The LEXIS PRACTICE ADVISOR Journal™

The LEXIS PRACTICE ADVISOR Journal™

Practical guidance backed by leading attorneys from Lexis Practice Advisor®

CONFIDENTIALITY & WHISTLEBLOWING: WHERE IN-HOUSE COUNSEL'S COMPETING INTERESTS COLLIDE

The GDPR Compliance Deadline Has Arrived—Are You Prepared?

Climate Change Considerations in M&A Transactions

LexisNexis®

Summer 2018

SUMMER 2018

www.lexispracticeadvisor.com

Contents

SUMMER 2018

The
LEXIS PRACTICE ADVISOR Journal™

SUMMER 2018 (Volume 3, Issue 3)

EDITORIAL ADVISORY BOARD

Distinguished Editorial Advisory Board Members for The Lexis Practice Advisor Journal are seasoned practitioners with extensive background in the legal practice areas included in Lexis Practice Advisor®. Many are attorney authors who regularly provide their expertise to Lexis Practice Advisor online and have agreed to offer insight and guidance for The Lexis Practice Advisor Journal. Their collective knowledge comes together to keep you informed of current legal developments and ahead of the game when facing emerging issues impacting your practice.

The Lexis Practice Advisor Journal (Pub No. 02380; ISBN: 978-1-63284-895-6) is a complimentary publication published quarterly for Lexis Practice Advisor® subscribers by LexisNexis, 230 Park Avenue, 7th Floor, New York, NY 10169. **Email:** lexispracticeadvisorjournal@lexisnexis.com | **Website:** www.lexisnexis.com/lexispracticeadvisorjournal

Michael E. Lackey and Oral D. Pottinger MAYER BROWN LLP

Stored Communications Act: Practical Considerations

The Stored Communications Act (SCA), 18 U.S.C. § 2701 et seq., governs the disclosure of electronic communications stored with technology providers. Passed in 1986 as part of the Electronic Communications Privacy Act (ECPA), the SCA remains relevant to address issues regarding the privacy and disclosure of emails and other electronic communications.

AS THE USE OF TECHNOLOGY CONTINUES TO GROW, SO does the importance of the SCA's protections—and limits—on the disclosure of stored electronic communications. The SCA's age, however, makes it difficult to apply in modern times. This article provides guidance on how to apply the SCA to today's fast-growing technology.

Understanding How SCA Issues Arise

As a privacy statute, diverse circumstances can give rise to SCA issues:

- **Direct liability.** As discussed below, the SCA limits the ability of certain technology providers to disclose information. It also limits third parties' ability to access electronic communications without sufficient authorization. Litigation alleging violations of the SCA's substantive provisions therefore directly presents SCA issues.
- **Civil subpoena limitations.** Because of the SCA's restrictions on disclosure, technology providers and litigants often invoke the SCA when seeking to quash civil subpoenas to technology providers for electronic communications.[1]
- **Government investigations.** The SCA provides a detailed framework governing law enforcement requests for electronic communications. SCA issues often arise in motions to suppress and related criminal litigation. For example, a growing number of courts have found that the SCA is unconstitutional to the extent that it allows the government to obtain emails from an internet service provider without a warrant in violation of the Fourth Amendment. See U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010).

1. *See* Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (quashing subpoena), aff'd in part on other grounds, vacated in part on other grounds, 676 F.3d 19 (2d Cir. 2012); In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008); O'Grady v. Superior Court, 139 Cal. App. 4th 1423, 44 Cal. Rptr. 3d 72 (2006).

Additionally, the circuit conflict about whether technology providers and litigants can invoke the SCA when quashing criminal subpoenas or search warrants requesting data from extraterritorial servers, was resolved by the passage of the CLOUD Act as part of the Consolidated Appropriations Act, 2018, H.R. 1625, Div. V, 115th Cong., 2d Sess. (2018). The Act provides that a service provider must produce information within its "possession, custody, or control, regardless of whether such . . . information is located within or outside of the United States." CLOUD Act § 103(a). The passage of the CLOUD Act also rendered moot the *U.S. v. Microsoft* case pending before the Supreme Court on this issue. See U.S. v. Microsoft Corp., No. 17-2, slip op. at 3 (April 17, 2018) (dismissing the appeal as moot). The government has subsequently obtained a new warrant against Microsoft for the information requested in the original warrant at issue in the case.

