Suffolk Journal of Trial and Appellate Advocacy

Volume 15 Article 10

1-1-2010

Exploring Challenges with the Discovery of Text Messages in Federal Cases Through the Lens of the Federal Rules of Civil Procedure and the Stored Communications Act, 18 U.S.C. Sec. 2701-11

Erin Marie Secord

EXPLORING CHALLENGES WITH THE DISCOVERY OF TEXT MESSAGES IN FEDERAL CASES THROUGH THE LENS OF THE FEDERAL RULES OF CIVIL PROCEDURE AND THE STORED COMMUNICATIONS ACT, 18 U.S.C. §§ 2701-11

I. INTRODUCTION

Abco, Inc. ("Abco") is suing Allen Dean ("Dean") in United States District Court for misappropriation of trade secrets based on text messages that Dean sent to Abco's lead competitor, Banes, Inc. ("Banes"). Dean exchanged sensitive information with Banes employees on his company-owned cell phone on nearly a dozen occasions. Dean's counsel moved to enjoin both Banes' and Abco's requests for text message data based on the Stored Communications Act ("SCA") and his Fourth Amendment rights. Dean's cellular service provider, Sprintel, Inc., refuses to release any of the text message data in response to Banes' and Abco's discovery requests. Both Abco and Banes have filed motions to compel release of the text message data based on the Federal Rules of Civil Procedure ("Rules"); the text message data is critical to all parties' claims.

This hypothetical case illustrates the complex party dynamics in the discovery of text messages and pager data. This note explores federal civil cases with similar text message and pager data discovery issues with a focus on the interplay between constitutional claims, federal law, and the Rules.

In 2009, as compared to twenty years ago, almost all stored information and communications are electronic; this shift complicates the scope of electronic discovery.[1] Widely accepted yet vague standards determine discovery rules for electronically stored data such as the raw text message data from cell phones and pagers.[2] Fourth Amendment challenges

---

[1] *See* FED. R. CIV. P. 34(a) advisory committee's note (2006) (basing amendments to Rules on need for clarification amidst "dramatic" surge in electronic information); *see generally* David K. Isom, *Electronic Discovery Primer for Judges*, 2005 FED. CTS. L. REV. 1, ¶ I.1 (2005) (asserting over 99% of information "created and stored is stored electronically"). Furthermore, the increased use of electronic information and communications has precipitated the need for additional clarity as to what constitutes a "document" under the Rules. *Id.* at ¶ II.A.1-3.

[2] *See* Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules*, 12 RICH. J.L. & TECH. 13, 13 (2006), available at http://law.richmond.edu/jolt/v12i4/article13.pdf (stating

are common in electronic discovery disputes and the criteria for determining the permissibility of certain types of electronic discovery are laid out in a handful of federal cases.[3] Though courts and legislatures have provided a modicum of guidance on issues of electronic discovery, many ambiguities remain.[4]

Text messages[5] are a relatively new application area for the Rules, and thus few courts have explicitly defined the standards for producing text messages.[6] The Rules were revised in 2006 to provide courts with more direction on issues of electronic discovery including metadata and electronic media that are dramatically altering the landscape of electronic discovery.[7] Among other goals, the revisions to the Rules sought to

---

standard for preserving and identifying electronic information requires "reasonable and good faith efforts") (quoting The Sedona Conference, The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production (2005)). Nevertheless, requiring parties to preserve all electronic information based on potential relevance is unreasonable. *Id.*

[3] *See* Katz v. United States, 389 U.S. 347, 360 (1967) (6-1 decision) (Harlan, J., concurring) (establishing "reasonable expectation of privacy" test to determine whether physical or electronic "intrusion" violated Fourth Amendment); *see also* O'Connor v. Ortega, 480 U.S. 709, 731-32 (1987) (Scalia, J., concurring) (advocating *Katz* analysis to find against hospital employee alleging privacy violation). The majority in *O'Connor* agreed with Justice Scalia's application of the *Katz* reasonable expectation of privacy analysis. *Id.* at 717-18 (majority opinion). *See generally* Timothy Casey, *Electronic Surveillance and the Right To Be Secure*, 41 U.C. DAVIS L. REV. 977, 977 (2008) (noting *Katz* test has evolved into "the touchstone of Fourth Amendment analysis"); William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must be Honest*, 12 EMPLOYEE RTS. & EMP. POL'Y J. 49, 58 (2008) (citing *O'Connor*, 480 U.S. at 717) (setting forth scope of employees' "reasonable expectation of privacy" in the workplace).

[4] *See* Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. 07-1029, 2008 U.S. Dist. LEXIS 33463, at *8-9 (W.D. Pa. Apr. 23, 2008) (illustrating lack of relevant case law regarding SCA, Electronic Communications Privacy Act of 1986 18 U.S.C. § 2510(4) (2008) and electronic discovery). *But see* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904-05 (9th Cir. 2008) (employing well-defined criteria to hold text message data on police officers' pagers not discoverable). The Ninth Circuit relied on the Fourth Amendment and the SCA to evaluate the discoverability of the text message data. *Id.* at 901-02, 905.

[5] For the purposes of this article, a text message is a message "that is entered via a keypad rather than spoken into a receiver," excluding e-mail and other communications via computers. Robin Miller, Annotation, *Expectation of Privacy in Text Transmissions to or from Pager, Cellular Telephone, or Other Wireless Personal Communications Device*, 25 A.L.R. 6TH 201, § 1 (2007).

[6] *See* Bohach v. City of Reno, 932 F. Supp. 1232-33, 1237 (D. Nev. 1996) (holding text messages sent by employees from City pagers and stored within City's database are discoverable); *see also Quon*, 529 F.3d at 904-06 (concluding audit of police officers' text data improperly violated officers' reasonable expectation of privacy); Flagg v. City of Detroit, 252 F.R.D. 346, 347 (E.D. Mich. 2008) (ruling magistrate judge could properly examine text message evidence *in camera* based on Rule 34); *Ideal Aerosmith*, 2008 U.S. Dist. LEXIS 33463, at *8-9 (noting dearth of definitive case law interpreting SCA).

[7] *See* Isom, *supra* note 1, at ¶¶ I.3, II.T.2 (arguing 2006 Rules revisions purport to provide additional guidance for electronic discovery).

specifically address both printed and electronic media.[8] Increasingly, accessibility and availability of electronic information have become the central grounds for objections to discovery requests.[9] Moreover, the rapid evolution of electronic communication and retrieval methods has revealed new frontiers of discovery, such as text messages and pager data.[10]

This note argues that advances in technology increasingly require judges to craft new approaches to discovery issues regarding text message and pager data, and that judges often inject a great deal of public policy reasoning into their holdings.[11] Rules 26, 34, and 45 emphasize a pragmatic, liberal approach to discovery, yet these rules alone are inadequate to create consistent electronic discovery practices.[12] Furthermore, the SCA[13] adds another level of complexity to text message discoverability that exacerbates case law inconsistencies because of its vague standards for electronic communication systems ("ECS") and remote computing services ("RCS").[14] These hazy layers of discovery rules and federal statutes have created a patch-work of precedent that is often too fact-specific to provide guidance for future cases.[15] Ultimately, the jurisprudence regarding the discoverability of text messages will likely become more cohesive as new cases emerge to clarify the myriad ambiguities that currently plague this area of law.[16]

---

[8] FED. R. CIV. P. 34(a) advisory committee's note (2006) (asserting 2006 amendments equalize applicability of Rules to electronic and paper documents); *see also* Scotts Co. v. Liberty Mut. Ins. Co., No. 2:06-CV-899, 2007 U.S. Dist. LEXIS 43005, at *4-5 (S.D. Ohio June 12, 2007) (relying on amended Rules to find plaintiff equally entitled to access to electronic and paper documents).

[9] *See* Allman, *supra* note 2, at 17-18 (arguing Advisory Committee took middle ground by permitting parties to specify electronic or paper production medium).

