


Winter 2007

Criminal Discovery of Internet Communications under the Stored Communications Act: It's Not a Level Playing Field

Marc J. Zwillinger

Christian S. Genetski

Follow this and additional works at: <https://scholarlycommons.law.northwestern.edu/jclc>

 Part of the [Criminal Law Commons](#), [Criminology Commons](#), and the [Criminology and Criminal Justice Commons](#)

Recommended Citation

Marc J. Zwillinger, Christian S. Genetski, Criminal Discovery of Internet Communications under the Stored Communications Act: It's Not a Level Playing Field, 97 J. Crim. L. & Criminology 569 (2006-2007)

This Symposium is brought to you for free and open access by Northwestern University School of Law Scholarly Commons. It has been accepted for inclusion in Journal of Criminal Law and Criminology by an authorized editor of Northwestern University School of Law Scholarly Commons.

CRIMINAL DISCOVERY OF INTERNET COMMUNICATIONS UNDER THE STORED COMMUNICATIONS ACT: IT'S NOT A LEVEL PLAYING FIELD

MARC J. ZWILLINGER & CHRISTIAN S. GENETSKI*

The Stored Communications Act, 18 U.S.C. § 2703, enacted in 1986, represents Congress' attempt to strike a fair balance between the privacy rights of individuals who have entrusted the contents of their electronic communications to Internet service providers and the government's legitimate interest in gaining access to such communications when investigating crimes. For over two decades, courts have relied on the Act to define the limits of online privacy, and have generally avoided tricky constitutional questions about the extent to which an e-mail's author, or recipient, should retain Fourth Amendment protection for copies of the e-mail retained on their ISP's server. To the extent scholars have debated the merits of the Act, they too have focused largely on whether it sufficiently protects e-mail correspondents and bloggers from the prying eyes of the government. This Article, however, explores an overlooked but increasingly prominent Stored Communications Act issue—the Act's restrictions on ISP disclosures to criminal defendants and civil litigants. At present, the Act places an absolute bar on ISP disclosures of the contents of communications in electronic storage to private parties. Accordingly, in cases where e-mail contents may only support a defense (and thus the government has no motivation to seek their disclosure), a criminal defendant may have no ability to compel disclosure of potentially

* The authors are partners in the Information Security and Internet Enforcement group at Sonnenschein, Nath & Rosenthal LLP, where they regularly advise companies and handle litigation related to mandatory and permissive disclosures under the Stored Communications Act. Both authors are also former members of the United States Department of Justice Computer Crime and Intellectual Property Section, where they investigated and prosecuted cybercrime and trained state and federal law enforcement on how to obtain electronic evidence. Mr. Genetski also serves as an adjunct professor at the Georgetown University Law Center. This is the first of two articles by the authors exploring open issues related to Electronic Communications Privacy Act.

exculpatory evidence in the hands of a third-party. As the cache of online evidence continues to expand, criminal defendants are beginning to discover that the Stored Communications Act may have created an uneven playing field. This Article explores how this uneven playing field came to exist, how it affects both criminal and civil cases, and how it may have constitutional implications. Finally, the authors propose a simple amendment to the Stored Communications Act that would fill this gap, and ensure the Act's continued role as the preeminent arbiter of rights to remotely stored electronic content.

I. INTRODUCTION

In the nearly twenty-one years since the Stored Communications Act (SCA) was added to Title 18 of the United States Code, online service providers of many different stripes have received tens of thousands of requests for information about their subscribers from government agencies and private parties.¹ And yet, notwithstanding the volume of requests, very few courts have had the opportunity to closely parse the meaning of the SCA's provisions related to permitted and prohibited disclosures by electronic communication service providers (ECS providers) and remote computer service providers (RCS providers) under 18 U.S.C. § 2702 and § 2703. Those courts that have examined these provisions have usually done so in the context of civil cases, as the absence of a suppression remedy for violations of the SCA virtually precludes the possibility of substantive analysis of the SCA in the context of criminal cases.² Because the provisions of the SCA were designed primarily to address restrictions on the government's access to documents held by third parties during criminal investigations, and are generally poorly understood, the civil cases involving the SCA often result in odd decisions,³ made even stranger by

¹ This conservative estimate is based on the authors' combined experience over the last decade, since the boom of the World Wide Web, first in working with prosecutors and agents on requests, and later in representing several major Internet service providers on compliance with such requests. The authors of this Article alone have been asked to intervene on behalf of their ISP clients to respond to criminal defendants' threats of motions to compel in several cases in just the last three months.

² See Orin S. Kerr, *Lifting The "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003) [hereinafter Kerr, *The "Fog"*]; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004); see also *Warshak v. United States*, No. 1:06-CV-357, 2006 U.S. Dist. LEXIS 50076, at *19 (S.D. Ohio July 21, 2006) (ruling that users have reasonable expectations of privacy under the Fourth Amendment in e-mail messages stored on a provider's server).

³ See Kerr, *The "Fog," supra* note 2.

imprudent concessions and stipulations that generally complicate and confuse matters.⁴ Nevertheless, despite these odd results, and the especially high frequency of amended or withdrawn panel opinions⁵ and en banc hearings,⁶ several essential questions surrounding the interpretation of the SCA have been addressed, and in some cases resolved.⁷

Oddly, however, not a single published state or federal case has considered the topic of how the SCA applies in the context of defendant-initiated criminal discovery. In the course of representing Internet service providers, web portals, and application service providers (together ISPs) the authors of this Article have witnessed firsthand how little is known about the SCA's restrictions by defense counsel, and how frequently public defender's offices, private criminal counsel, and even pro se defendants serve subpoenas unlawfully seeking to compel production of the contents of Internet communications.⁸ These defendants and their counsel are invariably surprised to learn that federal law precludes the subpoenaed ISPs from disclosing, at least to them, the communications they seek.

Although largely overlooked to date, this seeming statutory anomaly has important repercussions for criminal law. The number of cases in which criminal defendants seek access to e-mail, blog entries, photos, and other user content held by ISPs is already significant, and the ever-expanding trend to entrust the safekeeping of sensitive, personal documents

⁴ In *Konop v. Hawaiian Airlines, Inc.*, the parties agreed that Konop's website was an electronic communications service, and that the website was in "electronic storage." 302 F.3d 868, 879-80 (9th Cir. 2002). Neither agreement was necessarily appropriate. In fact, both propositions appear affirmatively incorrect and have been rejected by other courts. See *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y. 2005); *Snow v. DIRECTV, Inc.*, 450 F.3d 1314 (11th Cir. 2006) (affirming on other grounds but acknowledging the district court's order holding that contents of a website are not in electronic storage).

⁵ See *Theofel v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003), *withdrawn and amended by* 359 F.3d 1066 (9th Cir. 2004).

⁶ See *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004), *vacated and superseded by* 418 F.3d 67 (1st Cir. 2004) (en banc).

⁷ For example, it now appears to be settled that the operator of a website that accesses cookies stored by it on a visitor's hard drive is not violating the SCA. See, e.g., *In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001). Also, websites that allow users to use website features to interact with the website, or send communications to the website operator are not ECS providers. See, e.g., *In re JetBlue*, 379 F. Supp. 2d 299; *In re Nw. Airlines Privacy Litig.*, No. 04-126, 2004 U.S. Dist. LEXIS 10580, at *6 (D. Minn. June 6, 2004).

⁸ Indeed, in the authors' experience, many criminal defense attorneys practicing in state courts are completely unfamiliar with the SCA. To date, these disputes in criminal cases have been resolved without published opinion, mostly through the agreement of the parties to obtain the contents of communications via either the government issuing process to obtain the information or securing the consent of the account holder.

and communications to third-party ISPs ensures that the demand will only increase. For example, an ISP may unwittingly possess electronic content amounting to contraband, such as trade secret documents or infringing copies, or contents of e-mail messages between the defendant and his victim that may evidence a lack of criminal intent. Although the government may seek to discover the former, only the defendant is likely to have an interest in disclosure of the latter. As it stands, the SCA permits the government, subject to certain limitations, to achieve its end by serving proper legal process on the ISP. Criminal defendants, by contrast, have no such recourse.