Categorizing the Technology Involved in an SCA Claim

The technology behind an SCA claim matters. In many instances, the applicable SCA rules hinge on the particular technology involved. Specifically, different SCA rules apply depending on whether technology is classified as electronic communication services (ECS), remote computing services (RCS), both, or neither.

The following sections discuss the definitions of ECS and RCS, the rules applicable to each, and certain applications of these definitions. While you should familiarize yourself with these concepts, you must exercise caution in applying them. Courts have reached disparate results, and this area continually evolves with each new technological development.

Electronic Communication Services

The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[2] With certain exceptions, ECS providers may

not "knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[3]

Clear examples of an ECS include an email provider's computer systems, a bulletin board system, or an internet service provider (ISP).[4] In addition, courts have classified text message service providers as ECS providers.[5] Even if providing a messaging service or internet service is not the entity's primary business, the entity can qualify as an ECS provider.[6]

As a practical matter, the definition of ECS often plays an important role in e-discovery matters. Because the SCA prohibits ECS providers from disclosing the contents of communications stored with them, do not expect to succeed in obtaining these communications by subpoenaing an ECS provider, such as a social media website or email vendor. Instead, you should request these records from the creator or recipient of such content.

Remote Computing Services

In contrast, the SCA defines an RCS as providing to the public "computer storage or processing services by means of an electronic communications system."[7] Again with certain exceptions, the SCA prohibits RCS providers from knowingly divulging to any person or entity the contents of any communication that the service carries or maintains:

- On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service
- Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing[8]

For example, a U.S. District Court in Illinois found that Microsoft's Hotmail's email service was an RCS because it found that "Microsoft [was] maintaining the messages 'solely for the purpose of providing storage or computer processing services to such subscriber or customer.'"[9]

Both ECS and RCS

In some instances, courts have concluded that modern technology providers act as both ECS and RCS providers with the different services they offer.[10] In Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010), the court concluded that social media websites were ECS providers, but alternatively held that they were RCS providers.

Where a provider acts as both an ECS and RCS, the SCA's applicable rules will apply to those aspects of the service that fit within the respective definitions.

Neither ECS nor RCS

In some instances, neither an ECS nor an RCS provider holds electronic communications. "[A] person who does not provide an electronic communication service [or a remote communication service] can disclose or use with impunity the

Related Content

For guidance on how to counsel employers to manage the risks that accompany employee social media use, see

> **SOCIAL MEDIA ISSUES IN EMPLOYMENT: COUNSELING EMPLOYERS ON KEY SOCIAL MEDIA ISSUES**

RESEARCH PATH: *Labor & Employment > Employment Policies > Company Property and Electronic Information > Practice Notes*

For a discussion on the key issues involving the Electronic Communications Privacy Act, see

> **ELECTRONIC COMMUNICATIONS PRIVACY ACT: KEY ISSUES**

RESEARCH PATH: *Labor & Employment > Employment Policies > Company Property and Electronic Information > Practice Notes*

For additional information on the Electronic Communications Privacy Act, see

> **ELECTRONIC COMMUNICATION PRIVACY ACT ISSUES CHECKLIST**

RESEARCH PATH: *Labor & Employment > Employment Policies > Company Property and Electronic Information > Checklists*