[10] *See The Litigator's Secret Weapon: ONSITE3's DXR Software*, METROTROPOLITAN CORPORATE COUNS., Jan. 2007, at 35, *available at* http://www.metrocorpcounsel.com/pdf/2007/January/35.pdf (indicating improvements in optical scan and electronic data recovery facilitate review of text message data).

[11] *See infra* notes 59-60 and accompanying text (summarizing standards for employee privacy and noting jurisdictional inconsistencies); *see also* Isom, *supra* note 1, ¶ II.k.1 (emphasizing judges' discretion in developing electronic discovery rules based on fairness and efficiency).

[12] *See infra* Part II (discussing relevant discovery requirements in Rules 26, 34, and 45, and SCA defenses to discovery).

[13] Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§ 2701-11 (2008) (providing requisite conditions for service providers responding to requests for release of electronic information).

[14] *See infra* Parts II-III (discussing effect of relevant Rules and SCA on discoverability of text messages).

[15] *See infra* Part IV (analyzing application of Rules and SCA within context of text message discovery).

[16] *See infra* Part V (predicting forthcoming clarity in electronic discovery issues).

II. HISTORY

Though many of the Rules are relevant to the discovery of electronic information, Rules 26, 34, and 45 specifically apply to electronic discovery issues.[17] Rule 26(b)(1) defines the scope of discovery and provides broad standards for courts granting discovery motions.[18] Some of the impetuses in amending the Rules in 2006 were to increase accessibility, to lower the cost of discovering electronic materials, and to clarify ambiguities with respect to privilege and waiver.[19] Generally, Rule 26 gives trial courts substantial latitude in deciding whether a discovery request constitutes an undue burden that would justify non-production.[20] Rule 26 also lays out the general interpretative approach to other Rules, which were amended in 2006, in part to address the legal community's imploration for guidance.[21] Rule 34 provides specific guidance factors that a court must employ when adjudicating electronic discovery disputes.[22]

---

[17] *See* Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 up to the Task?*, 41 B.C. L. REV. 327, 342 (2000) (asserting Rules 26-37 lay foundation for modern discovery process). These Rules render trials "a search for truth rather than a battle of wits." *Id.*; *see also* Isom, *supra* note 1, at ¶ II.T.2 (2005) (explaining amended Rule 45 allows litigants to subpoena third parties for electronic discovery).

[18] *See* FED. R. CIV. P. 26(b)(1) ("Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence."); *see also* Modern Eng'g, Inc., v. Peterson, No. 07-CV-1055, 2007 U.S. Dist. LEXIS 51131,*1-2, 7-8 (C.D. Ill. July 16, 2007) (granting plaintiff's motion to compel production of transmitted information including text messages under defendant's control). The district court reasoned that the "care, custody, and control" standard is the proper production criteria and cited Moore's Federal Practice as the definitive approach to determining control. *Id.* at *6-7.

[19] *See* Richard L. Marcus, *E-Discovery Beyond the Federal Rules*, 37 U. BALT. L. REV. 321, 331 (2008) (observing "major shift" in corporate attitudes towards electronic discovery and Advisory Committee's willingness to provide concrete guidance). Since 2000, the Federal Rules Advisory Committee has made recommendations on electronic discovery and preservation policies in piecemeal fashion. *Id.* at 331-33.

[20] *See Modern Eng'g*, 2007 U.S. Dist. LEXIS 51131, at *2-3 (citing Packman v. Chicago Tribune Co., 267 F.3d 628, 646 (7th Cir. 2001)) ("District Courts have broad discretion in discovery matters.").

[21] *See generally* Scheindlin & Rabkin, *supra* note 17, at 329, 341 (summarizing Rule 26(b)(1) as defining scope of discovery and predicting surge in electronic discovery disputes).

[22] *See* FED R. CIV. P. 34. The Rules provide well-enumerated standards for complying with document requests, as evidenced in Rule 34(a), which states, in relevant part:

> (a) A party may serve on any other party a request within the scope of Rule 26(b):
>
> > (1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:
> >
> > > (A) any designated documents or electronically stored information--including writings, drawings, graphs, charts, photographs, sound

This rule requires the responding party to search and produce electronic information in some form, but does not necessarily allow the requesting party to conduct the actual search of the relevant data.[23] Moreover, the complexity of electronic discovery issues and the interplay between Rules 26 and 34 have incited some courts to craft novel responses to a requesting party's motion to compel discovery, such as allowing a qualified third party to inspect the data.[24] Many courts have declined to accept the premise that requests for electronic data constitute an unreasonable burden on the producing party and have required each party to substantiate its claims.[25]

> recordings, images, and other data or data compilations--stored in any medium. . . .
>
> (2) to permit entry onto designated land or other property possessed or controlled by the responding party, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

FED. R. CIV. P. 34 (a). In addition, Rule 34(b)(2)(D) and (E) provide the scope of the discoverability of electronic information.

> (D) Responding to a Request for Production of Electronically Stored Information. The response may state an objection to a requested form for producing electronically stored information. If the responding party objects to a requested form--or if no form was specified in the request--the party must state the form or forms it intends to use.
> (E) Producing the Documents or Electronically Stored Information. Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:
>
> (i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;
> (ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and
> (iii) A party need not produce the same electronically stored information in more than one form.

FED. R. CIV. P. 34(b)(2)(D)-(E); *see also* Auto Club Family Ins. Co. v. Ahner, No. 05-5723, 2007 U.S. Dist. LEXIS 63809, at *10-11 (E.D. La. Aug. 29, 2007) (determining opposing counsel's objection regarding difficulty of retrieving electronic information insufficient to show undue burden); Scheindlin & Rabkin, *supra* note 17, at 356-57 (asserting determination of undue burden depends on electronic information accessibility).

[23] FED. R. CIV. P. 34 advisory committee's notes (2006) ("[Rule 34] is not meant to create a routine right of direct access to a party's electronic information system. . . ."); *see also* Scotts Co. v. Liberty Mut. Ins. Co., No. 2:06-CV-899, 2007 U.S. Dist. LEXIS 43005, at *9-10 (S.D. Ohio June 12, 2007) (citing *In re* Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003)) (relying on 2006 Advisory Committee's Note to deny plaintiff access to defendant's electronic databases).

[24] *See* Thielen v. Buongiorno USA, Inc., No. 1:06-CV-16, 2007 U.S. Dist. LEXIS 8998, at *8-9 (W.D. Mich. Feb. 8, 2007) (permitting restricted access to plaintiff's electronic data by qualified forensic expert).

[25] *See Auto Club Family Ins.*, 2007 U.S. Dist. LEXIS 63809, at *11 (declining to find undue

Determining the respective burden on each party in producing electronic materials, such as text messages and pager data, is highly dependent on the specific facts of each case, resulting in wide variability among the federal courts.[26]

Rule 45(a)(1)(C) specifically addresses third party subpoenas for the production of electronic materials and applies to both non-electronic and electronic information.[27] Though some federal courts have held that electronic and hard copies of documents are equally discoverable, Fourth Amendment privacy concerns abound.[28] Other federal courts have taken markedly different approaches, including altering the burden of proof required for a party objecting to an electronic discovery request.[29] Though the amended Rules sought to avoid such inconsistencies, some have observed the inherent electronic discovery disparities among circuits.[30]

In addition to the Rules, the SCA, which was enacted as a revision to the Electronic Communications Privacy Act of 1986,[31] provides specific

---

burden in producing electronic information without sufficient evidence of inaccessibility).

[26] *See infra* Part IV (analyzing inconsistent standards for electronic discovery of text messages and pager data).

[27] FED R. CIV. P. 45(a)(1)(C). In relevant part, Rule 45 states:

> Combining or Separating a Command to Produce or to Permit Inspection; Specifying the Form for Electronically Stored Information. A command to produce documents, electronically stored information, or tangible things or to permit the inspection of premises may be included in a subpoena commanding attendance at a deposition, hearing, or trial, or may be set out in a separate subpoena. A subpoena may specify the form or forms in which electronically stored information is to be produced.

Id.; *see also* Jonathan O. Harris, Expert Commentary, *E-Discovery: the Good, the Bad and the Ugly*, 1 (LexisNexis May 2008) (on file with journal).

