, and frequent contributor of amicus briefs in ECPA cases, remarked in a recent BNA interview. "This is both a policy and a constitutional issue," she added.

The Sixth Circuit cited Freiwald's *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 135 (2008), co-written with Patricia L. Bellia, favorably in the *Warshak* decision.

"The Sixth Circuit has clearly established that the Stored Communications Act is unconstitutional to the extent that law enforcement can obtain stored e-mail, in which subscribers have a reasonable expectation of privacy, without a warrant," Freiwald said.

The case could provide added incentive for lawmakers to turn their attention to the statute this session. "*Warshak* is definitely a case that should push lawmakers to revisit ECPA and make sure the law is consistent with the Fourth Amendment," Marcia Hofmann, a senior staff attorney with the Electronic Frontier Foundation, told BNA.

EFF is also part of the Digital Due Process coalition, and published a detailed comparison Jan. 20 of 13 social media sites' policies for granting law enforcement access to information about their subscribers.

From a policy standpoint, courts, lobbyists, and lawmakers have questioned the utility of the statute's distinctions between remote and other services.

Online businesses have complained that the statute's lesser protections for remotely stored communications are now counter-intuitive in an environment where most communications—and a growing body of documents—are stored in cloud computing services (15 ECLR 1459, 9/29/10). That unnecessary distinction could impede innovation, and should change, they added.

Charles H. Kennedy, a partner at Wilkinson Barker Knauer LLP and professor at the Catholic University of America's Columbus School of Law, pointed to a recent Seventh Circuit decision as just one example in which courts have identified a gap between statutory privacy protections for electronic communications and current market practices.

In *United States v. Szymuszkiewicz*, No. 10-1347 (7th Cir. Sept. 9, 2010) (15 ECLR 1435, 9/22/10), the court discussed at length its conclusion that the "interception" of e-mail, for purposes of the Wiretap Act, 18 U.S.C. § 2511(1)(a), is not comparable to "intercep-

tions" of other types of communications because it happens in pieces, a process known as "packet switching." The court added that a party might simultaneously violate the ECPA and the Wiretap Act when intercepting e-mail.

Warshak: SCA Is Unconstitutional. The *Warshak* decision demonstrates a tension between the Fourth Amendment and the SCA.

The court held that even if the SCA permitted an online service to disclose the contents of stored e-mail in response to a subpoena or court order, law enforcement could not obtain it through that method because it would violate the Fourth Amendment.

The court held that e-mail subscribers enjoy a reasonable expectation of privacy in the contents of their e-mail messages. However, that expectation could give way when an ISP's terms of service "express[] an intention to 'audit, inspect, and monitor' its subscriber's emails[.]" In those situations, the contract could be enough to destroy any expectation of privacy.

As a result, it is unclear exactly what an ISP would have to do to vitiate a subscriber's reasonable expectation of privacy in stored e-mails, Freiwald remarked. "But this ruling is important because it makes clear that ISPs' access to messages is not a waiver of users' privacy interests," she added.

In *City of Ontario, Calif. v. Quon*, No. 08-1332 (U.S. June 17, 2010), the Supreme Court declined to address the Fourth Amendment's application to electronic communications, in the context of text messages on a company-provided device.

"The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear[.]" Justice Anthony M. Kennedy wrote for the majority.

Other courts have identified Fourth Amendment problems in ECPA cases involving location information, as well.

In *In re Application of United States of America for Order Directing Provider of Electronic Communication Service to Disclose Records to Government*, No. 08-4277 (3d Cir. Sept. 7, 2010), the court concluded that a judge may, at his or her discretion, require the government to satisfy the Fourth Amendment's probable cause standard to obtain cell tower location information, even if it might otherwise be available under the SCA, at 18 U.S.C. § 2703(d), via a court order.