2. 18 U.S.C. § 2510(15). 3. 18 U.S.C. § 2702(a)(1). 4. *See* In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1057 (N.D. Cal. 2012). 5. *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008), rev'd on other grounds, City of Ontario v. Quon, 560 U.S. 746 (2010). Courts have ruled as well for social media sites. *See* Ehling v. Monmouth-Ocean Hosp. Service Corp., 961 F. Supp. 2d 659 (D.N.J. 2013); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010). 6. *See* In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2705(b), 2018 U.S. Dist. LEXIS 19556 (D.D.C. Jan. 30, 2018) (Airbnb was an ECS provider as it provided a messaging service for its users to communicate with each other); In re United States for an Order Pursuant to 18 U.S.C. § 2703(d), 2018 U.S. Dist. LEXIS 52183 (D.D.C. Mar. 8, 2018) (Royal Caribbean Cruises provided internet service to its customers and thus qualified as an ECS provider). 7. 18 U.S.C. § 2711(2). 8. 18 U.S.C. § 2702(a)(2). 9. United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (quoting 18 U.S.C. § 2703(b)(2)). 10. *See* United States v. Weaver, 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009) (email service provider was both ECS and RCS provider); *see also* In re United States, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) ("Today, most ISPs provide both ECS and RCS.").

Terminated employees may retain access credentials or otherwise seek to obtain electronic records from the company. While the SCA may provide an employer with a remedy against such actions, a successful claim usually necessitates clear evidence that the employer had revoked the employee's authorization before the employee accessed the information.

contents of an electronic communication unlawfully obtained from electronic storage."[11]

In general, courts have concluded that personal devices, such as laptop computers and smartphones, do not provide electronic communications services for purposes of the SCA, even though they allow users to access such services.[12] Thus, individual computer users generally do not count as ECS or RCS providers.

However, while the SCA's disclosure limits would not apply, even entities that do not qualify as ECS or RCS providers can fall afoul of the SCA's limits on unauthorized access.[13] Importantly, the SCA provides for criminal and civil penalties for anyone who:

- Intentionally and without sufficient authorization
- Accesses "a facility through which an electronic communication service is provided"
- And in doing so, "obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system"[14]

Because the SCA does not prohibit the disclosure of information by non-ECS or RCS providers, you should not rely on it to protect against all possible disclosures of sensitive electronic communications.[15] Instead, you should counsel employers to maintain close control over individual devices, such as company laptops and cell phones.

Determining What Is in Electronic Storage

The SCA's ECS restrictions, 18 U.S.C. § 2702(a)(1), and access restrictions, 18 U.S.C. § 2701, only apply to communications that are in electronic storage. Electronic storage means:

- Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof
- Any storage of such communication by an ECS for purposes of backup protection of such communication[16]

In today's world of cloud computing and remote hosting, applying this definition can prove difficult. In particular, courts continue to struggle with whether documents stored remotely, such as web-based email, are stored "for purposes of backup protection" or for some other purpose that would render them outside the scope of the SCA's definition.[17] Nonetheless, certain general principles can help you analyze this portion of a potential SCA claim:

- Messages (such as emails, bulletin board postings, or pager messages) being stored pending delivery are generally deemed to be in electronic storage for purposes of the SCA.[18]
- Items stored on personal devices, such as cookies (small pieces of data stored on an internet user's computer) and text messages are generally not deemed to be in electronic storage for purposes of the SCA.[19]
- Messages that have already been delivered and read, but that a user chooses to leave on the server, have produced divergent results. Courts disagree on whether such emails are stored "for purposes of backup protection."[20]

Because technology continues to change, and in light of the disagreement among the courts in applying the SCA's definitions to today's technology, you should exercise caution in coming to fixed conclusions about the SCA's implications to particular facts.

---

11. Wesley College v. Pitts, 974 F. Supp. 375, 389 (D. Del. 1997). **12.** *See* Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012); United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); In re iPhone Application Litig., 844 F. Supp. 2d at 1057–58; In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001); Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1270–71 (N.D. Cal. 2001). **13.** *See* Penrose Computer Marketgroup, Inc. v. Camin, 682 F. Supp. 2d 202, 211 (N.D.N.Y. 2010) ("[S]ection 2701 outlaws illegal entry, not larceny.") **14.** 18 U.S.C. § 2701. **15.** *See* K.F. Jacobsen & Co. v. Gaylor, 947 F. Supp. 2d 1120 (D. Or. 2013) (rejecting SCA claim because employers' individual computers were not ECS facilities). **16.** 18 U.S.C. § 2510(17). **17.** *See* Lazette v. Kulmatycki, 949 F.Supp.2d 748, 758-59 (N.D. Ohio 2013) (discussing the divergence in opinions). **18.** *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2003) (collecting cases); Quon, 529 F.3d 892. **19.** *See* In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 511–12; Garcia, 702 F.3d 788. **20.** Compare Theofel, 359 F.3d 1076-77, (holding delivered messages were in electronic storage for purposes of the SCA); Bailey v. Bailey, 2008 U.S. Dist. LEXIS 8565, at *16–18 (E.D. Mich. Feb. 6, 2008) (same); Ehling v. Monmouth-Ocean Hosp. Service Corp., 961 F. Supp. 2d 667 (D.N.J. 2013) (holding that Facebook wall postings were in electronic storage) with United States v. Weaver, 636 F. Supp. 2d 771–73 (C.D. Ill. 2009) (holding previously opened messages not in electronic storage for purposes of the SCA); Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012).