[28] *See infra* note 56 and accompanying text (recounting interplay between Rules and Fourth Amendment claims); *see also* Harris, *supra* note 27, at *3 (noting Federal Rules Advisory Committee expressed concerns regarding employee privacy).

[29] *See Auto Club Family Ins.*, 2007 U.S. Dist. LEXIS 63809, at *9-10 (holding the objecting party did not meet heightened burden of proof). "[The objecting party] must make an *evidentiary showing* that the data sought is not reasonably accessible because of undue burden or cost." *Id.* at *8.

[30] *See* Scotts Co. v. Liberty Mut. Ins., No. 2:06-CV-899, 2007 U.S. Dist. LEXIS 43005, at *10 (S.D. Ohio June 12, 2007) (citing Diepenhorst v. City of Battle, No. 1:05-cv-734, 2006 U.S. Dist. LEXIS 48551, at *9 (W.D. Mich. June 30, 2006)) (noting dearth of cases addressing whether opposing counsel may inspect electronically stored information). The "nascent conflict between electronic privacy laws and communications technology" has led to a marked increase in electronic surveillance and has rendered electronic discovery "confusing and uncertain." Frederick M. Joyce & Andrew E. Bigart, *Liability for All, Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 VAL. U. L. REV. 1481, 1482-83 (2007).

[31] 18 U.S.C. §§ 2701-11 (2008) (outlining requirements for private and public entities seeking to disclose electronic communications including e-mail).

protections for parties seeking to prevent the discovery of electronic materials.[32] The SCA prohibits electronic service providers from releasing the contents of electronic communications unless the communications fall into narrow categories and meet specific consent requirements.[33] Specifically, the SCA balances an individual's reasonable expectation of privacy against the legitimate public need for the disclosure of information such as in a criminal investigation.[34] The SCA often plays a role in employment cases where an electronic service provider is accused of wrongfully divulging electronically stored information and incurs criminal or civil liability.[35] Some observers have argued that case law has done little to clarify the poorly drafted, ambiguous provisions of the SCA.[36]

The SCA adds precision to its rules and terminology by dividing electronic communications into two types: 1) electronic communications systems (ECS) such as radio and computer devices for active communication; and 2) remote computing services (RCS) that process and store electronic communications.[37] One of the first steps in applying the

---

[32] *See* Joyce & Bigart, *supra* note 30, at 1487-91 (arguing revisions to 1986 Electronic Communications Act balanced electronic discovery policy against efficiency concerns).

[33] *Id.* at 1490-91 (acknowledging SCA prohibits provider from "knowingly divulg[ing] the contents of a communication while in electronic storage"). Nevertheless, an electronic communications provider may release such information if the recipient or originator consents. *Id.* Generally, most providers use either "phone manager" or forensic tools to recover text message data, despite the risk of "accidentally" writing data onto a phone in the extraction process. Wayne Jansen, et al., *Overcoming Impediments to Cell Phone Forensics*, 41 Annual Hawaii International Conference on System Sciences (HICSS January 2008), 484, at ¶ 2 (on file with journal). Moreover, deleted text messages are not erased from in the cell phone carrier's system but rather are typically flagged and may be extricated through forensic proprietary software. *Id.* at ¶ 3.2.

[34] *See* Joyce & Bigart, *supra* note 30, at 1485-86 (asserting reasonable expectation of privacy as foundation to Fourth Amendment and federal communications legislation).

[35] *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 910-11 (9th Cir. 2008), (granting plaintiff police officers' motion for judgment as a matter of law) *cert. granted*, City of Ontario v. Quon, 2009 U.S. LEXIS 9058 (U.S. Dec. 14, 2009) (No. 08-1332); Flagg v. City of Detroit, 252 F.R.D. 346, 347 (E.D. Mich. 2008) (declining to find cellular phone service provider violated SCA); Bohach v. City of Reno, 932 F. Supp. 1232, 1236-37 (D. Nev. 1996) (vacating injunction against City and finding no liability under SCA). In *Quon*, two City of Ontario police officers sued the service provider of its employee pagers for releasing text message transcripts in violation of their rights under the SCA and Fourth Amendment. Quon, 529 at 898. The text messages were the subject of an internal affairs investigation regarding the officers' text allocation overages. *Id.* at 897-98. The Ninth Circuit held for the police officers on their Fourth Amendment, state constitutional, and SCA claims. *Id.* at 910-11. The United States Supreme Court accepted the City of Ontario's petition for a writ of certiorari on December 14, 2009. City of Ontario v. Quon, 2009 U.S. LEXIS 9058 (Dec. 14, 2009) (No. 08-1332).

[36] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV.1208, 1208 (2004) (criticizing SCA's lack of clarity and noting interpretational difficulties for legislators, reporters, and scholars).

[37] 18 U.S.C. § 2510(14) (2008); 18 U.S.C. § 2711(2) (2008). An "electronic

SCA is to classify an electronic communication based on its functional use as an ECS, an RCS, or neither.[38] The SCA's definitions are by no means bright line, and therefore determining the type of communication system under the statute is often difficult.[39] Furthermore, the liberal discovery approach of the Rules and SCA adds another level of complexity to electronic discovery standards.[40]

After classifying communication as an ECS or an RCS under the SCA, a court must then determine whether a service provider can release the communications to a third party.[41] If a communication is an active communication device (ECS) rather than mere storage (RCS), then the provider must acquire the lawful consent of both the subscriber and the intended recipient to release the electronic information.[42] If the provider merely stores electronic information, the service is considered an RCS and the provider can lawfully release the information if either the sender or the intended recipient consents.[43] Thus, the standard for releasing RCS

---

communications system," encompasses "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14); *see also Flagg*, 252 F.R.D. at 349 & n. 8 (citing § 2510(14) for ECS definition). In contrast, a "remote computing service" ("RCS"), is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2) (2008); *see also Flagg*, 252 F.R.D. at 349 & n.7 (citing § 2711(2) for RCS definition).

[38] *See* Kerr, *supra* note 36, at 1215-16 (emphasizing difficulties in classifying both communication and recipient type); *see also infra* notes 79, 85-86 (analyzing case law interpreting variations in ECS and RCS categorization).

[39] *See* Kerr, *supra* note 36, at 1215-16 (explaining provider can act as an RCS, an ECS, or neither for the same communications). The provider type depends heavily on the functional usage of the communication. *Id.*

[40] *See id.* at 1229-31 (asserting SCA definitional ambiguities regarding applicability to Internet create compliance difficulties).

[41] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900-01 (9th Cir. 2008) (citing 18 U.S.C. § 2702(a)(2), (b)(3) (categorizing service provider after analyzing SCA definitions)). Generally, the requirements for an RCS provider to release information to a third party are less demanding than the standards for an ECS provider because an RCS provider needs only to obtain the consent of the "subscriber" or the entity contracting with the provider. *Id.* at 901.

[42] *Id.* at 906-07 (reasoning absence of originator and recipient consent violated plaintiffs' constitutional rights). Generally, the Fourth Amendment protects public employees from "unreasonable search and seizure in the workplace." *Id.* at 910.

[43] 18 U.S.C. § 2702(b)(3) (2008) (enumerating exceptions for disclosure of electronic communications). A provider may divulge RCS data with "lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber." *Id.*; *see also* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3d Cir. 2003) (affirming summary judgment because email search fell within § 2701(c) exception). In *Fraser*, the Third Circuit focused on the fact that the e-mails were stored in the defendant employer's computer system in reasoning that the provider satisfied § 2701(c). *Id.* Moreover, the Third Circuit agreed with other circuit courts, holding that as a requisite matter, a communication must fall under the definition of an

information is less stringent than the ECS release requirements; this difference is often at the heart of disputes regarding the release and discovery of such electronic communications.[44] Though these standards may appear relatively straightforward, they are complicated by several exceptions to the SCA, which result in further ambiguity and litigation.[45]

The first broad exception allows a service provider to release stored electronic communications, such as RCS data, to an employee or to an individual who is incidentally or institutionally authorized to view them.[46] The second SCA exception permits the service provider to release stored information if to do so is in the provider's normal course of business.[47] The SCA also includes several exceptions for valid warrants and administrative subpoenas.[48] These release requirements depend on the duration of the information storage.[49] If a service provider stores text message data for six months or more, a government entity can utilize additional means of release authorization, including administrative subpoenas or court orders.[50] Finally, if the service provider stores text

---

"electronic communication" in order for an unlawful interception to occur under the SCA. *Id.* at 114. *See* Joyce & Bigart, *supra* note 30, at 1490-91 (noting distinctly different standards for ECS and RCS disclosure).

