# Key Issues in Electronic Communications Privacy Act (ECPA) Litigation

ERIC BOSSET AND HANNAH LEPOW, COVINGTON & BURLING LLP, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

Search the Resource ID numbers in blue on Westlaw for more.

A Practice Note providing an overview of the Electronic Communications Privacy Act (ECPA) and examining key issues that counsel should consider when litigating civil ECPA actions.

Congress passed the Electronic Communications Privacy Act (ECPA) in 1986 to add electronic communications into the existing scheme of privacy protections for communications and to regulate technology companies that store electronic communications.

The ECPA protects the privacy of electronic communications through:

- Title I: Wiretap Act, which prohibits the interception of electronic communications during trans and the use of intercepted communications (18 U.S.C. § 2510 to § 2523) (see Wiretap Act)
- Title II: Stored Communications Act (SCA), which protects electronic communications in storage (as opposed to communications in transit) (18 U.S.C. § 2701 to § 2713) (see Stored Communication Act).
- Title III: Pen Register/Trap and Trace Devices, which restricts the use of:
  - pen registers, which are devices that record the numbers dialed for outgoing calls made from the target phone; and
  - trap and trace devices, which capture the numbers of calls made to a target phone.
- (18 U.S.C. § 3121 to § 3127.)

This Note focuses on civil Wiretap Act and SCA litigation. It does not address provisions specific to the government or private entities disclosing content to the government (including law enforcement). While many states have enacted statutes based on the ECPA, this Note also only focuses on federal law.

## WIRETAP ACT

The Wiretap Act provides a private right of action against anyone intentionally intercepting, attempting to intercept, or procuring any person to intercept any wire, oral, or electronic communication (18 U.S.C. § 2511(1)(a)). To state a claim under the Wiretap Act, the plaintiff must allege:

- The defendant's intent (see Intent).
- The nature of the defendant's intended conduct (see Intercept).
- What the defendant sought to intercept (see Content Under the Wiretap Act).
- The nature of the targeted communications (see Electronic Communication and Service Providers).
- The tools used (or intended to be used) to intercept the protected content (see Device).
- Whether any statutory exceptions apply (see Exceptions to the Federal Wiretap Act and Consent Under the Wiretap Act and SCA).

This Note focuses on a primary cause of action under the Wiretap Act for interceptions of electronic communications. However, the statute also imposes liability on anyone intentionally using or disclosing the contents of any wire, oral, or electronic communication if the user knows or has reason to know that the information was obtained in violation of the Wiretap Act. This liability may:

- Apply even if the user or distributor is not the interceptor.
- Serve as a second count against an interceptor later using or distributing the intercepted information.

(18 U.S.C. §§ 2511(1)(c), (d).)

### INTENT

To state a Wiretap Act claim, a plaintiff must allege that the defendant acted with intent. ECPA's legislative history states that "intentional" means more than voluntarily engaging in conduct that caused a result. To be liable under the Wiretap Act, a defendant must instead have purposely or consciously wanted to cause a result. (S. REP. NO. 99-541 (1986).)

Multiple courts have similarly noted that an act is not intentional under the Wiretap Act if it is the product of inadvertence or mistake (see, for example, *In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir. 2003); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 742-43 (4th Cir. 1994); *United States v. Townsend*, 987 F.2d 927, 930 (2d Cir. 1993)).

© 2020 Thomson Reuters. All rights reserved.

Some courts suggest that a defendant's motive is not relevant when assessing whether the defendant acted intentionally (see, for example, *Abraham v. Cty. of Greenville,* 237 F.3d 386, 391-92 (4th Cir. 2001) (jury instruction that "defendant's motive is not relevant" to determine intent under the Wiretap Act was proper)). However, a court is more likely to find the requisite intent when the party's conduct (interception) is in its self-interest (*see Pharmatrak*, 329 F.3d at 23).

### INTERCEPT

The Wiretap Act requires a plaintiff bringing a civil action to establish that the defendant intentionally intercepted, attempted to intercept, or procured any person to intercept any wire, oral, or electronic communication (18 U.S.C. § 2511(1)(a)). The statute defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication" by using any:

- Electronic device.
- Mechanical device.
- Other device.

(18 U.S.C. § 2510(4).)

Courts have concluded that Wiretap Act liability attaches only if the interception occurs contemporaneously with the communication's transmission (see *Boudreau v. Lussier*, 901 F.3d 65, 77 (1st Cir. 2018) (citing *Luis v. Zang*, 833 F.3d 619, 628 (6th Cir. 2016) (collecting cases))). Once the transmission of an electronic communication ends, the communication is considered to be in electronic storage and is subject to the SCA instead of the Wiretap Act.

