AN ECPA FOR THE 21ST CENTURY: THE PRESENT REFORM EFFORTS AND BEYOND

Charles H. Kennedy†

I. INTRODUCTION

Electronic surveillance in the United States is governed primarily by the Electronic Communications Privacy Act ("ECPA").¹ Most of ECPA's provisions date from 1986, before the public Internet, widespread mobile telephone service, cloud computing or social networking.² The challenge of applying ECPA's framework to technologies its drafters did not anticipate has become a source of increasing frustration for courts, law enforcement agencies, service providers and ordinary citizens.³

A number of organizations have spearheaded credible and serious reform efforts that show promise of bringing ECPA into the 21st Century, but the

¹ Partner, Wilkinson Barker Knauer, LLP; Adjunct Lecturer, Columbus School of Law, The Catholic University of America; J.D. 1976, University of Chicago. The views expressed in his article are the author's, and do not represent the opinions of Wilkinson Barker Knauer, LLP or its clients. The author is an individual member of the Digital Due Process Coalition. Who We Are, DIGITAL DUE PROCESS COALITION, http://commcns.org/rSDiFO (last visited Dec. 15, 2011).

proposed reforms are incomplete. For example, these efforts do not address foreign intelligence surveillance and the voluntary exchange of customer information among private entities. While there are sound reasons for deferring solutions to such questions, these issues should not be avoided indefinitely.

This article explores these questions by first describing the background and structure of ECPA. Next, it describes the specific, ongoing efforts to reform the statute. It concludes by recommending the adoption of reforms proposed by the Digital Due Process Coalition, and discussing additional reforms that must be considered in order to complete the project of bringing ECPA into the 21st Century.

II. ECPA: ITS BACKGROUND, TERMS AND STRUCTURE

ECPA is best understood against the background of the statute it amended: the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III" or "1968 Act"). The 1968 Act was a direct response to two landmark decisions of the United States Supreme Court: United States v. Katz, in which the Court held that the bugging of a telephone booth was a search subject to the protections of the Fourth Amendment, and Berger v. New York, in which the Court, applying Fourth Amendment principles, set out an exacting set of "superwarrant" requirements for court orders authorizing electronic surveillance. The 1968 Act was the first federal statute to place effective limits on the ability of

---


6 Notably, deferring reform of the voluntary disclosure provisions of ECPA keeps the focus on governmental action, which presents the greater risk to civil liberties. Also, deferring recommendations for change to the intelligence-gathering practices sanctioned by the Foreign Intelligence Surveillance Act keeps the focus on ECPA and avoids involving the intelligence community in the present debate. See 2010 ECPA Hearing, supra note 3, at 69-70 (memorandum from J. Beckwith Burr, Partner, Wilmer, Cutler, Pickering, Hale, and Dorr, LLP).


8 See Mulligan, supra note 2, at 1577 n.157; United States v. Katz, 389 U.S. 347, 353 (1967); Berger v. New York, 388 U.S. 41, 62-64 (1967). These decisions overturned the Court’s 1928 finding that wiretapping was not a search or seizure subject to Fourth Amendment protections. Olmstead v. United States, 277 U.S. 438 (1928).
government to intercept private communications.  

A. Statutory Framework of Title III

Title III marked the boundaries of electronic surveillance by both state and federal officials, and criminalized certain surveillance activities by private parties. Specifically, it criminalized wiretapping and electronic eavesdropping by making it an offense to intercept any wire or oral communication, except as permitted by the statute. Governmental entities were prohibited from intercepting any wire or oral communication without the consent of a party or, alternatively, an interception order obtained in accordance with a rigorous Berger superwarrant process. Private parties could only intercept wire and oral communications when a statutory exception applied, such as the consent of a party to the conversation.

The 1968 Act’s limits on interception were largely determined by the definitions of its terms. Notably, “intercept” was defined as “the aural acquisition of the contents of any wire or oral communication through the use

---

9 Before the 1968 Act was passed, the principal constraint on federal wiretapping was section 605 of the Communications Act of 1934, which stated, among other provisions, that “no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.” 47 U.S.C. § 605 (1952). As interpreted by the courts and federal law enforcement agencies, section 605 had a number of limitations; notably, it did not apply to the states and it offered no remedy for wiretaps that did not result in an effort to introduce the information obtained into evidence. See Michael Goldsmith, The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance, 74 J. CRIM. L. & CRIMINOLOGY 1, 11-13, 32 (1983); Daniel J. Solove, Surveillance Law: Reshaping the Framework, 72 GEO. WASH. L. REV. 1264, 1272-1273 (2004).


12 See id. § 2511(2). Among other provisions, Title III permitted interception orders to issue only pursuant to requests from specified officials in connection with investigations of specified, serious crimes. Id. § 2516. The interception order was required to include a finding that less intrusive investigative methods had been tried and had failed, or that those less intrusive techniques would be futile or excessively dangerous. Id. § 2518(3). Interception orders could be effective for no more than 30 days, and surveillance had to be “minimized” so that only relevant communications within the scope of the interception order were intercepted. Id. § 2518(5); Berger, 388 U.S. at 55-60 (requiring the submission of an affidavit “alleging the commission of a specific criminal offense,” a description of the “particular communication, conversations, or discussions to be seized,” and a return on the order after it is executed).

of any electronic, mechanical, or other device." By negative implication, this
definition distinguished between the "contents" of a conversation, which only
could be acquired pursuant to Title III, and non-content information such as
telephone numbers and signaling transmissions that were not subject to Title
III.15