Analyzing "Authorization"

Proper analysis of an SCA claim under 18 U.S.C. § 2701 also requires you to examine the factual question of whether the defendant acted "without authorization" or "exceed[ed] an authorization" in accessing the facility involved. In general, "[p]ermission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances."[21]

However, where an individual was "entitled to see" the information, courts do not generally find liability.[22] This result holds even where an individual puts the electronic communications to unauthorized use.[23] Relatedly, joint use of a computer will often preclude an SCA claim by one user against another.[24]

This issue often arises in the context of post-termination employment disputes. Terminated employees may retain access credentials or otherwise seek to obtain electronic records from the company. While the SCA may provide an employer with a remedy against such actions, a successful claim usually necessitates clear evidence that the employer had revoked the employee's authorization before the employee accessed the information.[25] You should therefore counsel clients to develop policies that will facilitate such proof.

Exceptions to SCA Prohibitions

The SCA includes many exceptions to its prohibitions, which the following sections discuss.

Certain Authorized Conduct

The SCA[26] does not apply with respect to conduct authorized:

- By the person or entity providing a wire or electronic communications service
- By a user of that service with respect to a communication of or intended for that user
- In Section 2703 (government access, 18 U.S.C. § 2703), 2704 (backup preservation, 18 U.S.C. § 2704), or 2518 (court-ordered electronic eavesdropping or wiretaps, 18 U.S.C. § 2518)

Allowable Disclosures of Communication Contents

The SCA allows providers of an RCS or ECS to disclose the contents of a communication:

- To an addressee or intended recipient of such communication or an agent of such addressee or intended recipient
- As otherwise authorized in Sections 2517, 2511(2)(a), or 2703 of the SCA
- With the lawful consent of the originator or an addressee or intended recipient of such communication or the subscriber in the case of an RCS
- To a person employed or authorized or whose facilities are used to forward such communication to its destination
- As may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service
- To the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 2258A
- To a law enforcement agency if the contents (1) were inadvertently obtained by the service provider and (2) appear to pertain to the commission of a crime
- 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 without delay of communications relating to the emergency[27]

---

21. Theofel v. Farey-Jones, 359 F.3d 1073. **22.** *See* Int'l Ass'n of Machinists & Aero. Workers v. Werner–Masuda, 390 F. Supp. 2d 479, 495 (D. Md. 2005). **23.** *See* Educational Testing Serv. v. Stanley H. Kaplan Educ. Ctr., 965 F. Supp. 731, 740 (D. Md. 1997). **24.** *See* White v. White, 781 A.2d 85, 90–91 (N.J. 2001); State v. Poling, 938 N.E.2d 1118, 1123 (Ohio 2010). **25.** *See* Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000) (rejecting SCA claim because individuals had authorization at the time of access); Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg., & Consulting, LLC, 600 F. Supp. 2d 1045, 1050 (E.D. Mo. 2009) (similar). **26.** 18 U.S.C. § 2701(c).