This Article seeks to expose the uneven playing field created by the SCA, highlight its implications, and propose a legislative solution. In Section II, the Article first places the SCA in historical context, reviewing the broad concerns that motivated the Act, the statutory scheme by which those concerns were addressed, and the basis, if any, for the disparate treatment of the government and criminal defendants. The Article in Section III examines how the voluntary and compelled disclosure provisions of the SCA preclude ISPs from disclosing contents of Internet communications between third-parties to criminal defendants and civil litigants under any circumstances. This is true even if the ISPs are ordered to do so by the court, even though the same materials can be disclosed to the government upon presentation of proper legal process and without court involvement. Sections IV and V further explain how the same provisions of the SCA that work to deny defendants access to contents of communications allow defense counsel to obtain certain non-content records more easily than the government can obtain such material. In Section VI, the Article explores the implications of this uneven playing field, and identifies the potential legal arguments and tactics criminal defendants might pursue to force disclosure under the current SCA scheme, including whether the present imbalance is grounds for a constitutional challenge. Finally, Section VII proposes amendments to the SCA that would address these relatively obvious oversights and insulate the Act from any potential constitutional infirmity while keeping the purpose and spirit of the SCA intact.

II. ORIGINS AND HISTORY OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The SCA was enacted by Congress in 1986 as part of the Electronic Communications Privacy Act (ECPA).⁹ At the time, the use of the Internet

⁹ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

for person-to-person communications was in its nascent stage, and large scale third-party data storage and processing was only an emerging business.¹⁰ As such, the SCA was conceived at a time that pre-dated the World Wide Web, and therefore did not contemplate the ubiquitous use of web-based communications services such as Hotmail, Yahoo!, MySpace, or Gmail, and the accompanying copious, long-term storage offered by such providers.¹¹

In the context of that environment, Congress pursued passage of the SCA as a measure to protect individuals' privacy and proprietary interests. The SCA reflects Congress's judgment that users have a legitimate interest in the confidentiality of electronic communications stored on third-party servers.¹² In seeking to protect these privacy interests, however, Congress also attempted to strike a balance with the recognized need for law enforcement access to such information in appropriate cases. Indeed, the theme of balancing "legitimate" privacy interests against equally "legitimate" law enforcement needs is echoed throughout the legislative history.¹³

As the legislative history makes clear, Congress believed that a federal statute was necessary to ensure that privacy interests were amply protected in this new medium because the applicability of well established constitutional protections was a "legal uncertainty."¹⁴ Specifically, Congress noted that forms of communication analogous to e-mail were

¹⁰ See S. REP. NO. 99-541, at 2 (1986) ("Today we have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing.").

¹¹ See JENNIFER CHEESMAN DAY ET. AL., U.S. BUREAU OF THE CENSUS, CURRENT POPULATION REPORTS, COMPUTER USE IN THE UNITED STATES: 2003 (2005), available at <http://www.census.gov/prod/2005pubs/p23-208.pdf>; ROBERT KOMINSKI, U.S. BUREAU OF THE CENSUS, CURRENT POPULATION REPORTS, COMPUTER USE IN THE UNITED STATES: 1984 (1988), available at <http://www.census.gov/population/socdemo/computer/p23-155/p23-155.pdf>; ERIC C. NEWBURGER, U.S. BUREAU OF THE CENSUS, CURRENT POPULATION REPORTS, COMPUTER USE IN THE UNITED STATES: 1997 (1999), available at <http://www.census.gov/prod/99pubs/p20-522.pdf>; see also Ari Schwartz, Deirdre Mulligan & Indran Mondal, *Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues*, 1 J.L. & POL'Y FOR INFO. SOC'Y 597 (2005).

¹² *Theofel v. Farey-Jones*, 341 F.3d 978, 1072 (9th Cir. 2003), *withdrawn and amended by* 359 F.3d 1066 (9th Cir. 2004); *Freedman v. Am. Online, Inc.*, No. 3:03cv1048, 2004 U.S. Dist. LEXIS 1548 (D. Conn. Jan. 4, 2004).

¹³ See S. REP. NO. 99-541, at 3 ("[The SCA] is modeled after the Right to Financial Privacy Act, 12 U.S.C. 3401 et seq., to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs. The [Act] represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.").

¹⁴ *Id.* at 5.

protected by the Fourth Amendment, by previously enacted federal law, or by some combination of the two. E-mail, by comparison, had no such established protections.¹⁵ Moreover, the prevailing sense of constitutional scholars was that the new technology's emphasis on third party storage did not square with the Fourth Amendment's traditional limitations to protecting personal, physical spaces.¹⁶

Indeed, two established lines of Fourth Amendment doctrine—the voluntary disclosure and business records cases—strongly suggested that if the Constitution was the sole source of protection for remotely-stored electronic communications, then third parties, including the government, would face no obstacle to compelling disclosure. The Fourth Amendment guarantees that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause”¹⁷ “The basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.”¹⁸ Its reach, however, has limits.¹⁹

One well-recognized limitation is the limit on protection for information voluntarily conveyed to a third party.²⁰ At the most fundamental level, this limitation recognizes that the government does not unlawfully invade a person's privacy when it uses information a defendant disclosed in conversation with a government informant, undercover agent, or other witness, regardless of whether that conversation took place in a “private” context. As the Supreme Court has stated, the Fourth Amendment

¹⁵ *Id.* (“A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations. Voice communications transmitted via common carrier are protected by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology.”).

¹⁶ *Id.* (“Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.”). See generally 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, 1209-13 (2004) [hereinafter Kerr, *A User's Guide*] (explaining why the Fourth Amendment offers weak privacy protections to information stored with third parties online).

¹⁷ U.S. CONST. amend. IV.

¹⁸ *Camara v. Mun. Court*, 387 U.S. 523, 528 (1967).

¹⁹ “[T]he Fourth Amendment does not proscribe all searches and seizures, but only those that are unreasonable.” *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 619 (1989).

²⁰ See *Hoffa v. United States*, 385 U.S. 293, 414 (1966); see also *Katz v. United States*, 389 U.S. 347, 351 (1967) (“What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”).

does not “protect[] a wrongdoer’s misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.”²¹

The voluntary disclosure doctrine was augmented in the specific context of third party storage of documents in what are now recognized as the “business records” cases. In *United States v. Miller*²² and *Smith v. Maryland*,²³ the Supreme Court affirmed that individuals do not maintain a reasonable expectation of privacy in information voluntarily revealed to third parties.²⁴ In *Miller*, the government subpoenaed the defendant’s bank records in order to provide evidence that he was engaged in criminal activity.²⁵ The Court held that a depositor relinquishes any expectation of privacy in his banking information by revealing it to the bank in the ordinary course of business.²⁶ Similarly, in *Smith*, the Court held that the Fourth Amendment does not protect the numbers that telephone users dial when making a call.²⁷ The holdings of *Miller* and *Smith* center on the fact that the information at issue was divulged as part of the regularly transacted business between the user and the third party, and was kept as a record of such transaction.²⁸

Given this precedent, Congress questioned whether the Fourth Amendment clearly protected users’ electronic communications from government reach.²⁹ Even if the Fourth Amendment were found to protect such communications, however, the fact that the communications resided in third-party ISP hands posed an additional threat to privacy interests. ISPs are not government actors, and therefore are not constrained by the Fourth Amendment. Accordingly, under the private search doctrine, ISPs would

²¹ See *Hoffa*, 385 U.S. at 413 (holding that Teamsters Union leader Jimmy Hoffa’s conversations with a government informant regarding his plan to bribe a jury were not protected, notwithstanding the fact that the conversations took place in Hoffa’s hotel room).

²² 425 U.S. 435 (1976).

²³ 442 U.S. 735 (1979).

²⁴ See also *Couch v. United States*, 409 U.S. 322, 335 (1973) (holding that a taxpayer does not have a reasonable expectation of privacy in records conveyed to an accountant because the preparation of the tax return—the ordinary course of the business between the parties—required disclosure of the information sought).

²⁵ See *Miller*, 425 U.S. at 437-38.

²⁶ See *id.* at 440-43.

²⁷ See *Smith*, 442 U.S. at 742.

²⁸ See Mulligan, *supra* note 2, at 1562.