Courts have held that an individual or entity may contemporaneously intercept a communication by:

- Acquiring communications while they are being written (see *Zang*, 833 F.3d at 624, 630 (a web-based program that recorded "all PC activity, including emails, IMs, websites visited, web searches, Facebook/Myspace activity, and anything typed in real time" intercepted communications "in flight"); *Rich v. Rich*, 2011 WL 3672059, at *5 (Mass. Super. July 8, 2011) (using a key logger program to acquire a message as it is composed constitutes contemporaneous interception)).
- Acquiring it on either the device side or the server side (see *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010) (the interception was "contemporaneous" regardless of whether the server or the recipient's device made the copies because the employee and the supervisor received the emails within the same second)).
- Obtaining the communication at the same time as the intended recipient (see *In re Pharmatrak*, 329 F.3d at 22 (a user's communications with a pharmaceutical company through an online form was simultaneously received by a marketing firm)).

(But see *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003) (a hacker did not obtain electronic communication from contemporaneous acquisition while in flight because the hacker used a Trojan Horse virus to download files stored on Steiger's hard drive); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879 (9th Cir. 2002) (unauthorized viewing of a private website did not constitute an interception of electronic communications because the user viewed stored electronic communications).)

The contemporaneity requirement preexisted the widespread usage of the internet and cases involving purported interceptions of online communications. Some courts question its continued relevance given the difficulty of determining whether an online communication is in transit or at rest (see *In re Pharmatrak*, 329 F.3d. at 21 (agreeing with the Ninth and Eleventh Circuits' concern about the application of a pre-internet statute to online communications); *Steiger*, 318 F.3d at 1047 (noting that the ECPA is ill-suited to address modern forms of communication and that courts struggle "to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying result") (quoting *Konop*, 302 F.3d at 874); *United States v. Councilman*, 245 F. Supp. 2d 319, 321 (D. Mass. 2003) ("Traveling the internet, electronic communications are often ... both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox.")).

Explaining the nature of the transmission at issue to a court may require detailed affidavits and even expert testimony.

### CONTENT UNDER THE WIRETAP ACT

A plaintiff may only bring a Wiretap Act claim for the interception of content (18 U.S.C. § 2510(4)). The Wiretap Act defines "content" as any information containing the "substance, purport, or meaning" of the communication (18 U.S.C. § 2510(8)). Courts have found that Congress intended contents under the Wiretap Act (and SCA) to mean a person's intended message to another, such as:

- The "essential part" of the communication.
- The "meaning conveyed."
- What a person intends to convey.

(*In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1034 (N.D. Cal. 2014) (finding that the plaintiffs' allegations that Yahoo shared the body of emails with third parties sufficient to survive the defendant's motion to dismiss).)

The line between content and non-content information depends entirely on the circumstances. For example, addresses, phone numbers, and URLs may be non-content information when performing dialing, routing, addressing, or signaling information functions. However, if an address, phone number, or URL is instead part of the substantive information conveyed to the recipient, it may be content (*In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 137 (3d Cir. 2015)).

Examples of non-content information when it is not part of a substantive communication include:

- General information about a telephone call, such as the number called, length, and time of the call (see, for example, *United States v. Reed*, 575 F.3d 900, 917 (9th Cir. 2009); *Gilday v. Dubois*, 124 F.3d 277, 296 n. 27 (1st Cir. 1997)).
- Usernames as indicators of the identity of a user (*In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1083 (N.D. Cal. 2015)).
- Logistical information transmitted to the third party, such as:
  - the individual's Facebook ID; and
  - the internet address of the webpage that contained the referral link.
- (See *In re Zynga Privacy Litig.*, 750 F.3d at 1106.)


© 2020 Thomson Reuters. All rights reserved.

A plaintiff must plead and establish with specificity why the communication at issue is content under the Wiretap Act.

## ELECTRONIC COMMUNICATION SERVICE PROVIDERS

### Electronic Communications

The Wiretap Act applies to the intentional interception of the contents of three types of communications:

- Oral communication (for example, an in-person conversation).
- Wire communication (for example, a traditional telephone communication).
- Electronic communications, which include any of the following transmitted by wire, radio, electromagnetic, photoelectronic, or photooptical system and that affect interstate or foreign commerce:
  - transfer of signs;
  - signals;
  - writing;
  - images;
  - sounds;
  - data; or
  - intelligence.
- (18 U.S.C. §§ 2510(12).)