[44] *See infra* Part IV and accompanying text (observing emerging case law trends interpreting SCA and Rules in context of text message discovery).

[45] *See* cases cited *supra* note 6 and accompanying text (identifying federal civil cases involving text message discovery disputes).

[46] *See* 18 U.S.C. § 2702(b) (2008); *see also* Joyce & Bigart, *supra* note 30, at 1490-91 (citing 18 U.S.C. § 2702(b)) (noting consent exception to SCA allows disclosure to third parties).

[47] *See* 18 U.S.C. § 2702(b)(5) (allowing disclosure of electronic materials in provider's ordinary course of business). The statute defines the ordinary course of business as instances where the provider "engag[es] in any activity which is necessarily incident to the rendition of service or to protect the rights . . . of the provider." Joyce & Bigart, *supra* note 30, at 1491 (citing 18 U.S.C. § 2702(b)(5)).

[48] Joyce & Bigart, *supra* note 30, at 1490-91 (observing relaxed release requirements for electronic communications under government subpoena or administrative order).

[49] *See* 18 U.S.C. § 2702(b); *see also* Joyce & Bigart, *supra* note 30, at 1491 (citing 18 U.S.C. § 2703(b)) (explaining broad service provider disclosure conditions for law enforcement officers seeking to obtain stored data). The SCA distinguishes between information stored for less than six months and information stored for longer than six months:

> Additionally, a service provider must disclose electronic communications to a governmental entity pursuant to a warrant for communications stored for six months; for communications stored longer than six months, the service provider must disclose the communications to a governmental entity with a warrant or if the government entity provides prior notice to the subscriber and either (1) uses an administrative subpoena authorized by a federal or state statute or a federal or state grand jury; or (2) obtains a court order for the disclosure.

Id. (citing 18 U.S.C. § 2703).

[50] Joyce & Bigart, *supra* note 30 at 1491 (requiring notice to subscriber in subpoena in

message or pager information about the commission of a crime or an impending emergency involving death or serious injury, the provider may divulge the information regardless of consent.[51] A service provider may assert these SCA exceptions as defenses to the claims for the unlawful release of electronic communications.[52]

These complex definitions lie against the backdrop of the Fourth Amendment, which plays a crucial role in most claims that have been brought under the SCA and as part of motions to quash discovery requests.[53] Based on the legislative record and the ever-increasing role of electronic communications, the amended Rules and the SCA represent a recognition of the need for more transparent discovery rules for electronic materials.[54] The Rules provide the general basis for determining whether the electronic information is discoverable, and the SCA and its various exceptions lay out potential defenses to criminal and civil liability for providers such as cell phone companies.[55] The majority of parties seeking to suppress cell phone or pager data have argued that releasing the information would violate their reasonable expectation of privacy implicit in the Fourth Amendment.[56] Some providers inadvertently find themselves

---

addition to warrant). The governmental entity must also disclose any "inadvertently obtained" communications to the cellular services provider. *Id.*

[51] *See* 18 U.S.C. § 2702(b)(8); *see also* Joyce & Bigart, *supra* note 30, at 1491 (detailing varying consent requirements for lawful divulgence of cell phone data).

[52] *See* Kerr, *supra* note 36, at 1241 (identifying lack of case law involving criminal punishment for SCA violations). SCA claims most commonly arise in the civil context rather than in criminal cases, which further adds to the statute's ambiguity. *Id.*

[53] *See* Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 389-392 (2009) (analyzing liability of third-party cellular providers under SCA and Fourth Amendment); *see also infra* notes 56-60 and accompanying text (outlining vague standards for establishing reasonable right to privacy embodied in SCA and Fourth Amendment).

[54] *See supra* notes 32-33, 40 and accompanying text (explaining need for revisions to text message discovery rules).

[55] *See supra* notes 46-50 and accompanying text (discussing enumerated exceptions for permissible discovery of electronic data).

[56] *See, e.g.*, Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (advocating use of reasonable expectation of privacy analysis in holding government's electronic listening device in phone booth violated Fourth Amendment); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 903, 908-09 (9th Cir. 2008) (holding divulgence of text messages unconstitutional and in violation of SCA); Adams v. City of Battle Creek, 250 F.3d 980, 984, 986 (6th Cir. 2001) (distinguishing facts from *Bohach* and finding production of pager text data statutorily permitted); Flagg v. City of Detroit, 252 F.R.D. 346, 352 n.14 (E.D. Mich. 2008) (explaining court's attempt to "implement a protocol that protects against overbroad disclosure of communications" based on *Quon*); Bohach v. City of Reno, 932 F. Supp. 1232, 1235 (D. Nev. 1996) (finding production of employee pager text messages did not violate employees' Fourth Amendment rights). *But cf.* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 109 (3d Cir. 2003) (allowing discovery of electronic data based on SCA exception criteria); Ideal Aerosmith, Inc. v.

in legal disputes because they often possess text message or pager data in which both parties have a strong interest.[57]

III. CONFLICTING CASE LAW REGARDING ELECTRONIC DISCOVERY

In addition to case law involving the Rules and the SCA, *Katz v. United States*[58] provides well-accepted standards for determining the bounds of the government's surveillance powers and evaluating a claimant's reasonable expectation of privacy.[59] The *Katz* Court laid the foundation for future courts to reject the premise that a public employee lacks a reasonable expectation of privacy in communication devices provided by his or her employer.[60] Though *Katz* was decided decades

---

Acutronic USA, Inc., No. 07-1029, 2008 U.S. Dist. LEXIS 33463, at *8-9 (W.D. Pa. Apr. 23, 2008) (interpreting SCA absent Fourth Amendment challenge); Auto Club Family Ins. Co. v. Ahner, No. 05-5723, 2007 U.S. Dist. LEXIS 63809, at *9-11 (E.D. La. Aug. 29, 2007) (requiring production of former insurance agent's electronic data based on Rule 45(c)); Modern Eng'g, Inc., v. Peterson, No. 07-CV-1055, 2007 U.S. Dist. LEXIS 51131, at *6-7 (C.D. Ill. July 16, 2007) (allowing in part plaintiff's motion to compel discovery in absence of constitutional claim); Scotts Co. v. Liberty Mut. Ins. Co., No. 2:06-CV-899, 2007 U.S. Dist. LEXIS 43005, at *4-6 (S.D. Ohio June 12, 2007) (basing ruling solely on amended Rules).

[57] *See, e.g.*, *Bohach*, 932 F. Supp. at 1237 (holding plaintiff employees' text messages discoverable in lawsuit against City and service provider); *Quon*, 529 F.3d at 904-06 (concluding City and service provider violated police officers' reasonable expectation of privacy by releasing text message data); *Flagg*, 252 F.R.D. at 347 (ruling *in camera* examination of text message data proper in plaintiff's suit against employer and service provider).

[58] 389 U.S. 347, 358-59 (1967).