²⁹ Indeed, the legislative history shows that even real-time interceptions of e-mails in transit presented a murky Fourth Amendment issue. See H.R. REP. NO. 99-647, at 22 (1986) (“There are no reported cases governing the acquisition of e-mail by the government, so an application of the Fourth Amendment to the interception of e-mail is speculative.”).

be free to disclose a user's communications to anyone, including law enforcement, without constitutional implication.³⁰

Thus, Congress' motivation in enacting the SCA stemmed primarily from its recognition that these lines of Fourth Amendment jurisprudence suggested that privacy protections were limited solely to the voluntary practices of ISPs in the first instance, and that any such voluntary protections would be easily trumped by minimal compulsory process from the government or any third party. The SCA is meant to fill precisely this gap, and, in essence, to create a Fourth Amendment Lite by statute.³¹ In filling the gap, Congress sought to "ensure the continued vitality of the Fourth Amendment" and prevent the "gradual erosion" of privacy rights, but equally to avoid a situation where "[t]he lack of clear standards may expose law enforcement officers to liability and may endanger the admissibility of evidence."³²

The statute's framework thus reflects the twin goals of constraining private ISPs from vitiating privacy interests through voluntary disclosures, and ensuring that these constraints also provide a clear mechanism for law enforcement to compel disclosure in appropriate circumstances and keep it within appropriate procedural safeguards. To address the first concern, Congress imposed a flat prohibition on ISPs' voluntary disclosure of the contents of communications to *any* third party.³³ This prohibition ensured that an ISP cannot, via a private search and voluntary disclosure, circumvent the Fourth Amendment. To address the second concern, Congress imposed a series of "exceptions" to this prohibition, embodied in 18 U.S.C. § 2703, that permit disclosure to *law enforcement* pursuant to specified legal process.³⁴

Perhaps not surprisingly, a statute designed to fill a Fourth Amendment gap created by the private search and voluntary disclosure doctrines did not account for the impact on private third parties seeking access to communications held by ISPs, even in instances where those parties, as with civil litigants and criminal defendants, have limited statutory authority to issue compulsory process or seek the assistance of the courts in doing so. Indeed, in the race to square up the balance of privacy

³⁰ See *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (recognizing that the Fourth Amendment does not protect against private searches and seizures); Kerr, *A User's Guide*, *supra* note 16, at 1212.

³¹ See Kerr, *A User's Guide*, *supra* note 16, at 1212-13.

³² *Id.*

³³ See 18 U.S.C. § 2702 (2000).

³⁴ The key portions of the SCA framework are discussed in detail in Sections III-IV, *infra*.

interests between the government and ISP subscribers, it appears that Congress left these third parties behind.

It is possible that the SCA's failure to provide a means for criminal defendants to compel disclosure of electronic communications reflects Congress's considered decision to also protect the privacy of such communications vis-à-vis third parties. But nothing in the legislative history suggests that Congress contemplated, much less intended, this result.³⁵ Given the focus on the Fourth Amendment, Congress appears simply to have overlooked the potential concerns of non-state actors seeking compulsory access to information held by ISPs. There is no suggestion in the legislative debates, for instance, of any need to balance the interests of users against those of criminal defendants or civil litigants. Indeed, the SCA explicitly places *no* restriction on ISPs' freedom to disclose non-content information and transactional records to private parties, even though it limits disclosure of the same information to law enforcement only pursuant to specific compulsory process.³⁶ This all-or-nothing approach suggests Congress simply did not contemplate compelled disclosures by private parties, an oversight that has led to seemingly unintended consequences.³⁷

³⁵ See generally H.R. REP. NO. 99-647 (1986); S. REP. NO. 99-541 (1986).

³⁶ By contrast, the Cable Act, a similar privacy statute applicable to providers of cable service, contains a series of provisions that dictate when certain information can be compelled or disclosed voluntarily, and provides a mechanism for disclosure via court order, which is available to both government and private actors. See 47 U.S.C. § 551(c)(2)(B).

³⁷ Congress apparently opted to provide free reign to non-content records to all but law enforcement in recognition that such records were properly viewed as "business records" under the *Miller* and *Smith* line of cases, and as such did not raise any private search Fourth Amendment issues. H.R. REP. NO. 99-647, at 23. Citing *Miller*, the report stated, "[U]nder current law a subscriber or customer probably has very limited rights to assert in connection with the disclosure of records held or maintained by remote computing services." *Id.* However, it is also noted that *Miller* can be distinguished because "[u]nlike records of the bank's (or remote computing service's) records, contents are analogous to items stored, under the customer's control, in a safe deposit box." *Id.* at 23 n.41. Under this rationale, Congress afforded greater privacy to content because of its lack of ease with where content fell along the Fourth Amendment continuum. Even assuming Congress apportioned rights under this rationale, however, this rationale does not account for the absence of an SCA exception permitting non-state actors to compel disclosure of content in certain circumstances. The legislative record is silent on this issue. Cf. *O'Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 88 (Cal. Ct. App. 2006) ("[I]t would be far from irrational for Congress to conclude that one seeking disclosure of the contents of email, like one seeking old fashioned written correspondence, should direct his or her effort to the parties to the communication and not a third party who served only as a medium and neutral repository for the message.").

III. BASIC SCA DEFINITIONS AND CASES

Generally, the structure of the SCA recognizes two types of entities: electronic communication service providers and providers of remote computing services. An “electronic communication service” is “any service which provides to users thereof the ability to send or receive wire or electronic communications.”³⁸ For purposes of the SCA an “electronic communication” is “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.”³⁹ Recent cases have helped further define this concept, holding that the definition of electronic communication includes, among other things, e-mail,⁴⁰ instant messages,⁴¹ and data input to online forms.⁴²

A remote computing service means “the provision to the public of computer storage and processing services by means of an electronic communications system.”⁴³ Whereas an entity need not offer electronic communication services to the public in order to be considered an ECS provider, the public offering of services is part of the definition of remote computer services. Thus, corporations that provide e-mail services to their employees are ECS providers, but not RCS providers.

By providing e-mail and private or instant messaging services, or both, ISPs offer electronic communication service, while online merchants and others who use websites only to interact with their own customers or to market services generally do not.⁴⁴ Moreover, ISPs may also offer remote computer services under certain circumstances, such as when they offer subscribers the opportunity to store materials like address books, calendars,

³⁸ 18 U.S.C. § 2510(15).

³⁹ *Id.* § 2510(12).

⁴⁰ *In re U.S. for an Order Authorizing the Installation and Use of a Pen Register*, 416 F. Supp. 2d 13 (D.D.C. 2006).

⁴¹ *Quon v. Arch Wireless Operating Co.*, 309 F. Supp. 2d 1204 (C.D. Cal. 2004).

⁴² *In re Pharmatrak, Inc.*, 220 F. Supp. 2d 263 (D. Mass. 2003).

⁴³ 18 U.S.C. §§ 2510(15), 2711(2).

⁴⁴ *See In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y. 2005) (holding that a company that maintains a website permitting the transmission of electronic communications between itself and its customers is not an ECS provider); *In re Nw. Airlines Privacy Litig.*, No. 04-126, 2004 U.S. Dist. LEXIS 10580, at *6 (D. Minn. June 6, 2004) (holding that an airline that purchased its electronic communication service from a third party was not itself an ECS provider); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001) (holding that an online retailer that purchased service from a third-party provider and did not independently offer service to the public was not an ECS provider).

photo albums, video content, and electronic files in user-controlled virtual directories.

In addition to defining two different types of providers that are covered by the SCA, the SCA also describes four different categories of information that may be found on the computers maintained by ECS and RCS providers. These four categories of information are: (1) materials "in electronic storage";⁴⁵ (2) contents of wire or electronic communications in a remote computing service;⁴⁶ (3) records or other information pertaining to a customer or subscriber;⁴⁷ and (4) information available with a subpoena under 18 U.S.C. § 2703(c)(2).⁴⁸ Of these four categories, content material, as described in the first two exceptions, is generally subject to the strictest prohibitions on disclosure, while transactional records relating to subscribers are provided the least protection. Each of these categories is explored more fully below.

A. IN ELECTRONIC STORAGE

The most protected category of information under the framework of the SCA is information "in electronic storage." As defined in the SCA, "electronic storage" is: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."⁴⁹ This definition was previously understood to encompass only those person-to-person messages that were stored on an ECS server temporarily after being sent by the originator but before the recipient had logged in to read or download the message.⁵⁰ In fact, the Department of Justice (DOJ) continues to believe that this is the correct understanding of the definition.⁵¹ However, in 2004, the Ninth Circuit ruled

⁴⁵ 18 U.S.C. § 2703(a).

⁴⁶ *Id.* § 2703(b).

⁴⁷ *Id.* § 2703(c)(1).

⁴⁸ *Id.* § 2703(c)(2).