Consent Exception

The consent exception (18 U.S.C. § 2702(b)(3)) is one of the more common exceptions to arise under the SCA. In addition to allowing disclosures with the sender's consent, this exception also allows the disclosure of communications directed to the service provider.[28]

Allowable Disclosures of Information Concerning a Subscriber or Customer

The SCA allows providers of an RCS or ECS to disclose information concerning a subscriber to, or customer of, such service (not including contents of communications covered by 18 U.S.C. § 2702 (a)(1) or (a)(2)):

- As otherwise authorized in 18 U.S.C. § 2703
- With the lawful consent of the customer or subscriber
- As may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service
- 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 without delay of information relating to the emergency
- To the National Center for Missing and Exploited Children, in connection with a report submitted thereto under 18 U.S.C. § 2258A
- To any person other than a governmental entity[29]

Court Orders, Warrants, Subpoenas, Statutory Authorization, or Certifications

The SCA has an exception for ECS providers who provide information in response to a legal mandate. Specifically:

> No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.[30]

Through this exception, service providers can disclose information not only in response to court orders and law enforcement requests, but also in cases of crisis. Specifically "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."[31]

Good Faith Defense

The SCA allows a complete defense when a defendant can show good faith reliance on:

- A court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under Section 2703(f))
- A request of an investigative or law enforcement officer under 18 U.S.C. § 2518(7)
- A good faith determination that 18 U.S.C. § 2511(3) permitted the complained-of conduct[32]

If a recipient of an SCA request complies with the request in good faith, it will enjoy immunity from suit even if the request is later determined to be invalid.[33] While courts differ slightly in their tests for determining whether a recipient has acted in good faith, the question generally boils down to reasonableness.[34] This exception lowers the burden

---

27. 18 U.S.C. § 2702(b). **28.** In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011), rev'd on other grounds, 572 Fed. Appx. 494 (9th Cir. 2014); In re Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 560–61 (N.D. Tex. 2005). **29.** 18 U.S.C. § 2702(c). **30.** 18 U.S.C. § 2703(e). **31.** 18 U.S.C. § 2702(c)(4). **32.** 18 U.S.C. § 2707(e). **33.** *See* Sams v. Yahoo! Inc. 713 F.3d 1175, 1179–1181 (9th Cir. 2013). **34.** *See* Sams v. Yahoo! Inc. 713 F.3d 1181; McCready v. eBay, Inc., 453 F.3d 882, 892 (7th Cir. 2006).

Related Content

For guidance on how to counsel employers to manage the risks that accompany employee social media use, see

> SOCIAL MEDIA ISSUES IN EMPLOYMENT: COUNSELING EMPLOYERS ON KEY SOCIAL MEDIA ISSUES

RESEARCH PATH: *Labor & Employment > Employment Policies > Company Property and Electronic Information > Practice Notes*

For a discussion on the key issues involving the Electronic Communications Privacy Act, see

> ELECTRONIC COMMUNICATIONS PRIVACY ACT: KEY ISSUES

RESEARCH PATH: *Labor & Employment > Employment Policies > Company Property and Electronic Information > Practice Notes*

For guidance on protecting confidential information, see

> CYBERSECURITY MEASURES TO PROTECT EMPLOYERS' CONFIDENTIAL INFORMATION AND TRADE SECRETS

RESEARCH PATH: *Labor & Employment > Non-competes and Trade Secret Protection > Protecting Trade Secrets > Practice Notes*

on recipients to scrutinize requests under the SCA for all potential flaws.

Statutory, Actual, and Punitive Damages

With respect to direct liability, you should take note that a plaintiff suing under 18 U.S.C. § 2707 for violations of the SCA can pursue either (1) their actual damages and any profits the violator obtained or (2) $1,000. The statute also provides for punitive damages.

Courts disagree, however, about whether a plaintiff must show some amount of actual damages in order to trigger the statutory damages provision.[35] Thus, you should take careful note of the jurisdiction in which an SCA claim is brought, as this disagreement may have significant implications for how a case is litigated. But note that even *Van Alstyne* holds that punitive damages may be available in the absence of proof of actual damages.