"The [Magistrate Judge] regarded location information as "extraordinarily personal and potentially sensitive[.]" the court noted. The court declined to decide whether cellular subscribers have a reasonable expectation of privacy in that data, and limited its ruling to an evaluation of the reasonableness of the magistrate's holding that a warrant was required.

Looking to the text of the SCA, the court focused on the phrase "may be issued." According to the court, the word "may" meant that, in some cases, courts can require the government to make a heightened showing. However, the court said that discretion should rarely be exercised.

The court took no position on the Fourth Amendment's protection of GPS data—which the government said is more precise but did not seek in the case.

That case is one of many in which courts are struggling to balance privacy interests in location data with the ECPA's text, Freiwald remarked.

What Are Communications Services Saying?

Andrew Noyes, a Facebook spokesperson, told BNA that the company is part of the Digital Due Process coalition, which supports substantive ECPA updates including the adoption of a warrant standard for all nonpublic communications.

“More broadly on information requests, I can tell you that we review each request individually for legal sufficiency before responding,” Noyes remarked. “We have a dedicated team of CIPP certified professionals responsible for managing requests (and that team is supervised by two former federal cybercrime prosecutors who are experts in the law in this area).”

He added that the company takes a strict approach to the disclosure of the contents of subscriber communications. “[W]e never turn over ‘content’ records in response to U.S. legal process unless that process is a search warrant reviewed by a judge.

Amy Storey, director of external affairs for CTIA—The Wireless Association, said the group has not taken a position on the recent rulings about location information.

“However, if Congress takes up these issues, wireless carriers would want to insure that their good faith reliance on [the following categories of information] continues to be a complete defense against any civil or criminal action”:

- a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;
- a request of an investigative or law enforcement officer under section 2518 (7) of this title; or
- a good faith determination that section 2511 (3) or 2511 (2)(i) of this title permitted the conduct complained of.

Hofmann agreed. “These cases highlight the challenge of applying an outdated law, and raise questions about whether the government’s use of it in certain circumstances is constitutional,” she said.

E-Mail Interception: Not Like Catching a Football. The *Szymuszkiewicz* case “calls into question the fundamental ECPA/SCA distinction between interceptions of communications and their acquisition from storage,” Kennedy noted.

In the case, the court explored the SCA’s potential application to an individual who had been convicted under the Wiretap Act for covertly setting up his supervisor’s e-mail to be simultaneously forwarded to his own account. The court rejected the defendant’s assertion

that he should have been prosecuted under the SCA instead, and explored the workings of modern e-mail at length. Along the way, the court questioned whether the distinction between communications in transit and storage is as clear-cut as it was when the Wiretap Act was enacted in 1968.

The court observed:

[The defendant]’s understanding of ‘interception’ as ‘catching a thing in flight’ is sensible enough for football, but for email there is no single ‘thing’ that flies straight from sender to recipient. When sender and recipient are connected by a single circuit, and the spy puts a ‘tap’ in between, the football analogy makes some sense For email, however, there are no dedicated circuits. There are only packets, segments of a message that take different routes at different times.

The court ultimately concluded that the defendant’s actions might have generated liability under both the ECPA and the Wiretap Act, and affirmed his conviction.

“In the age of ubiquitous packet switching, it’s anachronistic to have to draw strained lines between interceptions and acquisitions from storage, and to hold governmental data requests to different standards according to the results of that artificial exercise,” Kennedy said.

Requiring a single, probable cause standard for all acquisitions of the contents of non-public communications would resolve this problem, he remarked.

Too Early to Examine Social Networks? At least one court has attempted to apply the ECPA to messages transmitted via social networks. In *Crispin v. Audigier*, No. 09-9509 (C.D. Cal. May 26, 2010)(15 ECLR 907, 6/9/10), the court concluded communications transmitted via social networks might be protected by the SCA’s prohibition on ISP disclosures of electronic communications.