Courts have held that electronic communications include:

- Emails (*Hately v. Watts*, 917 F.3d 770, 784-85 (4th Cir. 2019) (collecting cases)).
- URLs and text messages (see, for example, *In re Carrier IQ, Inc.*, 78 F. Supp. 3d at 1083; *United States v. Jones,* 451 F. Supp. 2d 71, 75 (D.D.C. 2006), aff'd in part, rev'd in part sub nom. *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010)).
- Satellite television transmissions (see *DIRECTV, Inc. v. Pepe*, 431 F.3d 162, 166 (3d Cir. 2005)).
- Pay-per-view television signals (see *United States. v. Herring*, 993 F.2d 784 (11th Cir. 1993, cert denied, 510 U.S. 933)).

### Electronic Communication Service Providers

The ECPA defines an electronic communication service (ECS) as any service that enables users to send or receive wire or electronic communications (18 U.S.C. § 2510(15)). The Wiretap Act uses the term electronic communications service provider (ECSP) when describing certain exceptions to the law (see Exceptions to the Wiretap Act).

An ECSP may include those providing:

- Email services.
- Phone services.
- Text messaging services.
- Social media platforms and other forms of internet-based messaging.

(See *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 792 (5th Cir. 2012) (explaining courts have interpreted ECSP provisions to apply to providers of communication services, such as telephone companies, e-mail service providers, and bulletin board services); *In re United States for PRTT Order for One Whatsapp Chief Account for Investigation of Violation of 21 U.S.C. § 841*, 2018 WL 1358812, at *4 (D.D.C. Mar. 2, 2018) ("WhatsApp is providing an [ECS]"); see also S. REP. NO. 99-541, at 14 (reprinted in 1986 U.S.C.C.A.N. 3555, 3568) ("[T]elephone companies and electronic mail companies are providers of electronic communications services."))

For a discussion of ECSPs under the SCA, see Electronic Communication Service Provider.

## DEVICE

The Wiretap Act defines an "electronic, mechanical, or other device" as any device or apparatus that can be used to intercept a wire, oral, or electronic communication. However, the Wiretap Act establishes two exceptions and excludes from the definition of device:

- A telephone or telegraph instrument, equipment, or facility or any component of these, used in a manner that satisfies the ordinary course of business exception (see Ordinary Course of Business Exception).
- A hearing aid or similar device used to elevate subnormal hearing to normal hearing.

(18 U.S.C. § 2510(5).)

## EXCEPTIONS TO THE WIRETAP ACT

The Wiretap Act permits individuals or entities to intercept and use electronic communications when:

- The interception satisfies either:
  - the ordinary course of business exception (see Ordinary Course of Business Exception); or
  - the normal course of employment exception (see Normal Course of Employment Exception).
  - A wire or ECSP gives information, facilities, or technical assistance to an authorized person to intercept the communication, as defined in Section 101 of the Foreign Intelligence Surveillance Act of 1978 (18 U.S.C. § 2511(2)(a)(ii)).
- One of the parties to the communication gives prior consent to an interception that is not to commit a criminal or tortious act (18 U.S.C. § 2511(2)(c), (d); see Consent Under the Wiretap Act and SCA).
- The communication intercepted was made using an electronic communication system that makes electronic communications readily accessible to the public (18 U.S.C. § 2511(2)(g)(i)).
- Responding to an order from a foreign government that has entered into a bilateral agreement under the Clarifying Lawful Overseas Use of Data (CLOUD") Act (18 U.S.C. § 2511(2)(j)).
- When an ESCP divulges the contents of a communication:
  - in compliance with 18 U.S.C. § 2511(2)(a) or 2517;
  - with the consent of the originator, addressee, or intended recipient of the communication;
  - to a person employed or authorized (or the facilities of which are used) to forward the communication to its destination; or
  - to a law enforcement agency, if the service provider inadvertently obtained the communication and it appears to pertain to the commission of a crime.
- (18 U.S.C. § 2511(3)(b); see Electronic Communication and Service Providers.)

© 2020 Thomson Reuters. All rights reserved.

The Wiretap Act also permits individuals and entities to disclose (but not intercept) a communication when they have a good faith belief that they are authorized to do so (18 U.S.C. § 2520(d)(3)).