Secondary Liability

Courts generally agree that, although the SCA creates civil liability for violations of its prohibitions, it does not create secondary civil liability, such as for aiding and abetting or conspiracy.[36]

Other Potentially Relevant Law

The SCA is not the only statute governing the disclosure of electronic communications. Many cases involving electronic communications also involve potential liability under the Wiretap Act, 18 U.S.C. § 2510 et seq., which was also passed as part of the Electronic Communication Privacy Act. In addition, depending on the facts involved, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Pen Register Act, 18 U.S.C. § 3121 et seq., or the Cybersecurity Act of 2015, 6 U.S.C. § 1501 et seq., may apply, as well as traditional common-law doctrines such as trespass and intrusion upon seclusion.

Michael E. Lackey leads Mayer Brown LLP's global litigation and dispute resolution practice, serves on the firm's Partnership Board, and is a co-leader of its Electronic Discovery & Information Governance group. His practice focuses on civil and criminal litigation, and he represents major companies and individuals in state and federal proceedings, including multi-district and class action litigation. In addition to being an accomplished litigator, Mike is nationally recognized for his knowledge of electronic discovery issues. ***Oral D. Pottinger*** *is a senior associate in the Antitrust practice at Mayer Brown. He specializes in mergers and acquisitions, civil and criminal antitrust investigations, antitrust counseling, and Federal Communications Commission cable and media representation. Oral has served as a trusted advisor addressing the needs of corporate clients from information risk management and data-retention planning to discovery planning, e-discovery collection, data analytics, managed electronic review, and production. Special acknowledgment is provided to* ***Sasha Keck****, Mayer Brown associate, for her research assistance.*

RESEARCH PATH: *Labor & Employment > Employment Policies > Company Property and Electronic Information > Practice Notes*

---

35. Compare Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199, 206 (4th Cir. 2009) (actual damages are a prerequisite to recover statutory damages) with Shefts v. Petrakis, 931 F. Supp. 2d 916, 918 (C.D. Ill. 2013) no actual damages necessary to recover statutory damages). **36.** *See* Council on American–Islamic Rels. Action Network, Inc. v. Gaubatz, 891 F. Supp. 2d 13, 26–27 (D.D.C. 2012); Garback v. Lossing, 2010 U.S. Dist. LEXIS 99059, at *19 n. 6 (E.D. Mich. Sept. 20, 2010); Jones v. Global Info. Grp., Inc., 2009 U.S. Dist. LEXIS 23879, at *5–7 (W.D. Ky. Mar. 25, 2009).

Stored Communications Act Issues Checklist

This is a high-level checklist for examining issues involving the Stored Communications Act (SCA), 18 U.S.C. § 2701 et seq., which comprises one of the major components of the Electronic Communication Privacy Act (ECPA). The other major component of the ECPA is the Wiretap Act, 18 U.S.C. § 2510 et seq. The Wiretap Act generally governs when communications (whether electronic, oral, or wire) are "intercept[ed]," while the Stored Communications Act governs access to electronic communications that are "in electronic storage."

Consider How SCA Issues May Arise

Keep in mind the variety of ways in which SCA issues may arise:

- ✓ **SCA compliance.** Consider direct liability for violations of the SCA's provisions.
- ✓ **Subpoenas.** Keep in mind the limitations on civil subpoena responses due to the SCA.
- ✓ **Government investigations.** Consider access to stored communications by government investigators.

Is the Technology an Electronic Communication Service or a Remote Computing Service?

Determine the relevant SCA rules for the particular technology involved. Different SCA rules apply depending on whether technology is classified as "electronic communication services" (ECS), "remote computing services" (RCS), both, or neither.

- ✓ **Consider whether the technology is an electronic communication service or a remote computing service.** In doing so, think about the following issues:
  - **Legislation outdated.** Recognize that Congress passed the SCA in 1986—before the development of most modern technology. Thus, applying the SCA to today's technology may be difficult/uncertain.
  - **Issues with categorization.** Note that some technologies may provide both an electronic communication service and a remote computing service. Some technologies may be neither.

Determine Whether Communications Were Stored Electronically

If the technology is an electronic communications service, consider whether the communications involved were in electronic storage.