The court analogized those messages to e-mails, and concluded that their protection depended on whether they had been opened. The court partially granted a social network user’s motion to quash a civil subpoena, and analogized unopened user-to-user messages to e-mails, which many courts have concluded are in “temporary storage” and protected by the ECS warrant standard.

The court reserved judgment on other types of communications and wall posts, remarking that the user’s expectation of privacy could depend on how that information had been shared with other users or the internet at large.

Freiwald told BNA that “social networks are really new territory,” so the status of messages inside them is by no means clear under the ECPA. For purposes of the Fourth Amendment, users’ privacy expectations should hinge on the availability of those messages to the public, she added.

By AMY E. BIVINS

Full text of the Electronic Frontier Foundation’s Social Media and Law Enforcement: Who Gets What Data and When? at <https://www.eff.org/deeplinks/2011/01/social-media-and-law-enforcement-who-gets-what>.

Recent ECPA Litigation Highlights Uncertain Digital Privacy Protections

Courts are increasingly faced with the challenge of juggling privacy protections for digital communications in the Electronic Communications Privacy Act with the Fourth Amendment's protection for communications in which subscribers have a reasonable expectation of privacy. As demonstrated below, the statute's distinctions between electronic communications services and remote computing services and divergent privacy protections for those messages are being tested—sometimes inconsistently—in cases that have stirred debate about the 1986 statute's relevance to today's online market in which consumers increasingly rely on remote services to process their communications.

Electronic Communications Privacy Act Litigation Update

Case	Holding
Recent Examples of ECPA's Tension With Fourth Amendment	
<i>In the Matter of an Application of the USA for an Order Authorizing the Release of Historical Cell-Site Information</i> , No. 10–897 (E.D.N.Y. Dec. 23, 2010)(16 ECLR 60, 1/12/11).	Holding that the release of cell phone call location data arguably authorized under SCA, but concluding that access via any mechanism less than a warrant—including a court order—would violate the Fourth Amendment.
<i>United States v. Warshak</i> , No. 08–3997 (6th Cir. Dec. 14, 2010)(15 ECLR 1925, 12/22/10).	Holding that portions of the SCA that permit law enforcement to obtain the contents of e-mail messages via a subpoena and court order obtained on less than the constitutionally required showing of “probable cause” violate the Fourth Amendment. Such access must comply with constitutional warrant requirement, although certain factors—including user agreements—might destroy legitimate expectations of privacy in e-mail.
<i>In re Application of the United States of America for Historical Cell Site Data</i> , No. 10–981 (S.D. Tex. Oct. 29, 2010).	Holding that a law enforcement request for cell-site data implicated Fourth Amendment privacy interests. The court recognized that such requests had been granted in the past, but said that recent changes in cell phone technology that enhance tracking capabilities require the government to obtain a warrant.
<i>In re Application of United States of America for Order Directing Provider of Electronic Communication Service to Disclose Records to Government</i> , No. 08-4277 (3d Cir. Sept. 7, 2010).	Holding that a judge may require the government to satisfy the Fourth Amendment's probable cause standard to obtain cell tower location information, even if it might otherwise be available under the SCA via a court order.
<i>City of Ontario, Calif. v. Quon</i> , No. 08–1332 (U.S. June 17, 2010)(15 ECLR 983, 6/23/10).	Holding that a police department search of an employee's text messages was “reasonable.” Did not address whether employee had a reasonable expectation of privacy in messages. The court denied certiorari with respect to the Ninth Circuit's holding that a text message service is an “electronic communications service” for purposes of the SCA, that the department's consent to disclose the messages was inadequate, and that the provider violated the SCA.
<i>Rehberg v. Paulk</i> , 598 F.3d 1268 (11th Cir. 2010)(15 ECLR 543, 4/7/10).	Holding that a defendant lacked a legitimate expectation of privacy in the contents of his e-mail, at least after he sent the messages and they were delivered to a third party. The court did not consider the SCA.
<i>United States v. Beckett</i> , No. 09-10579 (11th Cir. March 9, 2010)(unpublished)(15 ECLR 473, 3/24/10).	Rejecting a criminal defendant's motion to suppress evidence under the ECPA based on ISPs allegedly unlawful disclosure of internet account data to law enforcement upon request. ECPA has no suppression remedy. Fourth Amendment provided no protection because information was shared with ISPs, so defendant lacked legitimate expectation of privacy.
What Services Qualify for Privacy Protection?	
<i>Thompson v. Ross</i> , No. 10–479 (W.D. Pa. Sept. 30, 2010)(15 ECLR 1538, 10/13/10).	Holding that an individual's personal laptop, taken by co-workers, was not an electronic communications service or facility under the SCA.
<i>Jennings v. Jennings</i> , No. 4711 (S.C. Ct. App. July 14, 2010)(15 ECLR 1257, 8/11/10).	Holding that Yahoo! acted as an “electronic communications service” with respect to stored webmail because the account was active, the plaintiff could send and receive e-mails, and one purpose of using an internet-based e-mail system is to provide “backup” storage.
<i>Devine v. Kapasi</i> , No. 09–6164 (E.D. Ill. June 7, 2010)(15 ECLR 988, 6/23/10).	Holding that a private server was an electronic communications service “facility,” even though the corporate owner did not provide communications services to the public.