[59] *See id.* at 360 (Harlan, J., concurring) (maintaining violations of Fourth Amendment reasonable expectation of privacy need not involve physical acts). In *Katz*, the United States Supreme Court reasoned that an F.B.I. wiretapping procedure violated the defendant's Fourth Amendment Rights and "reasonable expectation of privacy." *Id.* at 360-61. Katz and its progeny have created a formal framework for determining whether an employee has a "reasonable expectation of privacy" through a two-part test that requires "(1) an 'actual (subjective) expectation of privacy' and (2) an expectation 'that society is prepared to recognized [sic] as reasonable,' or 'justifiable under the circumstances.'" Mindy C. Calisti, *You Are Being Watched: The Need for Notice in Employer Electronic Monitoring*, 96 KY. L.J. 649, 651 (2007-2008) (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)). Though the *Smith* Court established the majority rule for public employee privacy claims, a minority of jurisdictions continue to maintain that public employees lack a reasonable expectation of privacy because they do not have a "possessory interest in the workplace." *Id.* at 652. It is important to note that although Fourth Amendment challenges typically must involve a state actor, the "reasonable expectation of privacy" analysis determines private employees' level of privacy and allows courts to evaluate the policy reasoning behind the current privacy standards. *Id.*

[60] *See Katz*, 389 U.S. at 351-54 (articulating reasonable expectation of privacy analysis based on First and Fourth Amendments); Quon, 529 F.3d at 904-06 (holding release of text message data violated employees' reasonable expectation of privacy); *see also* Herbert, *supra* note 3, at 57 (2008) (identifying "gap between perception and legal reality" regarding employee privacy). Generally, privacy rights for employee e-mail and other electronic communications are

before cell phones and pagers came into common use, the case provided the necessary basis for subsequent cases holding that a public employee claiming a violation of his Fourth Amendment rights or his rights under the SCA must first establish his reasonable expectation of privacy.[61]

In addition to addressing employees' constitutional claims, prior to the passage of the SCA, federal courts faced complex issues surrounding the discovery of electronic materials not easily discoverable in hard copy form.[62] In *Bohach v. City of Reno*,[63] the United States District Court for the District of Nevada focused on the location and nature of the electronic information in determining whether the text messages stored on city pagers were discoverable.[64] Police officers Bohach and Catalano were the subjects of an internal affairs investigation in part based on their alleged abuse of the City's Alphapage system.[65] In deciding to apply the stored electronic information release standard (RCS) rather than the active electronic transmission rule (ECS), the court focused on the fact that the City itself was the service provider and allowed easy access to nearly all employees in its normal course of business.[66] As a preliminary matter, the court required the officers to prove they had a "reasonable expectation of privacy" as a basis for their 42 U.S.C. § 1983 and Fourth Amendment claims.[67] *Bohach* was one of the earliest cases addressing privacy and discovery issues in electronic communication device data.[68] Recently, several courts have relied on the *Bohach* Court's approach to classifying electronic communications and determining whether an individual had a

---

"minimal." *Id.*

[61] *See* Herbert, *supra* note 3, at 57 (noting inaccurate perceptions of employee privacy). *But see* Calisti, *supra* note 59, at 652 (noting minority of jurisdictions have declined to recognize public employees' reasonable expectation of privacy).

[62] *See Bohach* 932 F. Supp. at 1236 (evaluating government disclosure of pager data prior to passage of SCA and amended Rules); *see also* Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001) (seeking guidance from *Bohach* opinion several years before amendments to Rules and SCA); Walden v. City of Providence, 495 F. Supp. 2d 245, 261 (D.R.I. 2007) (characterizing *Adams* holding as declining to decide constitutional issue where not absolutely necessary).

[63] 932 F. Supp. 1232, 1237 (D. Nev. 1996) (ruling on discoverability of text messages on employees' pagers).

[64] *Id.* at 1237 (denying plaintiffs' motion to enjoin City of Reno from releasing text message data).

[65] *Id.* at 1235 (reasoning plaintiffs' expectation of privacy not reasonable in part because city's central computer system was widely accessible).

[66] *Id.* (noting all members of police department had easy access to electronic pager information without password).

[67] *Id.* at 1234 (summarizing claimants' civil rights and Fourth Amendment claims resulting from release of text message data).

[68] *See* cases cited *infra* notes 95 (observing cases recognizing *Bohach* as an early leading case).

reasonable expectation of privacy.[69]

Though *Bohach* is a prominent text message data case, the most often-cited case addressing the discoverability of text messages and pager data is *Quon v. Arch Wireless Operating Co.*[70] In holding that the audit of the plaintiff police officers' cell phones and pagers was improper, the Ninth Circuit drew an analogy between text messages and e-mail to find that the officers had a reasonable expectation of privacy based on the precedent in *Katz*.[71] The Ninth Circuit emphasized that the transmission of text messages constituted an ECS, and thus the release of text message information required the consent of both the subscriber and the intended recipient.[72] Several courts have acknowledged the scarcity of case law interpreting the SCA in the electronic discovery context and have looked to *Quon* for guidance.[73] *Quon* has to some extent clarified the ambiguity surrounding text message discovery, yet new cases are emerging at a rapid pace that complicate the already inconsistent landscape surrounding text message discovery standards.[74]

Though the case law involving text message and pager data is

---

[69] *See* cases cited *infra* note 95 (analyzing federal case law citing to *Bohach*); *see also* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3d Cir. 2003) (analogizing *Bohach* reasoning to discoverability of employee e-mail). "Like the court in *Bohach*, we read § 2701(c) literally to except from Title II's protection all searches by communications service providers." *Id.* at 115.

[70] 529 F.3d 892, 910-11 (9th Cir. 2008); *see* cases cited *infra* note 96 and accompanying text (identifying civil cases relying on *Quon* holding); Miller *supra* note 5, § 8 (identifying *Quon* as leading case for electronic discovery disputes involving text messages).

[71] *Quon*, 529 F.3d at 903-06 (identifying *Katz* and its progeny as foundational for Fourth Amendment challenges involving interception of communications).

[72] *See id.* at 900-01 (rejecting lower court's characterization of text messages as RCS data); Heather Wolnick, Case Summary, *The Extension of Privacy Rights to the Workplace Text Messages Under* Quon v. Arch Wireless, 39 GOLDEN GATE U. L. REV. 351, 357-59 (2009) (analyzing Ninth Circuit's reasoning regarding ECS/RCS distinction under SCA); *supra* note 41-43 and accompanying text (explaining text message disclosure requirements and exceptions for ECS and RCS providers).

[73] *See* Louis Vuitton Malletier v. Akanoc Solutions, Inc., No. C 07-03952 JW, 2008 U.S. Dist. LEXIS 63115, at *3-4 (N.D. Cal. Aug. 7, 2008) (overruling objection to producing computer server data based on SCA and *Quon*'s distinction between service providers and interceptors); Hone v. Presidente U.S.A., Inc., No. C08-80071 JF (HRL), 2008 U.S. Dist. LEXIS 55722, at *3-6 (N.D. Cal. July 21, 2008) (applying SCA consent exceptions discussed in *Quon* to grant plaintiff's motion to quash subpoena of personal e-mail); Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. 07-1029, 2008 U.S. Dist. LEXIS 33463, at *11-14 (W.D. Pa. Apr. 23, 2008) (contrasting facts to *Quon* to interpret SCA in determining whether reading competitors' stored e-mails violated trade secret law); *see also* Joyce & Bigart, *supra* note 30, at 1495 (extolling *Quon* as "one of the most comprehensive discussions" of text message discovery standards); cases cited *infra* note 96 (identifying and analyzing recent cases relying on *Quon* in electronic discovery disputes).