⁴⁹ *Id.* § 2510(17).

⁵⁰ See *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2003); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461-62 (5th Cir. 1994); *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001) (holding that messages in post-transmission storage are outside the scope of § 2701), *aff'd in part, vacated in part on other grounds*, 352 F.3d 107 (3d Cir. 2003); *In re Toys R Us, Inc. Privacy Litig.*, C 00-2746 MMC, 2001 U.S. Dist. LEXIS 16947, at *10-11 (N.D. Cal. Oct. 9, 2001) (holding the same).

⁵¹ See COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § 2 (2002), available at <http://www.usdoj.gov/criminal/>

that the definition of “electronic storage” is broad enough to encompass previously-read e-mails that a user elects to store on his ISP’s servers, even though such e-mails, having been opened and read, are no longer in temporary storage incidental to their transmission.⁵²

In *Theofel v. Farey-Jones*, counsel for the defendant issued a civil subpoena to the plaintiffs’ e-mail service provider, seeking numerous e-mails for use in the civil litigation.⁵³ The small e-mail service provider, which at the time was not represented by counsel, responded to the subpoena by making available to defendant’s counsel a representative sample of e-mails.⁵⁴ When plaintiffs discovered what the service provider had done, they moved to quash the subpoena and asked the court to award sanctions.⁵⁵ The court did both, and plaintiffs then brought a civil suit against counsel for defendants for, inter alia, violations of the SCA.⁵⁶ Although the district court initially dismissed the plaintiffs’ SCA claim, the Ninth Circuit, in a panel opinion, reversed the dismissal, finding that in spite of the ISP’s voluntary disclosure of the e-mails, defendants’ subpoena was in clear violation of the SCA and gave the defendants unauthorized access to e-mails in electronic storage.⁵⁷ Although the *Theofel* court’s analysis is somewhat tortured, the court essentially relied on the second prong of the definition of electronic storage, which includes “storage for purposes of . . . backup protection,” ruling that when a user decides to leave her e-mails on the e-mail server, she is essentially doing so for purposes of backup protection.

Although the United States was not a party to the litigation initially, the effect of the ruling in *Theofel* was to substantially expand the universe of material in electronic storage from a tiny bit of received but unread e-mail to all of the e-mails maintained by an ISP on a subscriber’s behalf. Because the SCA requires governmental entities to get a search warrant before any materials in “electronic storage” are disclosed, the *Theofel* decision posed a significant problem for law enforcement. As a result, the DOJ intervened in the litigation and petitioned for rehearing and rehearing en banc.⁵⁸ In its briefing, the DOJ argued that a more appropriate reading of the “backup” protection prong was that it was limited to circumstances

cybercrime/s&smanual2002.html [hereinafter SEARCHING AND SEIZING].

⁵² *Theofel*, 359 F.3d 1066.

⁵³ *Id.* at 1071.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.* at 1072. The SCA provides that users injured by virtue of a violation can bring a civil action. 18 U.S.C. § 2707 (2000).

⁵⁷ *Theofel*, 359 F.3d at 1074-75.

⁵⁸ *Id.* at 1064-70.

where an ISP makes a backup copy of the messages on its servers, so that any unread messages captured in the backup remain in electronic storage even after the user may have opened and downloaded the messages on the live server.⁵⁹ The Ninth Circuit rejected the DOJ's argument, maintaining its position that the "backup protection" prong of the definition of electronic storage was not limited to backups made by the e-mail provider or the ISP.⁶⁰ Instead, the court held that the stored copies functioned as a backup for the user, noting that "nothing in [the ECPA] requires that the backup protection be for the benefit of the ISP rather than the user."⁶¹

Despite continuing uncertainty as to the correctness of the *Theofel* reading of the backup storage provision, the decision in *Theofel* is followed by most major ISPs, who now require search warrants before producing any e-mail or private message content less than 180 days old. Even after *Theofel*, contents held in electronic storage for more than 180 days lose their special quality under the statute and are rendered the same as the contents of materials that may be found within a subscriber's online account and which are described below in Section III.B.

B. CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE

One of the most common (and understandable) misconceptions about the SCA is that all materials stored electronically are "in electronic storage." But, as described above, "electronic storage" is a term of art, requiring that the storage be temporary and incidental to transmission, or the backup of such communications. The SCA has a different provision intended to address materials that are intentionally, and more permanently, stored with an ISP, such as photos, address books, calendars, web sites, files, documents, and other types of content, as well as stale e-mails over 180 days old.⁶² Although voluntary disclosure of such material by an ISP is also prohibited, the relevant provision of the SCA—18 U.S.C. § 2703(b)—allows the government to gain access to such materials with lesser process than materials "in electronic storage."⁶³ For this category of materials, the

⁵⁹ *Id.* at 1076.

⁶⁰ *Id.*

⁶¹ *Id.* at 1075.

⁶² The distinction between materials in "electronic storage," and materials that may just be stored electronically is crucial. In fact, the SCA makes it a criminal offense to access materials that are in electronic storage, but there is no provision of the SCA making it illegal for a private party to access materials that are *not* in electronic storage. See 18 U.S.C. § 2701 (2000).

⁶³ See *id.* § 2703(b).

government can compel production through the use of a court order pursuant to 18 U.S.C. § 2703(d) or with a simple administrative or grand jury subpoena, as long as the subscriber or customer is given prior notice of the subpoena, unless the need for such notice is excused in accordance with 18 U.S.C. § 2705.⁶⁴ Generally, the permissible grounds for delaying such notice are: (1) risk to the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) circumstances that would otherwise seriously jeopardize an investigation.⁶⁵

Because the SCA treats contents of communications in electronic storage with an ECS provider differently than contents of communications stored in an RCS provider, content contained in an e-mail from one user to another may be entitled to different protection from government access than, for instance, the identical content posted to a message board. The SCA makes no distinction between the two categories, however, for purposes of disclosure to private parties.

C. RECORDS AND OTHER INFORMATION PERTAINING TO A SUBSCRIBER OR CUSTOMER

The least understood category of information defined by the SCA is arguably the broadest. This includes all non-content records about a subscriber or customer of an ISP, with the exception of the basic information about the subscriber's identity that is specially carved out and described below in Section III.D. Any records of subscriber activity that are neither basic subscriber information nor the contents of subscriber communications may be obtained by the government only with a warrant, a court order as provided under § 2703(d), or subscriber consent, but not with a subpoena.⁶⁶ Common examples of such customer records include transactional records, such as addresses of websites visited by the customer; records of online configurations and passwords; and e-mail addresses of other individuals with whom the account holder has communicated.⁶⁷

⁶⁴ This provision allows the government to delay notice to a subscriber about a subpoena for a period not to exceed ninety days upon the execution of a written certification by a supervisory official that determines that there is reason to believe that notification of the subscriber may have an adverse result of the type described in 18 U.S.C. § 2705(a)(2). *Id.* § 2705(a)(1)(A). It also allows a court to order that delayed notice be used in connection with information sought via a court order, if the court determines that there is reason to believe that notification of the subscriber may have an adverse result. *Id.* § 2705(a)(2)(B).

⁶⁵ *Id.* § 2705(a)(1)-(2).

⁶⁶ *Id.* § 2703(c)(1).

⁶⁷ SEARCHING AND SEIZING, *supra* note 51, § III.C.2.

D. BASIC SUBSCRIBER INFORMATION

From the larger category of “records or other information about a subscriber or customer,” the ECPA carves out certain types of customer records, typically referred to as “basic subscriber information,” for which the government need only obtain a subpoena rather than a court order or warrant (although a court order or warrant would also suffice). Specifically, the ECPA provides that, in response to an administrative, grand jury or trial subpoena, an ECS or RCS provider must disclose to a government entity the following customer records:

- (A) name;
- (B) address;
- (C) local and long distance telephone connection records, or records of session times or durations;
- (D) length of service (including start date) and types of service utilized;
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address [i.e., IP address]; and
- (F) means and source of payment for such service (including any credit card or bank account number).⁶⁸

Generally, the types of subscriber information the government is entitled to receive under a subpoena “relate to the identity of the subscriber, his relationship with his service provider and his basic session connection record.”⁶⁹

IV. ANALYSIS OF SCA PROHIBITIONS ON DISCLOSURE OF CONTENT

For ECS providers who offer services to the public, as well as RCS providers, the SCA contains a clear framework by which the contents of electronic communications may be disclosed. That framework begins with the clear and unequivocal prohibitions on disclosure of both types of content records that may be in the possession and control of a third-party ISP—materials in “electronic storage,” and “contents of wire or electronic communications in a remote computing service”:

- (1) A person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service

⁶⁸ 18 U.S.C. § 2703(c)(2).