Electronic Communications Privacy Act Litigation Update – Continued

Case	Holding
<i>Crispin v. Audigier Inc.</i> , No. 09-9509 (C.D. Cal. May 26, 2010)(15 ECLR 907, 6/9/10).	Holding that social networks can act as both “electronic communications services” and “remote computing services” when processing subscriber communications. Wall posts and other comments might also qualify for SCA protection, depending on privacy settings.
Meaning of SCA’s ‘Backup Protection’	
<i>Jennings v. Jennings</i> , No. 4711 (S.C. Ct. App. July 14, 2010)(15 ECLR 1257, 8/11/10).	Rejecting argument that messages were not stored for “backup protection” because they were stored only in Yahoo webmail account.
<i>KLA-Tencor Corp. v. Murphy</i> , No. 09-1922 (N.D. Cal. May 11, 2010)(15 ECLR 803, 5/19/10).	Holding that e-mails stored on a corporate server cannot be “backups,” and the server is thus not an electronic communications service, because they were synched with an employee’s account and deleted simultaneously.
Effect of Message Opening Under SCA	
<i>Jennings v. Jennings</i> , No. 4711 (S.C. Ct. App. July 14, 2010)(15 ECLR 1257, 8/11/10).	Holding that the opening of e-mails does not affect their SCA protection.
<i>Crispin v. Audigier Inc.</i> , No. 09-9509 (C.D. Cal. May 26, 2010)(15 ECLR 907, 6/9/10).	Holding that social network messages’ protection under the SCA changes at opening: Unopened messages are protected by the electronic communications service warrant requirement; opened messages under the more-lenient “remote computing service” standard.
ECPA, SCA Damages	
<i>Pure Power Boot Camp Inc. v. Warrior Fitness Boot Camp LLC</i> , No. 08-4810 (S.D.N.Y. Dec. 22, 2010)(16 ECLR 12, 1/5/11).	Holding that SCA violations should be counted, for purposes of statutory damages, per account accessed—not per message or day of access. Court disagreed with <i>Van Alstyne v. Elec. Scriptorium Ltd.</i> , 560 F.3d 199 (4th Cir. 2009)(14 ECLR 403, 3/25/09)’s holding that proof of actual damages is required to obtain statutory damages under the SCA.
Effect of Terms of Service on Communications Privacy Claims	
<i>Mortensen v. Bresnan Communication LLC</i> , No. 10-13 (D. Mont. Dec. 13, 2010)(16 ECLR 10, 1/5/11).	Holding that an ISP’s online privacy notice and subscriber agreement defeated subscribers’ Wiretap Act claim involving tracking for advertising.