[74] *See* Flagg v. City of Detroit, 252 F.R.D. 346, 363 & n.29 (E.D. Mich. 2008) (admitting court was "puzzled" by *Quon*'s application of the facts to SCA); cases cited *infra* note 96 (summarizing recent cases involving text message discovery disputes that cited to *Quon*).

sparse and somewhat limited to employment claims, the jurisprudence in this area continues to evolve with a keen focus on the active or passive nature of the service provider.[75] Recent cases such as *Flagg v. City of Detroit*,[76] demonstrate the importance of electronic discovery to cases in which an employee alleged violation of federal law and his or her Fourth Amendment rights based on a cellular service provider's disclosure of text message data.[77] In ruling that the Magistrate Judge could properly examine the City employees' text message data *in camera*, the court in *Flagg* reasoned that under the amended Rule 34(a), prohibiting such discovery would run contrary to decades of case law encouraging the open discovery of relevant materials.[78] Though the *Flagg* Court explicitly relied on the *Quon* holding, it arrived at an opposite conclusion because it determined that the communications at issue fell under the RCS definition and therefore the less stringent consent requirement applied.[79] These discovery standards remain blurry, and only a handful of relevant civil cases help to clarify them.[80]

IV. APPLICATION OF SCA AND FEDERAL RULES OF CIVIL PROCEDURE TO CONFLICTING CASE LAW

Though the SCA assigns criminal liability for disclosing stored electronic information such as text message data, the Act has been cited almost exclusively in employment cases.[81] Moreover, as of 2009, no federal court has categorically barred the discovery of text messages and pager data; most courts have taken the liberal approach to discovery embodied in the Rules.[82] In general, cases involving the disclosure of

---

[75] *See infra* Part IV (identifying and discussing patterns in case law); Herbert *supra* note 3, at 103-04 (noting public employees enjoy greater Fourth Amendment protection than private employees). Typically, Fourth Amendment protections do not apply to private employers and this key difference decreases a private employee's expectation of privacy. *See id.*

[76] 252 F.R.D. 346 (E.D. Mich. 2008).

[77] *Id.* at 346-47 (declining to interpret SCA broadly enough to prohibit relevant lawful discovery).

[78] *Id.* at 347 (emphasizing electronic materials in possession and control of opposing party are "plainly" subject to discovery).

[79] *Id.* at 359 n.24 (distinguishing ECS and RCS definition rules and emphasizing role of service provider). In contrast to a situation involving an ECS provider, an RCS provider need only obtain the consent of either the subscriber or the intended recipient to release the electronically stored data. *Id.* at 349-50.

[80] *See infra* Part IV (describing diverging trends in case law involving text message discovery).

[81] *See infra* notes 88-89 and accompanying text (observing two distinct case law trends in discovery of text message and pager data).

[82] *See infra* notes 85-89 and accompanying text (categorizing federal courts' approaches to

employee text messages seem to employ solid legal reasoning, yet a closer look reveals inconsistencies among cases involving similar facts.[83]

The 2006 Amendments to the Rules embraced pragmatism and sought to provide adequate guidance for courts ruling on electronic discovery issues.[84] Due to the liberal nature of the Rules, text message discovery challenges based on the Rules tend to favor discoverability when employing both Rules 34 and 45.[85] In general, the Rules have not constituted the type of roadblock that many objecting parties may seek.[86]

Though case law interpreting standards for discovering text messages and pager data is in its nascent stages, two distinct trends have emerged.[87] The first group of cases involves public employees filing claims against public entities based on the SCA and the Fourth Amendment.[88] The second line of cases pertains to private employees

---

text message discovery based on SCA, Rules, and Fourth Amendment); *cf.* Quon v. Arch Wireless Operating Co., 529 F.3d 903, 910-11 (9th Cir. 2008) (determining service provider's release of cell phone data improper due to lack of consent). Though the Ninth Circuit determined that the release of the plaintiffs' cell phone data violated the Constitution and federal law, the court noted that "at the time of the search, there was no clearly established law regarding whether users of text-messages that are archived, however temporarily, by the service provider have a reasonable expectation of privacy in those messages." *Id.* at 910.

[83] *See* Flagg v. City of Detroit, 252 F.R.D. 346, 366-67 (E.D. Mich. 2008) (allowing magistrate judge to inspect public employee's cell phone data). *But see Quon*, 529 F.3d at 910-11 (holding City's inspection of police officers' text message data violated officers' Fourth Amendment rights); Justin Conforti, Comment, *Somebody's Watching Me: Workplace Privacy Interests, Technology, Surveillance, and the Ninth Circuit's Misapplication of the* Ortega *Test in* Quon v. Arch Wireless, 5 SETON HALL CIRCUIT REV. 461, 467-469 (2009) (asserting *Quon* holding indicative of trend of upholding employee privacy in electronic communications).

[84] *See* Marcus, *supra* note 19, at 330-33 (describing Advisory Committee process for drafting electronic discovery rules to create acceptable concrete standards).

[85] *See* Thielen v. Buongiorno USA, Inc., No. 1:06-CV-16, 2007 U.S. Dist. LEXIS 8998, at *7-9 (W.D. Mich. Feb. 8, 2007) (granting defendant's forensic expert access to text message database using liberal discovery rules); *see also* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3d Cir. 2003) (applying exception allowing employer to lawfully disclose employee's communications in finding no SCA violation; Modern Eng'g, Inc. v. Peterson, No. 07-CV-1055, 2007 U.S. Dist. LEXIS 51131, at *6-7 (C.D. Ill. July 16, 2007) (requiring defendant to produce transmitted electronic information including text message data).

[86] *See Flagg*, 252 F.R.D. at 354-58, 366-67 (allowing magistrate judge to inspect text data despite employees' objections based on Rules and SCA).

[87] *See infra* notes 88-89 and accompanying text (separating text message and pager discovery disputes into two categories based on discovery objection).

[88] *See, e.g.*, *Quon* 529 F.3d at 910-11 (determining City violated SCA and police officers' Fourth Amendment rights by releasing text message data); Adams v. City of Battle Creek, 250 F.3d 980, 984, 986 (6th Cir. 2001) (declining to rule on Fourth Amendment and federal claims for monitoring of employee's clone pager); *Flagg*, 252 F.R.D. at 354-58, 366-67 (applying liberal discovery approach of Rules and granting magistrate judge access to city employee's cell phone and pager data); Black v. City & County of Honolulu, 112 F. Supp. 2d 1041, 1054 (D. Haw. 2000) (denying summary judgment in favor of City due to illegal wiretapping of employee's pager); Bohach v. City of Reno, 932 F. Supp. 1232, 1237 (D. Nev. 1996) (ruling in favor of

attempting to bar discovery of text message data based on the burden of discovery standard in the Rules, coupled with privacy concerns.[89] If these case law patterns persist, the public and private employee cases will likely continue to diverge and text message discovery issues will be handled in a piecemeal fashion until these types of disputes become more commonplace.[90]

A. Public Employee Objections to Discovery of Text Message Data

An exhaustive search of the available federal case law regarding the discoverability of text messages yielded only five civil cases involving text message discovery disputes with public entities, all of which rely on precedent from disparate federal courts.[91] Interestingly, all five cases involved an investigation of a public employee's text message use that precipitated an employee's allegations of an Fourth Amendment or SCA violation to block the release of text message data by a service provider.[92] The *Bohach* case was one of the earliest federal civil cases to rule on proper disclosure standards for text message data.[93] In finding against the plaintiff police officers, the Nevada District Court focused on the provider's role in storing the data and the employees' inability to meet their burden in showing a reasonable expectation of privacy.[94] Several other cases involving public employees' claims against municipal entities have

---

defendant that text messages sent by City public employees were discoverable).

[89] *See, e.g.*, *Fraser*, 352 F.3d at 115 (citing SCA exception and ruling defendant private employer could lawfully disclose employee's electronic communications); Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. 07-1029, 2008 U.S. Dist. LEXIS 33463, at *8-12 (W.D. Pa. Apr. 23, 2008) (ruling defendant not bound by SCA disclosure provisions in trade secrets claim involving private employee e-mail); *Modern Eng'g*, 2007 U.S. Dist. LEXIS 51131 at *6-8 (clarifying specific electronic documents that defendant employee must produce in conjunction with trade secrets claim); *Thielen*, 2007 U.S. Dist. LEXIS 8998 at *7-8 (allowing forensic expert access to text message and e-mail data relevant to class action lawsuit).

[90] *See* Isom, *supra* note 1, at ¶ a.1 (noting exponential increase in electronic information necessitating clarification of electronic discovery standards); *see also Ideal Aerosmith*, 2008 U.S. Dist. LEXIS 33463 at *8-9 (observing dearth of cases interpreting SCA).