### Ordinary Course of Business Exception

The Wiretap Act exempts from liability the interception of communications of a telephone or telegraph instrument, equipment, or facility (or any component of these) that:

- A wire or ECSP furnished to a subscriber (or user) in the ordinary course of its business and that the subscriber (or user) used in the ordinary course of its business (18 U.S.C. § 2510(5)(a)(i)).
- A subscriber (or user):
  - furnished to connect to a wire or ECS; and
  - used in the ordinary course of its business.
- (18 U.S.C. § 2510(5)(a)(i).)
- An ECSP used in the ordinary course of its business (18 U.S.C. § 2510(5)(a)(ii)).
- An investigative or law enforcement officer used in the ordinary course of the officer's duties (18 U.S.C. § 2510(5)(a)(ii)).

The Wiretap Act therefore has two ordinary course of business exceptions for non-law enforcement purposes:

- For users or subscribers of an ECS. Cases litigated under this provision often involve employer monitoring of employee telephonic conversations (see, for example, *United States v. Murdock*, 63 F.3d 1391, 1396 (6th Cir. 1995)).
- For ECSPs. Cases litigated under this provision often involve email or internet service providers that collect user information for marketing and advertising purposes (see, for example, *In re Google Inc. Gmail Litig.*, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013)).

Most courts narrowly construe the ordinary course of business exception and require a nexus between the need to engage in the alleged interception and the user's, subscriber's, or ECSP's ability to provide the underlying service or good. Under this construction, the exception applies only where the interception either:

- Facilitates the transmission of the communication at issue.
- Is incidental to the communication's transmission.

(See, for example, *In re Google Inc. Gmail Litig*, 2013 WL 5423918, at *8, *11 (finding the plaintiffs plausibly alleged no nexus between Google's providing a Gmail account and the alleged interception and scanning of email for advertising purposes).)

However, other courts read the ordinary course of business exception broader as including all "legitimate business purposes," such as advertising (*In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *11 (N.D. Cal. Dec. 3, 2013); *see also Berry*, 146 F.3d at 1009 (noting that the activity in question must "be justified by a valid business purpose" or "'perhaps, at least ... be shown to be undertaken normally'")).

For example, in *Arias v. Mutual Central Alarm Service, Inc*, the Second Circuit found that legitimate business reasons supported the continual recording of all incoming and outgoing telephone calls at an alarm company to ensure that:

- The alarm company's personnel did not divulge sensitive customer information.
- Events are reported quickly to emergency services.
- Customer claims regarding events are verifiable.
- The police and other authorities may rely on the records during investigations.

(202 F.3d 553, 559 (2d Cir. 2000).)

Courts determining whether an interception falls within the ordinary course of business exception may also consider whether the inception violates the defendant's internal policies (see, for example, *In re Google Inc.*, 2013 WL 5423918, at *12; *Berry v. Funk*, 146 F.3d 1003, 1010 (D.C. Cir. 1998)).

### Normal Course of Employment Exception

The Wiretap Act generally permits a switchboard operator or an officer, employee, or agent of a provider of wire or ECS to intercept, disclose, or use wire or electronic communications "in the normal course" of their employment while engaged in activity that is a "necessary incident" to either:

- Provide the service.
- Protect the rights or property of the provider, subject to exceptions.

(18 U.S.C. § 2511(2)(a)(i).)

However, a provider serving the public **may not** observe or randomly monitor communications except as part of a mechanical or service quality control check (18 U.S.C. § 2511(2)(a)(i).)

Courts have noted that Congress did not intend to allow wire or ECSPs "unlimited leeway to engage in any interception that would benefit their business models" (*In re Google Inc.*, 2013 WL 5423918, at *9).

Few cases discuss the meaning of a "necessary incident" to the rendition of service. However, US Department of Justice guidance (DOJ Guidance) suggests that the exception applies when an interception is unavoidable. DOJ Guidance explains that this exception "generally arose when analog phone lines were in use" and:

- A switchboard operator briefly overheard conversations when connecting calls.
- Repair personnel overheard snippets of conversations during repairs.

Recent case law applying this exception is scarce and decisions vary about whether the exception exempts only individuals (see *In re Google Inc.*, 2013 WL 6248499, at *10 n.86; but see *Holomaxx Techs. Corp. v. Microsoft Corp.*, 2011 WL 3740813, at *3 (N.D. Cal. Aug. 23, 2011) (exception applies to "artificial persons" such as corporations)).

## DAMAGES UNDER THE WIRETAP ACT

Persons the communications of which were intercepted, disclosed, or intentionally used in violation of the Wiretap Act may bring a private cause of action against any person or entity other than the US (18 U.S.C § 2520(a)). In civil litigation, plaintiffs may:

- Seek damages and injunctive relief. Damages may be the greater of either:
  - the sum of actual damages suffered by the plaintiff and profits made by the violator as a result of the violation; or


© 2020 Thomson Reuters. All rights reserved.