⁶⁹ SEARCHING AND SEIZING, *supra* note 51, § III.C.1.

(2) A person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity

(A) 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 that service;

(B) 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.⁷⁰

Although these prohibitions are found in a section of the SCA entitled “Voluntary Disclosures,”⁷¹ nothing in the text of these two clear prohibitions limits their application to circumstances where the ISP is seeking to make a voluntary disclosure. More importantly, there is no general exception for disclosures made pursuant to legal process or where otherwise required by law. Instead, the SCA provides only eight specific exceptions to the prohibition on disclosing contents of communications.⁷² None of these exceptions provide a basis for a disclosure in response to a subpoena served by a criminal defendant, nor a court order secured at the defendant’s request.

In order, the listed exceptions are:

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in [18 U.S.C. §§ 2517, 2511(2)(a), or 2703];

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) 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;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990;

(7) to a law enforcement agency

(A) if the contents

(i) were inadvertently obtained by the service provider; and

⁷⁰ 18 U.S.C. § 2702(a)(1)-(2).

⁷¹ *See id.* § 2702.

⁷² *Id.* § 2702(b).

(ii) appear to pertain to the commission of a crime; [and,]

(8) 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.⁷³

Exceptions 6, 7, and 8 concern specific circumstances when disclosures are permitted to governmental entities. Two more of these exceptions, 4 and 5, pertain to disclosures made by an ISP in order to render service or to forward communications. Of the three exceptions that remain, two, 1 and 3, allow disclosures either directly to government entities, or with the consent of the authors, addressees, or intended recipients of the message. In circumstances where a criminal defendant is seeking to obtain his own messages, or messages intended for him, these exceptions may be helpful. In a case where a criminal defendant or party to a civil lawsuit is seeking to obtain the messages of a third-party, such as the victim in a criminal case, none of these exceptions apply. Accordingly, the only possible remaining exception allows disclosure "as otherwise authorized in 18 U.S.C. §§ 2517, 2511(2)(a), or 2703."⁷⁴ From this framework, it is clear that the only non-voluntary disclosures that are permitted by an ECS provider to the public, or of a remote computing service, are those compelled disclosures that are authorized within the statutory framework contained in 18 U.S.C. §§ 2517, 2511(2)(a), or 2703.

Even a close examination of all three of the provisions cited in this exception reveals no pathway for anyone other than a government entity to compel disclosures of contents of customer communications. First, 18 U.S.C. § 2517 authorizes the use and disclosure of contents of communications lawfully intercepted under the Wiretap Act.⁷⁵ Thus, this exception is specifically aimed at law enforcement.⁷⁶ The two exceptions of general applicability contained within § 2517 merely make clear that any communication that is obtained lawfully under the provisions of the Wiretap Act can be used and disclosed while giving testimony, but that no privileged communications will lose their privileged character merely because their interception was lawful.⁷⁷

Second, the exception for authorized disclosures pursuant to 18 U.S.C. § 2511(2)(a) pertains only to disclosures by providers of wire or electronic communications, when such providers deem it necessary to "intercept,

⁷³ See *id.*

⁷⁴ *Id.* § 2702(b)(2).

⁷⁵ *Id.* § 2517.

⁷⁶ See *id.* § 2517(1)-(2), (5)-(8).

⁷⁷ *Id.* § 2517(3)-(4).

disclose, or use that communication in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider.”⁷⁸ As with the first exception, such authority provides no exception for disclosures of contents of communications that are subpoenaed by criminal defendants or civil parties.

The third and final exception allows disclosure under 18 U.S.C. § 2703. Although § 2703 sets out a detailed framework for the disclosure of contents of communications pursuant to compulsory legal process, all of the procedures contained in § 2703 pertain to the process required for a governmental entity to seek data from an ISP.⁷⁹ Section 2703(a) describes the government’s use of a warrant to obtain materials in electronic storage for 180 days or less.⁸⁰ Section 2703(b) provides the process for a governmental entity to obtain contents of customer communications that are not in electronic storage, or have been in electronic storage for more than 180 days.⁸¹ Section 2703(c)(1) authorizes a governmental entity to obtain records or other information about a subscriber or customer using a special form of court order, as described further in § 2703(d).⁸² Finally, § 2703(c)(2) sets forth the government’s ability to obtain basic subscriber information by subpoena.⁸³ Thus, there is simply no provision in 18 U.S.C. § 2703 that authorizes any type of disclosure of customer communications in response to legal process issued by criminal defendants or civil litigants.

Although this serious omission in ECPA procedure is somewhat obvious, only one published decision has addressed this oddity directly. In *O’Grady v. Superior Court of Santa Clara County*,⁸⁴ the California Court of Appeal became the first court to acknowledge that the SCA places the contents of communications in the possession of an ISP out of reach of all parties but governmental entities. In that case, two “online news magazines” dedicated to providing information about Apple and its products published reports about a new rumored Apple product.⁸⁵ Apple sent subpoenas to one of the publishers’ e-mail service providers in order to obtain evidence relating to theft of trade secrets.⁸⁶ In response to the

⁷⁸ *Id.* § 2511(2)(a).

⁷⁹ *Id.* § 2703.

⁸⁰ *Id.* § 2703(a).

⁸¹ *Id.* § 2703(a)-(b).

⁸² *Id.* § 2703(c)(1), (d).

⁸³ *Id.* § 2703(c)(2).

⁸⁴ 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006).

⁸⁵ *Id.* at 77-78.

⁸⁶ *Id.* at 80-81.

subpoenas, the publisher moved for a protective order to prevent this discovery, which was denied.⁸⁷ The appellate court held that the trial court erred in denying the protective order to the publisher because, inter alia, the subpoena violated the SCA.⁸⁸ Apple argued that the subpoena fell under exceptions to the SCA, but the appellate court rejected both arguments.

First, Apple contended that the publisher's noncompliance with the subpoena would subject it to contempt or other sanctions, so that the publisher's production of the requested items would be "necessarily incident . . . to the protection of the rights or property" of the publishers.⁸⁹ The appellate court rejected this argument as circular, since it presupposed the validity of the subpoena, and the subpoena was not valid in the first place.⁹⁰ The appellate court also rejected Apple's argument that the SCA contained an implied exception for civil discovery.⁹¹ Noting the SCA's lengthy list of exceptions and the statutory construction canon *expressio unius exclusio alterius est*, "under which the enumeration of things to which a statute applies is presumed to exclude things not mentioned," the court concluded that the SCA contained no exception for civil discovery.⁹²

Just as the SCA contains no exception for civil discovery, it contains no exception for criminal defense subpoenas. Contents of materials in electronic storage or materials stored by a remote computing service are virtually out of reach for any defense counsel because only the government can use the compelled disclosure provisions of 18 U.S.C. § 2703 to obtain such materials.⁹³ Without an approved exception, the prohibitions on disclosures contained in 18 U.S.C. § 2702 provide an absolute bar to disclosures of contents of communications to private parties. To the chagrin of many ISPs, this bar appears to remain in force even if such disclosures are court ordered.⁹⁴ As noted, the court order exception contained in 18 U.S.C. § 2703(d) pertains only to the government and comes into play only when a governmental entity "offers specific and

⁸⁷ *Id.* at 81-82.

⁸⁸ *Id.* at 77.

⁸⁹ *Id.* at 84 (citing 18 U.S.C. § 2702(b)(5) (2000)).

⁹⁰ *Id.* at 84-85.

⁹¹ *Id.* at 85-86.

⁹² *Id.* at 86-89.

⁹³ Furthermore, as described above, by enlarging the category of materials deemed to be "in electronic storage," to include all e-mails stored on the server for less than 180 days, the *Theofel* court created an even bigger hurdle for defense counsel to overcome, as contents of e-mails left on an ISPs servers are now entitled to the most rigorous protection that the SCA has to offer and are available only through a search warrant. See discussion *supra* Section III.A.