- ✓ **Messages pending delivery.** Messages pending delivery are generally held to be in electronic storage. See, e.g., Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008), rev'd on other grounds, 560 U.S. 746 (2010).
- ✓ **Delivered messages.** Courts have reached varying results regarding delivered messages. Compare, e.g., Theofel v. Farey-Jones, 359 F.3d 1066, 1076–77 (9th Cir. 2003) (holding delivered messages were in electronic storage for purposes of the SCA) with United States v. Weaver, 636 F. Supp. 2d 769, 771–73 (C.D. Ill. 2009) (holding previously opened messages not in electronic storage for purposes of the SCA).
- ✓ **Items stored on personal devices.** Courts generally conclude that items stored on personal devices are not in electronic storage. See, e.g., In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001); Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012).

Consider Potential Defenses or Exceptions to Liability

- ✓ **Authorization not exceeded.** If the policy or procedures in place entitled the accessing individual to see the information, courts will generally not find SCA liability. See 18 U.S.C. § 2701(c); Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000) (rejecting SCA claim because individuals had authorization at the time of access).
- ✓ **Permissible disclosures of communication contents.** The SCA allows remote computing services or electronic communication services to disclose the contents of a communication in circumstances specifically addressed in 18 U.S.C. § 2702(b).
- ✓ **Permissible disclosures of information concerning a subscriber or customer.** The SCA allows providers of a remote computing service or electronic communication service to disclose information concerning a subscriber to, or customer of, such service in circumstances specifically addressed in 18 U.S.C. § 2702(c).
- ✓ **Court orders, warrants, subpoenas, statutory authorization, or certifications.** The SCA has an exception for electronic communication service providers who provide information in response to a legal mandate pursuant to 18 U.S.C. § 2703(e) or 18 U.S.C. § 2702(c)(4).
- ✓ **Good faith reliance on legal requests.** There is generally no SCA liability for individuals or entities relying in good faith on a court order or law enforcement request for access to stored communications. See 18 U.S.C. § 2707(e).

Consider Potential Liability

Consider the following types of potential liability under the SCA:

- ✓ **Civil remedies.** A civil plaintiff can recover:
  - **Actual/statutory damages.** A civil plaintiff can recover either actual or statutory damages. See 18 U.S.C. § 2707.
    - Note that some courts hold that plaintiffs must prove at least some actual damage to recover statutory damages. See, e.g., Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199, 206 (4th Cir. 2009).
  - **Punitive damages.** The SCA provides for punitive damages. See 18 U.S.C. § 2707.
- ✓ **Aiding/abetting liability.** Courts have held that the SCA does not impose civil liability under an aiding and abetting theory. See, e.g., Council on American–Islamic Rels. Action Network, Inc. v. Gaubatz, 891 F. Supp. 2d 13, 26–27 (D.D.C. 2012).
- ✓ **Criminal liability.** The SCA also includes potential criminal liability for violations of its provisions. See 18 U.S.C. § 2707.

Research Other Potentially Applicable Laws

The following laws may also be applicable:

- ✓ The Wiretap Act, 18 U.S.C. § 2510 et seq.
- ✓ The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. For information on the CFAA, see Cybersecurity Measures to Protect Employers' Confidential Information and Trade Secrets and Counterclaims or Separate Lawsuits against Plaintiff Employees.
- ✓ The Pen Register Act, 18 U.S.C. § 3121 et seq.
- ✓ The Cybersecurity Act of 2015, 6 U.S.C. § 1501 et seq.
- ✓ State tort laws concerning privacy

Related Content

For more information on the Wiretap Act and the SCA, see

ELECTRONIC COMMUNICATIONS PRIVACY ACT: KEY ISSUES

RESEARCH PATH: *Labor & Employment > Employment Policies > Company Property and Electronic Information > Practice Notes*

For more information on the ECPA, see

ELECTRONIC COMMUNICATION PRIVACY ACT ISSUES CHECKLIST

RESEARCH PATH: *Labor & Employment > Employment Policies > Company Property and Electronic Information > Checklists*

*Checklist provided by **Michael E. Lackey and Oral D. Pottinger** at Mayer Brown LLP.*

RESEARCH PATH: *Labor & Employment > Employment Policies > Company Property and Electronic Information > Checklists*