  - statutory damages of whichever is the greater of $100 per day for each day of violation or $10,000.
- (18 U.S.C § 2520(c)(2).)
- Recover attorneys' fees and costs.
- (18 U.S.C § 2520(b)(3).)

## STORED COMMUNICATIONS ACT

The SCA focuses on communications when they are at rest in storage. It provides a private right of action when:

- An ECSP either:
  - knowingly divulges the contents of a communication that the ECS is electronically storing;
  - intentionally accesses, without authorization, a facility through which an ECS is being provided and "obtains, alters, or prevents authorized access to a wire or electronic communication" while it is being electronically stored in the facility; or
  - intentionally exceeds its authorization to access a facility through which an ECS is being provided and "obtains, alters, or prevents authorized access to a wire or electronic communication" while it is being electronically stored in the facility.
- (18 U.S.C. §§ 2701(a) and 2702(a); see Electronic Communication Service Provider and Content Under the SCA.)
- A remote computing service provider (RCSP):
  - carries or maintains a communication pertaining to a subscriber's or customer's electronic transmission;
  - acts solely to provide storage or computer processing services to the subscriber or customer;
  - is not authorized to access the communication's contents other than for storage or computer processing; and
  - knowingly divulges the contents of the communication.
- (18 U.S.C. § 2702(a)(2); see Remote Computing Service Provider and Content Under the SCA.)

Whether an entity acts as an RCSP or an ECSP (or neither) is fact-specific and depends, in part, on the information disclosed (see *In re United States*, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) ("[M]ost ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or regarding a particular piece of electronic communication at a particular time), rather than to define the service provider itself.")).

The SCA does not preclude an entity from simultaneously functioning as both an ECSP and an RCSP (see *Hately*, 917 F.3d at 788).

### ELECTRONIC COMMUNICATION SERVICE PROVIDER

The SCA adopts the Wiretap Act's definition of electronic communication and electronic communication service (see 18 U.S.C. 2711(1) and Electronic Communication Service Providers). ECSP include those providing:

- Email services.
- Phone services.
- Text messaging services.
- Social media platforms and other forms of internet-based messaging.

(See *City of Laredo, Tex.*, 702 F.3d at 792 (explaining courts have interpreted ECS provisions to apply to providers of communication services, such as telephone companies, e-mail service providers, and bulletin board services); *In re United States for PRTT Order for One Whatsapp Chief Account for Investigation of Violation of 21 U.S.C. § 841*, 2018 WL 1358812, at *4 ("WhatsApp is providing an [ECS]"); see also S. REP. NO. 99-541, at 14 (reprinted in 1986 U.S.C.C.A.N. 3555, 3568) ("[T]elephone companies and electronic mail companies are providers of electronic communications services.").)

#### Electronic Storage Requirement

The SCA only allows for liability against an ECSP when it is engaged in "electronic storage," which means it either:

- Temporarily and intermediately stores a wire or electronic communication incidental to its electronic transmission.
- Stores an electronic communication for backup protection.

(18 U.S.C. § 2510(17).)

Courts have held that temporary, immediate storage may include e-mail messages stored on a server pending delivery to the recipient (see, for example, *United States v. Councilman*, 418 F.3d 67, 80 (1st Cir. 2005); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001)). However, at least one court has held that a recipient's decision not to delete an email after receiving and opening it suggests that the recipient does not intend to keep the message temporarily and that previously received, accessed, and retained (undeleted) emails are not being electronically stored (*Hately*, 917 F.3d at 785).

The ECPA does not define or provide guidance on electronic storage for backup protection (*Fraser*, 352 F.3d at 114 (noting that the statute or in the legislative history does not define "backup protection")). Courts interpreting this provision suggest that:

- Prior access to the communication is irrelevant (see *Hately*, 917 F.3d at 786; *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004)).
- Backup purposes means providing a second copy of a communication in case the user needs to download it again (for example, due to accidental erasure from the user's own computer) (see *Theofel*, 359 F.3d at 1075; *Hately*, 917 F.3d at 793 ("[T]he purpose of the web-based email service in providing storage for the message ... is to afford the user a place to store messages the user does not want destroyed.")).