⁹⁴ See 18 U.S.C. § 2703(c).

articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing *criminal* investigation.”⁹⁵ By definition, no criminal defendant or party to civil litigation could make this showing. Thus, even when presented with a court order to disclose customer contents upon pain of contempt, the SCA does not authorize such disclosures.⁹⁶

V. ANALYSIS OF SCA PROVISIONS REGARDING DISCLOSURE OF RECORDS

Curiously, whereas the framework put in place in 18 U.S.C. §§ 2702-2703 creates inequities for criminal defendants seeking disclosure of electronic content, that same framework flips the relative burdens and benefits with regard to non-content information held by ISPs. For government entities, the SCA regulates non-content in much the same manner as it does content, prohibiting disclosure to government entities as a default rule, but then providing a series of exceptions permitting disclosure in response to specific legal process. In the case of private parties, however, the SCA treats non-content information much differently, imposing no restrictions whatsoever on disclosure.

Specifically, § 2702(a) of the SCA provides a blanket prohibition on ISP disclosures of non-content information, but limits the prohibition only to government entities:

⁹⁵ *Id.* § 2703(d) (emphasis added).

⁹⁶ Arguably, an ISP faced with such an order can comply with it without significant fear of retribution or liability. As noted, the SCA allows disclosures for the “protection of the rights or property of the provider.” *Id.* § 2702(c)(3). That exception, however, does not allow an ISP to produce documents in response to blatantly improper process merely because of the cost or expense that might be associated with lodging an objection to the improper process. In *O’Grady*, the court soundly rejected the notion that an ISP could be justified in relying on the exception for protecting its own rights as a basis for producing contents of communications in response to a civil subpoena, noting that:

[T]he effect of such an interpretation would be to permit disclosure whenever someone threatened the service provider with litigation. Arguably, even a subpoena would be unnecessary; the mere threat would be enough. Further, it is far from apparent that compliance with an invalid subpoena would save the provider any money, since it might expose the provider to a civil suit by an aggrieved user.

O’Grady, 44 Cal. Rptr. 3d at 85. When an ISP has articulated its objection to a subpoena, and the court nevertheless orders compliance upon pain of contempt, the exception for “protection of the rights or property of the provider,” is far more likely to be deemed a sufficient basis to justify disclosure. 18 U.S.C. § 2702(c)(3). Furthermore, 18 U.S.C. § 2703(e) provides an ISP with absolute immunity for complying with “the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.” *Id.* § 2703(e). Thus, complying with a valid court order that purports to require disclosure under the SCA should not result in any liability for an ISP, even if the court is without authorization to issue such an order under the SCA.

[A] provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.⁹⁷

Section 2702 contains no further restrictions on disclosure of non-content records. In fact, § 2702(c) sets forth six specific exceptions to § 2702(a)'s prohibition.⁹⁸ Those exceptions largely track the exceptions permitting disclosure of content information embodied in § 2702(b). The first exception in § 2703(c) refers to the exceptions authorized in § 2703.⁹⁹ As with content, § 2703 contains a series of exceptions permitting the government to compel disclosure of certain non-content information in response to specific process.¹⁰⁰

For all other non-content customer records, a government entity may compel disclosure from an ECS or RCS provider only when the government entity:

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court . . . or equivalent State warrant;

(B) obtains a court order for such disclosure [that meets the requirements of § 2703(d)];

(C) has the consent of the subscriber or customer to such disclosure; [or]

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider¹⁰¹

The § 2702 exceptions for disclosing non-content contain one notable difference from those applicable to content. Section 2702(c)(6) specifies that:

A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) . . .

(6) to any person other than a governmental entity.¹⁰²

⁹⁷ 18 U.S.C. § 2702(a)(3) (emphasis added).

⁹⁸ *Id.* § 2702(a), (c).

⁹⁹ *Id.* § 2702(c)(2).

¹⁰⁰ *Id.*

¹⁰¹ *Id.* § 2703(c)(1).

¹⁰² The remaining exceptions are:

(2) with the lawful consent of the customer or subscriber;

(3) 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;

Thus, the SCA does not merely omit private parties from the prohibition on disclosure, it specifically authorizes ISPs to disclose non-content information to any non-government entity. Accordingly, criminal defendants (and private parties) are free to seek disclosure of non-content information from ISPs (such as the IP addresses of government informants, the buddy lists of alleged co-conspirators, or the identity of an insulting poster to a message board) without the use of any legal process whatsoever, whereas the government must have an open investigation pursuant to which it can issue compulsory process in order to gain access to the same information. Accordingly, in the context of non-content information held by ISPs, the roles are reversed, with the government facing greater, though not insurmountable, challenges, and criminal defendants facing no legal hurdle at all.

VI. THE UNEVEN PLAYING FIELD AT WORK: NO REAL HINDRANCE FOR GOVERNMENT, NO RECOURSE FOR DEFENDANTS?

As we have demonstrated, the SCA imposes a set of curious double standards governing ISPs' disclosure of Internet communications that turn on the nature of the information sought and the identity of the person seeking it. If the government is the seeker, then non-content and content information are both given qualified privacy protection along a sliding scale in which the privacy of content is more closely guarded. If, however, the seeker is a criminal defendant or civil litigant, then content is afforded absolute privacy protection, and non-content is afforded no protection at all. Clearly, the statutory playing field is not level for either party to a criminal case at any given time. In practical application, however, the "sliding scale" regime imposed on the government is far less burdensome than the "all or nothing" regime for criminal defendants.

First, any benefit to defendants of the SCA's free pass for disclosures of non-content information has been more or less eroded by the voluntary privacy practices of ISPs. Nearly all providers of any measurable scope adhere to privacy policies or practices or both, that promise users the ISP will not disclose their information to any third party absent legal process.¹⁰³

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure [of the information]; [or]

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032).

Id. § 2702(c).

¹⁰³ See Google Privacy Center, <http://www.google.com/intl/en/privacy.html> (last visited

Generally speaking, then, a criminal defendant seeking non-content information about an ISP subscriber must serve a subpoena on the ISP in order to receive the information. Thus, although the SCA dictates that an ISP receive a subpoena or court order only before disclosing non-content information to a *government entity*, the overwhelming majority of ISPs impose this same requirement on criminal defendants and civil litigants as well. The playing field for non-content information, as a matter of ISP policy, is leveled.¹⁰⁴

Whereas the benefits of the “all” have proved elusive for criminal defendants and civil litigants, the consequences of the “nothing” remain quite real. ISPs have the freedom, and the market incentive, to enhance the protection of their users’ privacy beyond what the law requires, but they may not, as a matter of policy, peel back the protection imposed by law. As a result, the government may compel disclosure of electronic contents from ISPs with either a search warrant or subpoena (depending on whether the content is in electronic storage or stale). By contrast, a criminal defendant seeking to compel the disclosure of electronic contents from an ISP will likely be forced to litigate the issue and convince a court (and thereafter presumably an appellate court or two) either that the SCA does not mean what it plainly says, or that its plain meaning application is constitutionally infirm. As demonstrated later in this section, neither is a promising path.

Given that any route to successful disclosure for criminal defendants likely requires contested litigation, one may fairly ask why the issue has yet to be the subject of a reported decision and has received little to no scholarly commentary to date. The answer appears to be some combination of the nature of a typical criminal case and the cooperative efforts of prosecutors and defense counsel (many of whom regularly interact over

Apr. 21, 2007); Microsoft Online Privacy Notice Highlights, http://privacy.microsoft.com/en-us/default.aspx?HTTP_HOST=privacy2.msn.com&url=/en-us/default.aspx (last visited Apr. 21, 2007); MySpace Privacy Policy, <http://www.myspace.com/Modules/Common/Pages/Privacy.aspx> (last visited Apr. 21, 2007); Yahoo! Privacy Center, <http://info.yahoo.com/privacy/us/yahoo/details.html> (last visited Apr. 21, 2007).