[91] *See* cases cited *supra* note 88 and accompanying text (listing public employee text message discovery disputes); *see also* Miller, *supra* note 5, §§ 4-5 (compiling list of criminal and civil cases involving text message disclosure). Criminal cases comprise the large majority of cases that involve text message or pager data disputes. *Id.*

[92] *See* cases cited *supra* note 88 and accompanying text (analyzing cases in which employees brought claims against public entities).

[93] *See Bohach*, 932 F. Supp. at 1235-36 (noting pager system administered entirely by City render facts distinguishable from other cases).

[94] *Id.* at 1234-35 (asserting officers' low likelihood of success in prevailing on Fourth Amendment claims); *see also* Miller *supra* note 5, § 9 (emphasizing *Bohach* court found subjective rather than objective expectation of privacy in its ruling).

cited directly to *Bohach* in determining whether text message and pager data was within the proper scope of discovery.[95]

Quon is a public employee case with a complex, far-reaching holding that several federal courts have relied upon in ruling on text message classification types and release standards.[96] The fact-specific nature of the claims and the lack of definitive standards for determining communication provider types under the SCA explain the stark contrast in policy reasoning between *Bohach* and *Quon*.[97] Moreover, a majority of federal cases have cited *Bohach* or *Quon* when deciding a substantive issue of cell phone and pager disclosure.[98]

Few cases involving public employee discovery disputes have drawn upon the Rules, the SCA, and the Fourth Amendment.[99] Interestingly, in *Flagg*, the Michigan District Court acknowledged the *Quon* holding, yet concluded that *Quon's* reasonable privacy analysis was inapplicable because the plaintiff did not assert a Fourth Amendment claim.[100] The conflicting precedent in *Quon* and *Flagg* illuminates the challenges United States District Courts face when confronting text

---

[95] *See* Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001) (relying on *Bohach* in analyzing employee's Fourth Amendment claim); Walden v. City of Providence, 495 F. Supp. 2d 245, 260 (D.R.I. 2007) (following *Adams* approach to Fourth Amendment in denying City's motion for summary judgment).

[96] *See* Louis Vuitton Malletier v. Akanoc Solutions, Inc., No. C 07-03952 JW, 2008 U.S. Dist. LEXIS 63115, at *3 (N.D. Cal. Aug. 7, 2008) (citing *Quon* in analyzing SCA distinction between intercepting electronic data and providing communications and storage); Hone v. Presidente U.S.A., Inc., No. C08-80071 JF (HRL), 2008 U.S. Dist. LEXIS 55722, at *3-6 (N.D. Cal. July 21, 2008) (citing *Quon* in applying SCA's ECS and RCS consent exceptions).

[97] *Compare* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 897 (9th Cir. 2008) (noting defendant city had informal policy allowing for public disclosure of personal data), *with Bohach* 932 F. Supp. At 1234-35 (vitiating reasonable expectation of privacy claim based on public accessibility to electronic pager data). The *Quon* court also distinguished the level of privacy protection applicable to the claimants' e-mail and computer files from stored text and pager data. *Quon*, 529 F.3d at 902-03. The Ninth Circuit noted that the Oakland Police Department had a formal written policy warning against public disclosure of e-mail and computer files but no formal policy on pager data disclosure. *Id.* at 897; *see also* Miller *supra* note 5, § 8 (asserting cases such as *Quon* "appealed to broad societal norms" in evaluating reasonable expectation of privacy).

[98] *See supra* notes 95-96 (observing two cases discussing *Bohach* and two cases citing to *Quon*).

[99] *See* Flagg v. City of Detroit, 252 F.R.D. 346, 361-63 (E.D. Mich. 2008) (combining disclosure standards of Rules and SCA consent rules for RCS providers). The district court's creative approach forged a compromise authorizing a magistrate judge to review the text message data *in camera*. *Id.* at 362-63.

[100] *Id.* at 351 & n.13 (relying on *Quon* to conclude that text message data is narrowly discoverable). The *Flagg* court also declined to adopt *Quon*'s Fourth Amendment reasoning in finding the text message data subject to discovery. *Id.* However, the court later noted that *Quon* aligns with its effort to "implement a protocol that protects against overbroad disclosure of [employee] communications." *Id.* at 352 n.14.

message disclosure issues for the first time given that the decisions of other federal courts are merely persuasive rather than precedential.[101] Furthermore, federal courts face a dearth of case law interpreting the Rules in the context of SCA claims, which results in creative solutions that may be workable for the case at bar, yet too case-specific to provide future guidance.[102]

B. Private Employee Claims Against Private Entities

The claims of a private employee objecting to the disclosure of text message data are inherently distinct from the claims of a public employee, yet private employers confront similar challenges with regard to text message disclosure.[103] Indeed, despite the inherent differences, several private employment cases have relied on *Quon* and *Bohach* in an effort to find clarity.[104] There are fewer private employment cases involving objections to text message disclosure than public employment cases, which largely rely on the Rules to resolve discovery disputes rather than the SCA or the Fourth Amendment.[105]

Another potential trend in text message and pager data jurisprudence is the tendency of courts to reason by analogy to e-mail and

---

[101] *See* Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. 07-1029, 2008 U.S. Dist. LEXIS 33463, at *8-9 (W.D. Pa. Apr. 23, 2008) (noting scarcity of civil case law addressing preemption in electronic discovery).

[102] *See Flagg*, 252 F.R.D. at 362-63 (entrusting magistrate judge with review of text message communications).

[103] *See* Herbert, *supra* note 3, at 51 ("The integration of employer computers with personal electronic communication devices is creating complex legal issues regarding the balance between employee and employer rights and legal responsibilities."); *see also* Joyce & Bigart, *supra* note 30, at 1481 (noting cell phones and e-mail have become "ubiquitous" in modern society).

[104] *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3d Cir. 2003) (analogizing case to *Bohach* holding regarding service provider exception for electronically stored text data); Louis Vuitton Malletier v. Akanoc Solutions, Inc., No. C 07-03952 JW, 2008 U.S. Dist. LEXIS 63115, at *3-4 (N.D. Cal. Aug. 7, 2008) (following *Quon* approach of distinguishing service provider from interceptor of publicly available communications); Hone v. Presidente U.S.A., Inc., No. C08-80071 JF (HRL), 2008 U.S. Dist. LEXIS 55722, at *3-4 (N.D. Cal. July 21, 2008) (applying *Quon* test to define service provider type under SCA); *Ideal Aerosmith*, 2008 U.S. Dist. LEXIS 33463, at *10-13 (engaging in lengthy discussion of *Quon* preemption reasoning).

[105] *See, e.g.*, Auto Club Family Ins. Co. v. Ahner, No. 05-5723, 2007 U.S. Dist. LEXIS 63809, at *9-11 (E.D. La. Aug. 29, 2007) (relying on Rules 34 and 45 to compel defendant to produce electronic information); Modern Eng'g, Inc. v. Peterson, 2007 U.S. Dist. LEXIS 51131, at *6-8 (C.D. Ill. July 16, 2007) (looking exclusively Rule 34 in resolving electronic discovery dispute); Thielen v. Buongiorno USA, Inc., No. 1:06-CV-16, 2007 U.S. Dist. LEXIS 8998, at *4-6 (W.D. Mich. Feb. 8, 2007) (citing only to Rules in allowing limited discovery of plaintiff's electronic communication devices).

telephone recordings.[106] The cases that have arisen outside of the employment law context seem to focus almost exclusively on the Rules in resolving text message discovery disputes, as do cases involving e-mail and electronic wiretapping.[107] Based on the modern trend towards increased cell phone and text message use in the workplace and in private life, the need for definitive discovery standards persists.[108]

C. *Trends in Application of SCA Definitions in Text Message Cases and Implications for Fourth Amendment Claims*

The majority of text message discovery disputes in federal court have involved claims of civil liability under the SCA against an adverse or third party service provider.[109] Though the legislative intent of the SCA was to protect citizen's electronic communications privacy through criminal penalties and civil liability, the Act has been mired by inconsistent applications of the consent standards for ECS and RCS providers.[110] Determining the lawfulness of releasing stored text message or pager data often turns on whether the court categorized the service provider as an RCS or an ECS.[111] However, rather than analyze factual situations according to provider type within the RCS and ECS framework of the SCA, many courts have employed unique terminology outside the SCA's statutory definitions including "interceptor" and "provider."[112] The use of these terms instead of

---

[106] *See, e.g.*, Scotts Co. v. Liberty Mut. Ins. Co., No. 2:06-CV-899, 2007 U.S. Dist. LEXIS 43005, at *4-9 (S.D. Ohio June 12, 2007) (relying on e-mail discovery precedent to resolve motion to compel electronic information including text messages); *Louis Vuitton Malletier*, 2008 U.S. Dist. LEXIS 63115, at *3-4 (requiring defendant to produce website transactions pertaining to offers to sell counterfeit goods); *Hone*, 2008 U.S. Dist. LEXIS 55722, at *3-6 (applying e-mail implications of Rule 45 and *Quon* in granting plaintiff's motion to quash).