However, courts have rejected arguments that electronic communications were for backup purposes if the communication does not exist in two places (see, for example, *Theofel*, 359 F.3d at 1076 ("An ISP that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages"); *United States v. Weaver*, 636 F. Supp. 2d 769, 772 (rejecting the argument that Microsoft was an ECSP because it maintained the message "solely for the purpose of providing storage or computer processing services to such subscriber or customer" and not for backup purposes); *Flagg v. City of Detroit*, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (archive of text messages that SkyTel continued to maintain on the city's behalf constituted the only available record of these communications and was not a "backup" copy of communications stored elsewhere)).

© 2020 Thomson Reuters. All rights reserved.

### REMOTE COMPUTING SERVICE PROVIDER

The ECPA defines an RCSP as providing "computer storage or processing services by means of an electronic communications system" to the public (18 U.S.C. § 2711(2); see Electronic Communication and Service Providers; *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 902 (9th Cir. 2008), rev'd and remanded sub nom. *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010) (referring to the RCSP as providing processing or data storage by an offsite third party or a "virtual filing cabinet")).

An electronic communications system means any:

- Wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire or electronic communications.
- Computer facilities or related electronic equipment for the electronic storage of wire or electronic communications.

(18 U.S.C. § 2510(14).)

Examples of RSCPs include:

- Physicians and hospitals maintaining medical files in offsite data banks.
- Businesses transmitting their records to remote computers to obtain sophisticated data processing services.

(S. REP. NO. 99-541, at 2-3 (1986); see also *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008) (the court concluded that YouTube was an RCSP because it provided storage services for the user on a web page).)

Cloud-based storage and computing typically qualify as RCSPs. However, a business that stores its own business records is not an RCSP (see for example, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1023 (N.D. Cal. 2012) (LinkedIn did not act as a "remote computing service" regarding the disclosed information because it was not processing or storing data by an offsite third party); *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 310 (E.D.N.Y. 2005) (holding that JetBlue was not an RCSP because it did not provide "computer processing services or computer storage to the public")).

ECSPs may become RCSPs after an electronic message has been read and stored. For instance:

- MySpace has been deemed:
  - An ECSP regarding messages that have not yet been opened; and
  - An RCSP regarding messages that have been opened and retained.
- (*Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010).)
- Twitter has been deemed:
  - an ECSP regarding its direct messaging services; and
  - an RCSP to the extent it retains direct messages that have been opened.
- (*Shenwick v. Twitter, Inc.*, 2018 WL 833085, at *2 (N.D. Cal. Feb. 7, 2018).)

### CONTENT UNDER THE SCA

An ESCP and RSCP face no liability under the SCA for disclosing non-content information (18 U.S.C. § 2701(a)). The SCA incorporates the Wiretap Act's definition of "contents" (18 U.S.C. § 2711(1); see Content Under the Wiretap Act).

Examples of non-content information under the SCA include:

- Location data (see *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 305-06 (3d Cir. 2010) (holding that cell phone users' location data is not content information under the SCA)).
- Device data "generated automatically, rather than through the intent of the user," is not content under the SCA (or Wiretap Act) (see *In re iPhone Application Litig.*, 2012 WL 2126351, at *14, *30 (N.D. Cal. June 12, 2012)).

### EXEMPTIONS UNDER THE STORED COMMUNICATIONS ACT

In addition to consent (see Consent Under the Wiretap Act and SCA), the SCA contains several exceptions under 18 U.S.C. Sections 2701(c)(1) and 2702.

#### Exception for Authorized Access

The SCA prohibits anyone from intentionally accessing without authorized access or exceeding authorization to access a facility through which an ECS is being provided and then obtains, alters, or blocks access to a communication while it is in electronic storage (18 U.S.C. § 2701(a) and see Stored Communication Act).

However, liability does not attach when the conduct is authorized by either:

- The wire or ESCP.
- A user of that service regarding a communication of or intended for that user.

(18 U.S.C. § 2701(c)(1).)

Courts interpret this exemption as applicable to all searches by communications service providers (see, for example, *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3d Cir. 2003) (an employer's search of the plaintiff-employee's emails fell within this exception because the employer stored and administered the emails); *Councilman*, 418 F.3d at 81).

#### Exemptions for Disclosures to Specified Individuals and Entities

The SCA also contains exceptions that permit an ECSP or RCSP to disclose communications to select individuals and entities including:

- An addressee or intended recipient of the communication or the addressee's or intended recipient's agents (18 U.S.C. § 2702(b)(1)).
- As otherwise authorized in the ECPA (including in response to law enforcement process issued under the SCA) (18 U.S.C. § 2702(b)(2)).
- With the originator's, addressee's, or intended recipient's lawful consent or, in the case of an RCS, the subscriber's legal consent (18 U.S.C. § 2702(b)(3); see Consent Under the Wiretap Act and SCA).
- To a person employed or authorized to forward the communication to its destination (18 U.S.C. § 2702(b)(4)).
- As may be necessarily incident to the rendition of the service or the protection of the service provider's rights or property (18 U.S.C. § 2702(b)(5)).
- To the National Center for Missing and Exploited Children, if submitting a report of child pornography (18 U.S.C. § 2702(b)(6)).