¹⁰⁴ If anything, the playing field tilts slightly back into the government’s favor by virtue of the fact that the SCA permits the government to delay notice to a subscriber, and forbids the ISP from notifying the subscriber, upon written certification. *See* 18 U.S.C. § 2705. Because the subpoena requirement is not imposed on non-government entities in the SCA, the SCA provides the right to delay notice only to the government. By contrast, many major ISPs, as a matter of practice, notify subscribers of a request for their information and provide the subscriber an opportunity to object before disclosure, and many state subpoena statutes similarly require criminal defendants to notify individuals whose records are being sought from a third party custodian and provide the individual an opportunity to protest the disclosure. *See, e.g.*, CAL. PENAL CODE § 1326 (2006); Microsoft Online Privacy Notice Highlights, *supra* note 103.

many cases simultaneously) serving to obviate the need for production directly from the ISP to the defendant. In most cases in which Internet communications are a key piece of evidence, law enforcement has used the investigative tools (search warrants, court orders, and grand jury subpoenas) specified by the SCA to compel the lawful production of such information in the process of building its case. As a result, prior to indictment, the government already possesses the same information held by the ISP. Once the government files charges, it generally must disclose to the defendant any relevant evidence it has unearthed pursuant to criminal discovery rules, and in all cases must disclose any exculpatory evidence in its possession.¹⁰⁵ In a standard case, then, a defendant may rely on the government to turn over, from the set of Internet communications the government deemed significant enough to compel, at least those communications upon which the government intends to rely or that favor the defendant.

In many cases, however, sole reliance on the government's disclosure obligations is insufficient to prepare a vigorous defense, particularly when law enforcement has built a case without the need to turn over every electronic stone, or when the defendant may be unaware that additional stones exist. For instance, the government may have no incentive (or even legal basis) to compel the production of e-mail messages from a defendant's friends. If, on the other hand, a defendant facing a life sentence believes those messages may support a defense theory that the defendant played a lesser role in an alleged conspiracy, or call into question the government's timeline for the alleged crime, then that defendant will obviously have a keen interest in reviewing them. Under the SCA, only the government may compel their production from the ISP, not the defendant. Thus, criminal defendants are left to press the government to exercise its discretion to use its investigative tools to obtain the information, or to pursue production from the senders and recipients of the messages.

Depending on the nature of the case, the first option of pursuing the senders or recipients—the option that *O'Grady* contends is what Congress contemplated—may be implausible. Specifically, in cases where the defendant's purpose in seeking the communications is to establish either that a confederate is in fact responsible for an act being pinned on the defendant or that a victim is providing a false version of events, the account holder confederate or victim has little or no reason to comply with a request to consent to disclosure. Where a defendant seeks to compel production by subpoena in such a case, the confederate may attempt to object on Fifth

¹⁰⁵ *Brady v. Maryland*, 373 U.S. 83 (1963) (holding that the suppression of evidence favorable to the accused violates due process where the evidence is material to either guilt or punishment).

Amendment grounds, given that the communications are likely to be disclosed to the government,¹⁰⁶ and even the victim may be able to assert sufficient privacy rights to require a heightened showing of need from the defendant.¹⁰⁷ Finally, even where a sender or recipient does not object to a subpoena, a defendant may still have reasonable concerns about the account holder's good faith in providing full disclosure, or even face the obstacle of the sender or recipient no longer having access to the pertinent account.

Given this reality, defendants may more often opt to ask the government to intercede and compel disclosure of the communications and then turn them over to defendants upon receipt. In such cases, the defendant will have put the government on notice that he believes relevant and perhaps exculpatory evidence resides in the accounts of certain Internet users, and appeal to the prosecutor's sense of fairness in requesting disclosure. Although this tactic may prove effective in cases where the prosecutor and defense attorney share long-standing cordial relationships, the rationale behind the *Brady v. Maryland* line of authority, as well as the federal discovery rules, is that criminal defendants should not be forced to rely merely on the government's generosity in sharing evidence to prepare their defenses.¹⁰⁸ And any attempt by criminal defendants to enlist the courts to force the government's hand in issuing process raises serious separation of powers issues.

In cases where a criminal defendant's efforts to obtain the Internet communications at issue through the above tactics prove futile, the only recourse may be a direct challenge to the SCA. The prospects for success, on either a statutory interpretation or constitutional objection, seem minimal at best. As explained in Section III, the SCA's prohibitions on disclosure to non-governmental entities are unequivocal. Accordingly, in order to mount a statutory challenge, a criminal defendant will need to demonstrate either that an exception for criminal defendants is implied or that the exceptions applicable to "governmental entities" must be construed broadly enough to include criminal defendants within their purview. The sound reasons employed by the *O'Grady* court discussed in Section IV apply with equal force to criminal defendants, who are afforded no unique standing by the SCA.

¹⁰⁶ See generally *Miranda v. Arizona*, 384 U.S. 436 (1966).

¹⁰⁷ See, e.g., *United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002); *Wilson v. Moreau*, 440 F. Supp. 2d 81 (D.R.I. 2006); *Warshak v. United States*, No. 1:06-CV-357, 2006 U.S. Dist. LEXIS 50076, at *19 (S.D. Ohio July 21, 2006); *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006); *United States v. Maxwell*, 45 M.J. 406, 417-18 (C.A.A.F. 1996).

¹⁰⁸ *Brady*, 373 U.S. 83.

Criminal defendants seem equally unlikely to establish that the “governmental entity” exceptions should extend to them. The term “governmental entity” was defined as part of the 2006 Amendments to the SCA in connection with the 2006 Congressional Reauthorization of the Patriot Act, and specifically includes “a department or agency of the United States or any state or political subdivision thereof.”¹⁰⁹ Given the reference to “agencies” of state and federal governments, a criminal defendant represented by a state or federal public defender’s office might assert that her counsel’s issuance of a subpoena qualifies as a compelled disclosure pursuant to 18 U.S.C. § 2703(b)(1)(B). Similarly, under some state criminal discovery statutes, subpoenas are technically issued by the court, which a defendant might argue also qualifies as the “governmental entity” for purposes of § 2703.

This argument is not compelling. The purpose and plain text of the SCA make clear that the exceptions for governmental entities apply only to Fourth Amendment government actors—investigative agencies and prosecuting attorneys—and not to criminal defendants, irrespective of whether they happen to be represented by a publicly funded criminal defender’s office. First, the party seeking to compel production is not the defendant’s lawyer; it is the defendant herself. Indeed, if this reasoning were correct, criminal defendants represented by “state agencies” such as the public defender would be permitted to compel disclosure from ISPs, while criminal defendants with retained counsel, or indigent defendants represented pro bono by private lawyers, would have no such right.¹¹⁰ This absurd result is clearly not the SCA’s intent.

In fact, the language and structure of the § 2703 exceptions make clear, in several instances, that those exceptions apply to law enforcement, and not to criminal defendants. As discussed in Section II, the legislative history of the SCA evidences Congress’s intent to fill a Fourth Amendment gap by balancing the need for user privacy against the legitimate needs of law enforcement. The limitation of “governmental entity” to law enforcement is further underscored by the specific types of process that permit disclosure. For communications in electronic storage, the only means for compelling disclosure is a search warrant, a process that only law enforcement may lawfully obtain. In addition, the requisite showings to

¹⁰⁹ 18 U.S.C. § 2711(4).

¹¹⁰ Even if the public defender is viewed, by virtue of his signing the subpoena, as the “entity” seeking the disclosure, public defenders are not generally viewed as state actors. See *Polk County v. Dodson*, 454 U.S. 312, 325 (1981) (holding that public defenders do not act under the color of law when performing a lawyer’s traditional functions as counsel to a defendant in a criminal proceeding despite any employment relationship with the state).

obtain a court order pursuant to § 2703(d) and to delay notice to the subscriber under § 2705 both require actions by a law enforcement official.¹¹¹ The language in these provisions similarly renders the argument that a court could serve as the governmental entity “obtaining” the requisite process patently implausible.

The failure of the SCA’s text and legislative history to provide any recourse to criminal defendants suggests that they ultimately will be forced to contend that the SCA’s prohibitions infringe their constitutional rights. Arguing that the SCA’s uneven playing field is unconstitutional is, however, only slightly less daunting than the statutory argument. As a practical matter, given that this issue will most often arise in criminal superior courts in the context of a motion to quash a subpoena, there is likely to be a strong inclination by such courts to adhere to the long-standing Supreme Court mandate that, where possible, a statute should be interpreted so as to preserve its constitutionality.¹¹²

Although a full discussion of the potential constitutional objections a criminal defendant might raise is beyond the scope of this Article, criminal defendants can raise at least colorable claims to a deprivation of their rights to due process and effective assistance of counsel. Criminal defendants are afforded the right to due process by the constitutions of the United States and most states,¹¹³ and such rights are generally protected even in the face of contrary statutory authority. Defendants are similarly afforded the rights to effective assistance of counsel under the Sixth Amendment.¹¹⁴

Arguably, a defendant able to make a showing that the content of a victim’s e-mail messages, if available, would undermine the victim’s credibility and create reasonable doubt about the government’s case could persuade a court that the SCA’s roadblock forecloses the defendant’s due

¹¹¹ Section 2705 requires that a “supervisory official,” defined as “the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency’s headquarters or regional office, or the *chief prosecuting attorney* or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney’s headquarters or regional office” provide a written certification to delay notice. 18 U.S.C § 2705(5)-(6) (emphasis added). This definition speaks for itself. Section 2703 requires the governmental entity to show that “the records or other information sought, are relevant and material to an ongoing criminal investigation.” *Id.* § 2703(3)(d). Clearly, a criminal defendant has no authority to initiate and conduct criminal investigations, and thus cannot avail herself of this exception.