[107] *See* cases cited *supra* note 105 and accompanying text (identifying discovery disputes pertaining to text messages outside public employment context).

[108] *See supra* note 103 and accompanying text (noting prominent role of electronic communications and cell phones in modern life).

[109] *See generally* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 895 (9th Cir. 2008); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 109 (3d Cir. 2003); Adams v. City of Battle Creek, 250 F.3d 980, 982 (6th Cir. 2001); Flagg v. City of Detroit, 252 F.R.D. 346, 347 (E.D. Mich. 2008); *Louis Vuitton Malletier*, 2008 U.S. Dist. LEXIS 63115, at *1-2; *Hone*, 2008 U.S. Dist. LEXIS 55722, at *1-2; *Ideal Aerosmith*, 2008 U.S. Dist. LEXIS 33463, at *1-2.

[110] *See supra* notes 37-43 and accompanying text (explaining ECS and RCS definitions and varying consent requirements).

[111] *See, e.g.*, *Quon*, 529 F.3d at 901 (illustrating differences between ECS and RCS standards); *Flagg*, 252 F.R.D. at 349 (emphasizing ECS and RCS distinction in determining properness of disclosure); *Hone*, 2008 U.S. Dist. LEXIS 55722, at *2 (concluding defendant Yahoo! functioned as ECS and was thus subject to heightened consent standard).

[112] *See, e.g.*, *Adams*, 250 F.3d at 982-83 (exploring definitions of "intercept" within statutory context); *Flagg*, 252 F.R.D. at 364 (holding RCS provider may intercept communications with

the precise language of the SCA creates yet another potentially contentious question of fact for parties to litigate.[113] Though the "provider" and "interceptor" terms seem less technical and understandable to those unfamiliar with the statute, these deviations exacerbate the SCA's ambiguities and inconsistencies.[114]

In addition to the unpredictable application of the SCA terms, Fourth Amendment claims provide another analytical twist in the meandering path towards resolving text message discovery disputes.[115] Of the claimants that relied on the SCA to prevent the disclosure of text information, roughly half of them asserted a Fourth Amendment claim based on the actions of a state actor or a private entity carrying out a public function.[116] Though the constitutional case law on text message disclosure is relatively sparse, the federal courts have relied on *stare decisis* to quickly dispense with a Fourth Amendment claim.[117] The SCA's protections against the unlawful search and seizure of electronic communications are more extensive than the rights embodied in the Fourth Amendment, which partially explains this trend in the case law.[118] Furthermore, a party seeking

---

consent of one or more intended recipients); *Louis Vuitton Malletier*, 2008 U.S. Dist. LEXIS 63115, at *3-4 (asserting interception of publicly available documents did not create liability under SCA); *see also Fraser*, 352 F.3d at 113-14 (recounting history of term "intercept" in federal communications law). In addition to the case law interpreting the SCA's definition of "intercept," numerous cases have also explored the definition of "intercept" under the Electronic Communications Privacy Act 18 U.S.C. § 2510(4) (2008). *See id.*

[113] *Fraser*, 352 F.3d at 115 (concluding release of employee's electronically stored data lawful without applying ECS and RCS consent standards); *Adams*, 250 F.3d at 986 (determining production of pager data proper irrespective of ECS and RCS distinctions); *Louis Vuitton Malletier*, 2008 U.S. Dist. LEXIS 63115, at *3-4 (discussing provider and interceptor distinction independent of ECS and RCS consent requirements).

[114] *See Quon*, 529 F.3d at 906 ("We do not endorse a monolithic view of text message users' reasonable expectation of privacy, as this is necessarily a context-sensitive inquiry.").

[115] *See supra* notes 56, 58-60 and accompanying text (summarizing Fourth Amendment claims in text message and pager data cases).

[116] *Compare Quon*, 529 F.3d at 910-11 (asserting service provider violated SCA by releasing employees' text message data during internal affairs investigation), *with supra* notes 56, 58-60 and accompanying text (identifying common arguments in Fourth Amendment challenges to production of text message and pager data).

[117] *See Adams*, 250 F.3d at 986 (denying constitutional claims and noting parties did not argue SCA protections differed from Fourth Amendment); Walden v. City of Providence, 495 F. Supp. 2d 245, 261 (D.R.I. 2007) (declining to rule on Fourth Amendment claims where not absolutely necessary). *But see Quon*, 529 F.3d at 910-11 (finding release of police officers' text message data violated both U.S. and California constitutions).

[118] *See* Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. 07-1029, 2008 U.S. Dist. LEXIS 33463, at *4-16 (W.D. Pa. Apr. 23, 2008) (engaging in lengthy discussion of SCA preemption). The Pennsylvania District Court in *Ideal Aerosmith* emphasized that its reasoning was consistent with the Ninth Circuit in *Quon* because the SCA did not preempt state communications law through conflict, express, or field preemption. *Id.* at *13 & n.2.

to prevent the disclosure of text message data has an arsenal of defenses including the Rules, federal statues, the United States Constitution, and state constitutions to protect his or her interests amidst the unpredictable landscape of electronic discovery disputes.[119]

VI. CONCLUSION

As text messages become integral to personal and workplace communication, cases challenging production of text message data based on the Rules, the SCA, and the Fourth Amendment will become increasingly prevalent. In particular, employment cases will continue to provide fruitful grounds for litigation involving text message disclosure. Case law regarding text messages is largely undeveloped, leaving an expansive canvas upon which future courts may craft the jurisprudence in this area. Furthermore, several federal courts have noted that the myriad ambiguities in this area will continue to plague electronic discovery disputes until an adequate body of case law emerges.

The ECS and RCS disclosure standards, in the context of SCA, provide a modicum of guidance to courts faced with text message discovery disputes, yet in practice, the ECS and RCS definitions are overly broad. Revisions to § 2701 of the SCA, specifically applying to text messages and other electronically stored information such as metadata, would ameliorate some of these inconsistencies. For example, provisions differentiating e-mail and text message disclosure consent standards would help to guide litigators encountering these issues for the first time. Moreover, given that the SCA was initially intended to prescribe criminal liability for unauthorized disclosure of electronically stored information, the statute's almost exclusive application in civil employment disputes demonstrates a fundamental disconnect between the statute's purpose and its impact. Clarity can only be achieved through legislative revision until more robust case law or legislation develops.

Along with revisions to the SCA, adopting official comments to Rules 26, 34, and 45, addressing the scope of issues relating to the discovery of text messages would provide much needed guidance. Third parties such as cellular service providers are often named as parties to lawsuits involving improper text message disclosure even though they had no involvement in the underlying action. Therefore, clarifying the scope of discovery and the proper role of entities storing contested electronic

---

[119] *See supra* notes 4, **Error! Bookmark not defined.**-89, 101, and accompanying text (exposing dearth of federal case law regarding text message discovery).

information has the potential to avoid third party uncertainty and expense. In sum, Congress must provide relevant workable guidelines to ensure that text message discovery disputes are resolved efficiently, consistently, and fairly. Though uniform discovery standards may be unattainable in the short term, federal courts will likely continue to rely on a handful of seminal cases in confronting this new horizon of electronic discovery.

Erin Marie Secord