© 2020 Thomson Reuters. All rights reserved.

- To a law enforcement agency if:
  - the service provider inadvertently obtained the contents; and
  - the contents appear to pertain to the commission of a crime.
- (18 U.S.C. § 2702(b)(7).)
- To a governmental entity if the provider in good faith believes that an emergency involving danger of death or serious physical injury to any person requires disclosure of communications relating to that emergency (18 U.S.C. § 2702(b)(8)).
- To a foreign government under an order from that foreign government issued under a new bilateral agreement under the CLOUD Act (18 U.S.C. § 2702(b)(9)).

**Record Information**

The SCA generally permits disclosure of record information in response to a government subpoena. Record information includes the subscriber's or customer's:

- Name.
- Address.
- Local and long-distance telephone connection records, or records of session times and durations;
- Length of service (including start date) and types of service used.
- Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address.
- Means and source of payment for that service (including any credit card or bank account number).

(18 U.S.C. § 2703(c)(2).)

**Good Faith Defense to Disclosure**

The SCA generally prohibits civil litigants from successfully subpoenaing technology companies for email content (see, for example, *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 609-12 (E.D. Va. 2008) (collecting cases)). However, an ECSP or RCSP that discloses subscriber information in response to a subpoena (or other process) may plead a "good faith" defense if:

- The subpoena or other process appeared valid on its face.
- The ECS or RCS did not know or have reason to know that it was invalid or contrary to applicable law.

(18 U.S.C. § 2707(e); see *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1180 (9th Cir. 2013) (Yahoo's good faith reliance on a grand jury subpoena seeking user records was a complete defense to an SCA claim).)

## DAMAGES UNDER THE SCA

A plaintiff bringing an SCA claim may:

- Seek injunctive relief and damages. Damages are the sum of actual damages suffered by the plaintiff and any profits the violator made as a result of the violation, but in no event less than $1,000.
- Recover attorneys' fees and costs.

(18 U.S.C § 2707(c).)

If a SCA violation is willful or intentional, a court may assess punitive damages (18 U.S.C § 2707(c)).

## CONSENT UNDER THE WIRETAP ACT AND SCA

The Wiretap Act and SCA do not apply if:

- Under the Wiretap Act, one of the parties to the intercepted communication consents to the interception (18 U.S.C. § 2511(2)(c),(d)).
- Under the SCA:
  - in the case of an ECS, the originator, addressee, or intended recipient consents to the disclosure; or
  - in the case of an RCS, the subscriber consents to the disclosure.
- (18 U.S.C. § 2702(b)(3).)
- The conduct is authorized by the wire or ESC provider, a user of that service regarding a communication of or intended for that user, or 18 U.S.C. §§ 2703, 2704, or 2518 (18 U.S.C. § 2701(c)).

Consent under both the Wiretap Act and SCA:

- Is only valid if the consenting, affected persons have adequate notice of the interception or disclosure (see, for example, *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014) ("[A]ny consent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice alleged in this case – that is, the scanning of message content for use in targeted advertising")).
- May pertain to either:
  - an entire communication; or
  - only part of a communication.
- (See, for example, *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *12 (citing *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581 (11th Cir. 1983)).)
- May be explicit or implied (see *Watkins*, 704 F.2d at 581 (holding that consent should not be "cavalierly implied"); *In re Pharmatrak*, 329 F.3d at 20)).

Organizations should obtain explicit consent if possible for evidentiary reasons (see, for example, *Perkins v. LinkedIn*, 53 F. Supp. 3d 1190, 1212-15 (N.D. Cal. 2014)) (the court found the plaintiffs had consented to the defendant harvesting their Gmail contacts because users were directed to various pages asking if LinkedIn may access a user's Gmail contacts and send invitations to join LinkedIn to every person from the user's Gmail contacts).