¹¹² See *NLRB v. Jones & Laughlin Steel Corp.*, 301 U.S. 1, 30 (1937).

¹¹³ U.S. CONST. amend. V & XIV; see, e.g., CAL. CONST. art. I, §§ 7, 15.

¹¹⁴ The right to counsel attaches to any critical stage of the criminal process, and although the precise standard for effective assistance is not easily defined, counsel clearly has a duty to investigate and pursue all evidence that may exonerate her client. *Strickland v. Washington*, 466 U.S. 668 (1984).

process rights and negates the defendant's counsel's ability to provide effective assistance.¹¹⁵ The defendant could assert that absent discovery of the victim's communications, the defense would be unable to identify other potential witnesses or conduct meaningful cross-examination of witnesses.¹¹⁶ At a minimum, this preclusion might suggest that due process demands that the government bears some obligation to invoke its rights under the SCA to obtain and make available such evidence.¹¹⁷

Each conceivable constitutional objection shares the same flaw, however, of centering on the obligation of the *government* to afford access to evidence or witnesses under *government control*. Here, however, the potentially exculpatory evidence is not within the government's control, even if it is potentially within its reach. The due process and effective assistance protections are not typically applied in instances where a federal statute expressly precludes a third-party intermediary from disclosing information it holds on behalf of a third-party owner.¹¹⁸ Moreover, a criminal defendant seeking to require the government to obtain and then disclose to the defendant evidence in the hands of third parties seemingly faces equally steep constitutional hurdles. The government would no doubt object on separation of powers grounds to such judicial interference with the Executive's exercise of prosecutorial discretion in pursuing evidence.

The ultimate resolution of the constitutional question is beyond the scope of this Article. The point of this Article is to demonstrate that the question is looming; that a variety of criminal courts across the country are

¹¹⁵ Presumably, to raise a constitutional concern, the defendant would need to show that the communications were only available from the ISP, and not the account holder.

¹¹⁶ *Coleman v. Alabama*, 399 U.S. 1, 9 (1970) (“[A] lawyer’s skilled examination and cross-examination of witnesses may expose fatal weaknesses in the State’s case.”).

¹¹⁷ The Supreme Court has recognized that “[c]riminal defendants have the right to the government’s assistance in compelling the attendance of favorable witnesses at trial and the right to put before a jury evidence that might influence the determination of guilt.” See *Pennsylvania v. Richie*, 480 U.S. 39, 40, 56 (1987) (also noting that the “[p]ublic interest in protecting sensitive information . . . does not necessarily prevent disclosure in all circumstances”).

¹¹⁸ In fact, the only cases to date questioning the constitutionality of the SCA center on whether the statute adequately protects the constitutional rights of the *account holder* in messages older than 180 days when the government seeks to compel disclosure with process other than a search warrant. See *Wilson v. Moreau*, 440 F. Supp. 2d 81 (D.R.I. 2006); *Warshak v. United States*, No. 1:06-CV-357, 2006 U.S. Dist. LEXIS 50076, at *19 (S.D. Ohio July 21, 2006) (holding that e-mail account holders may have a reasonable expectation of privacy in e-mail messages stored on the server of commercial ISP regardless of whether the messages are older than 180 days); *United States v. Maxwell*, 45 M.J. 406, 417-18 (C.A.A.F. 1996). A trend toward greater constitutional protection of the privacy of user accounts will certainly not advance the arguments of criminal defendants seeking disclosure of the contents of those accounts.

likely to soon confront it; and that a one paragraph amendment to the SCA would obviate the issue. In 1986, Congress stepped into an area of constitutional uncertainty and struck what has proved, despite myriad technological advancements in the intervening two decades, an effective bargain between user privacy rights and law enforcement needs. Congress should once again act to remedy a lingering gap of its own making, and strike an equally fair bargain between those same user privacy rights and the needs of criminal defendants by amending the SCA to provide private parties the ability to secure court orders to compel disclosure of Internet communications in limited circumstances.

VII. PROPOSED ECPA AMENDMENTS

Fortunately, fixing the SCA to create exceptions for the disclosure of contents of communications to criminal defendants or civil litigants is not particularly complicated. Assuming that the current court order provisions in 18 U.S.C. § 2703(d) serves as a benchmark for the type of judicial scrutiny that is desired before contents of communications should be turned over to a non-governmental entity, a similar court order provision could be added to § 2703 which allows the disclosure of information to criminal defendants and civil litigants upon a similar showing. This type of exception would actually harmonize the provisions of ECPA with a similar exception for disclosure contained in the provision of the Cable Act, which at least ostensibly governs the production of information relating to subscribers of Internet services who receive broadband service from a cable provider.¹¹⁹ A sample amendment might contain the following text:

18 U.S.C. § 2702(c)(4): Court orders by non-governmental entities.

A non-governmental entity who is a party to pending criminal or civil litigation may petition the court in which such litigation is pending for an order requiring a service provider to disclose contents of electronic communications in electronic storage or contents of wire or electronic communications in a remote computing service and such order shall issue only if the requesting party can demonstrate that the requested information is relevant and material to the ongoing litigation and is unavailable from other sources, and both the subscriber or customer whose materials are sought and the service provider from whom the materials will be produced are provided reasonable notice and the opportunity to be heard. In the case of a State court, such a court order shall not issue if prohibited by the law of such state. A court issuing an order pursuant to this section, on a motion made

¹¹⁹ The Cable Act prohibitions on disclosure, which are stricter in many ways than those contained in the ECPA, allow for disclosures about Internet subscribers to governmental entities using the same processes found in the ECPA. For non-governmental entities who seek any information about cable subscribers, whether content or records, a court order is required. See 47 U.S.C. § 551(h) (2000).

promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature, or compliance with such an order would cause an undue burden on such provider. In all cases, the service provider shall be entitled to cost reimbursement by the requesting party, as set forth in 18 U.S.C. § 2706.

This proposed amendment would harmonize the interest of the criminal defendant, civil litigant, subscriber, and ISP. It would require that before information could be produced, both the subscriber and the service provider would receive notice and an opportunity to be heard. It would preserve the ECPA's preference for requiring a subpoena to be served on the subscriber or customer, rather than the ISP, by authorizing production only when the communications are "unavailable from other sources." In addition, it would protect the interests of the ISP by allowing the ISP to move to quash or modify the order, and to recover reasonable cost reimbursement, using the same statutory mechanism that currently exists for court orders obtained by the government. In short, it preserves the balance of SCA, while fixing the collateral consequences that have adversely affected criminal defendants, civil litigants, and ISPs because of the failure of Congress to fully address the relationship between the SCA and criminal and civil discovery.

VIII. CONCLUSION

In 1986, Congress anticipated a potential gap in constitutional privacy protections for remotely-stored electronic communications, and set out to bridge that gap. In doing so, it carefully delineated the categories of information afforded protection and assigned corresponding limitations on the rights of the government to compel the production of that information. Despite some bumps along the way in applying those rules to unforeseen new technologies, the SCA has largely served its purpose well, establishing a clear regime that dictates when privacy rights must yield to the needs of law enforcement, and imposing procedural safeguards to enforce that regime.

Congress' singular focus on the interplay between ISPs and government requests for electronic content, however, has left at least one gap that remains to be filled. The present inability under the SCA for criminal defendants, and to a lesser extent civil litigants, to compel disclosure of electronic content from ISPs raises the specter of constitutional issues that the SCA has to date successfully mooted. As proposed herein, a simple amendment to the SCA that provides private parties the means to seek disclosure of content in appropriate cases, in keeping with appropriate safeguards, will clarify the law on an issue of growing contention, level the playing field for criminal defendants, and

ensure the SCA's continued role as the preeminent arbiter of rights to remotely stored electronic content.