Courts have also struggled with implied consent, particularly when a defendant claims that their Terms of Use or Privacy Policy described the interceptions or disclosures. For example:

- In *In re Google Gmail Litigation*, the court found that the Privacy Policy and Terms of Use did not establish consent to the interception of communications for use in targeted advertising because:
  - the Privacy Policy only referenced interceptions for a limited set of uses (not including advertising); and
  - the Terms of Use only demonstrated that Google had the capacity to intercept communications, not that it intended to.
- (*In re Google*, 2013 WL 5423918, at *13.)
- In contrast, the court in *In re Yahoo Mail Litigation* found that Yahoo properly obtained consent through the Terms of Use which

© 2020 Thomson Reuters. All rights reserved.

specifically contemplated the intercepting of communications for targeted advertising (7 F. Supp. 3d at 1029).

## STANDING ISSUES IN ECPA LITIGATION

Plaintiffs bringing ECPA claims must establish an injury-in-fact sufficient to support Article III standing in federal court. Injury-in-fact is an invasion of a legally protected interest that is both:

- Concrete and particularized.
- Actual or imminent and not conjectural or hypothetical.

(*Low v. LinkedIn Corp*. 900 F. Supp. 2d 1010, 1020 (N.D. Cal. 2012.))

Courts disagree about what allegations support standing in ECPA claims. Some courts hold that allegations regarding mere access to personal information are insufficient to establish standing (see, for example, *In re Doubleclick, Inc., Privacy Litig*., 154 F. Supp. 2d 497, 525≈(S.D.N.Y. 2001) (cookies case, holding that unauthorized collection of personal information by a third-party is not "economic loss"); *In re JetBlue Airways Corp. Privacy Litig*., 379 F. Supp. 2d 299, 327 (E.D.N.Y.2005) (airline's disclosure of passenger data to third party in violation of airline's privacy policy had no compensable value)).

In contrast, some courts have allowed ECPA case to proceed based on an alleged consequence to the device through which an interception has occurred (see, for example, in *In re iPhone Application Litig*., 2011 WL 4403963, at *5 (N.D. Cal. Sept. 20, 2011) (finding allegations of actual injury based on diminished and consumed iDevice resources (such as storage, battery life, and bandwidth), decreased, unexpected, and unreasonable risk to the security of sensitive personal information, and detrimental reliance on Apple's representations regarding the privacy protection for iDevice apps); *In re Google Inc. Cookie Placement Consumer Privacy Litig*., 806 F.3d at 134-35 (the court found standing based on allegations that the defendants, in the course of serving advertisements to their personal web browsers, implanted tracking cookies on their personal computers)).

In *Spokeo, Inc. v. Robbins*, the US Supreme Court further addressed whether plaintiffs have Article III standing to sue for statutory damages regardless of whether they suffered any concrete harm (136 S. Ct. 1540 (2016)). *Spokeo* instructs that in determining whether an injury is concrete, courts may look to whether the alleged harm "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts" (*Spokeo*, 136 S. Ct. at 1549).

For more information, see Practice Note, Non-Statutory Grounds for Challenging Class Actions: Standing and Ascertainability: Standing and Statutory Violations (5-606-5912).

Applying *Spokeo*, some courts liken ECPA's causes of action to other common law or statutory claims (including the common law tort of invasion of privacy) in which plaintiffs alleged a sufficiently concrete injury to confer Article III standing (see, for example, *Campbell v. Facebook, Inc*., 2020 WL 1023350 (9th Cir. Mar. 3, 2020); see also *Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019) (Supreme Court vacated and remanded an SCA case against Google to address whether the plaintiffs had sufficiently alleged standing under *Spokeo*)).

For more on the *Campbell v. Facebook, Inc*., case, see Legal Update, Facebook Users Alleging Statutory Privacy Claims Have Article III Standing: Ninth Circuit (W-024-3203).

Courts assessing standing under *Spokeo* are therefore likely to analyze whether the ECPA codified a context-specific extension of the substantive right to privacy (see *In re Nickelodeon Consumer Privacy Litig*., 827 F.3d at 274 ("Congress has long provided plaintiffs with the right to seek redress for unauthorized disclosures of information that, in Congress's judgment, out to remain private"); *Satchell v. Sonic Notify, Inc*., 234 F. Supp. 3d 996, 1004 (N.D. Cal. 2017) (citing *Matera v. Google Inc*., 2016 WL 5339806, at *11 (N.D. Cal. Sept. 23, 2016) ("Invasion of privacy has been recognized as a common law tort for over a century.")).

**ABOUT PRACTICAL LAW**

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at **legalsolutions.com/practical-law**. For more information or to schedule training, call **1-800-733-2889** or e-mail **referenceattorneys@tr.com.**

06-20

© 2020 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (http://static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (https://a.next.westlaw.com/Privacy).