"Wire communication" was defined as:

any aural transfer made in whole or in part through the use of facilities for the
transmission of communications by the aid of wire, cable, or other like connection
between the point of origin and the point of reception...furnished or operated by any
person engaged in providing or operating such facilities for the transmission of
interstate or foreign communications.16

An "oral communication" was defined as any "communication uttered by a
person exhibiting an expectation that such communication is not subject to
interception under circumstances justifying such expectation."17

Putting these definitions together, Title III applied to interceptions of the
contents of wireline telephone calls transmitted by common carriers, and to
any use of a device to intercept oral communications made under
circumstances that reflected a reasonable expectation of privacy in the
speaker.18

B. Terms and Structure of ECPA

Evolving communications technology soon tested the adequacy of the 1968
Act. By the time Senator Patrick Leahy (D-VT) began to consider amendments
to Title III in 1984, the common carrier, wireline environment was beginning
to yield to newer services and service providers.19 Mobile telephone service,

14 Id. § 2510(4) (2006).
15 When Congress enacted ECPA in 1986, it added a new chapter, 206, to the United
States Code that defined a process by which government could obtain non-content
information associated with telephone calls through the use of so-called "trap and trace"
from which calls are placed to a telephone; a pen register records the numbers that are dialed
from a telephone. Id. § 3127(3)-(4) (2006 & Supp. III 2009). More recently, the pen-trap
statute was amended to include governmental requests for access to email addresses and
other non-content information generated by newer communications technologies. See USA
17 Id. § 2510(2) (2006).
18 Id. §§ 2510(2), (4).
19 According to the narrative set out in the Senate Report on ECPA, consideration of an
This concerned the adequacy of existing law in order to protect the privacy of electronic
mail and computer-to-computer communications. S. REP. NO. 99-541, at 2-3 (1986). The
Criminal Division of the Justice Department responded with "Federal law protects
electronic communications against unauthorized acquisition only where a reasonable
though far from ubiquitous, was established and growing. Telephone service was available from non-common carrier sources not recognized in the 1968 Act, a result of deregulation and the divestiture of AT&T and its Bell System monopoly. Computer networking had spawned new types of communications, such as email messages and transmissions to data processing services, that could be acquired from storage long after the communications had been sent and received.

Congress easily addressed the first two developments in Title I of ECPA, which amended the definition of “wire communication” in two ways. First, Congress removed the definition’s limitation of wire communications to those facilitated by a “person engaged as a common carrier.” Second, Congress modified the definition’s description of the facilities used to carry wire communications to include mobile as well as wireline telephone facilities. With these changes, the drafters ensured that the new statute would protect all wireline and wireless voice communications transmitted by an established or competing carrier.

Congress also ensured protection for email and other computer-to-computer communications by adopting a new category of “electronic communication,” which was defined as “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 . . .” In order to avoid double classification of telephone conversations as both “wire” and “electronic,” the definition of electronic communication expressly excluded

expectation of privacy exists.” Id. at 4. This was equivalent to saying that such communications were protected, if at all, only by the Fourth Amendment.


Id. at 3.

Id. at 11, 54-55.

Id.

ECPA’s new definition of wire communication was “any aural transfer [i.e., a transfer containing the human voice] made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication.” Id. The newly-added phrase “including the use of such connection in a switching station” was intended to capture wire facilities in a cellular company’s mobile telephone switching office, which are involved in any cellular call, including those between one cell phone and another. Id. at 54-55.

“any wire or oral communication.”

The new statute created two categories of service providers: (1) the electronic communication service ("ECS"), which provides users the ability to send or receive wire or electronic communications; and (2) the remote computing service ("RCS"), which provides to the public computer storage or processing services by means of an electronic communication system.

Extending the 1968 Act's protections to include stored communications presented a more difficult problem that required more drastic changes. The 1968 Act established rules for surveillance of fleeting telephone calls and oral conversations, but those rules did not address how the government could lawfully obtain access to communications stored on the facilities of service providers. Unfortunately, the drafters of Title III did not foresee that stored information would become an integral part of modern communications, and that individuals' privacy expectations concerning stored communications would be as strong as their expectations for communications acquired in real time.

The task of defining the circumstances under which communications could be acquired from storage was further complicated by the Supreme Court's interpretation of the Fourth Amendment. There was little question that if a person's communications were stored in a computer located at his home or office, the police could only seize those communications pursuant to a probable-cause warrant. However, if those communications were maintained

---

27 Id. See also S. REP. NO. 99-541, at 56. The definition of "electronic communication" was so broad that it appeared to include wire communications, potentially making the latter category redundant. Accordingly, ECPA added the term "aural transfer" to the wire communication definition and defined electronic communications to exclude wire communications. Id. at 55-56. These modifications ensured that any communication containing the human voice would be classified as a wire communication rather than an electronic communication.


29 Electronic surveillance at the time Title III was drafted consisted of two activities: listening to wireline telephone conversations by connecting a device to the voice circuits over which those conversations were carried, and listening to oral conversations through the use of microphones, radio transmitters and other devices. The first of these activities was generally referred to as wiretapping, and the second was referred to as electronic eavesdropping or bugging. See Berger v. New York, 388 U.S. 41, 45-47 (1967). Both activities involve the use of electronic or mechanical devices to acquire the contents of communications in real time.

30 Compare United States v. Kyllo, 533 U.S. 27 (2001) (confirming that the warrantless search of a home is unconstitutional), with United States v. Miller, 425 U.S. 435 (1976) (holding that seizure of information that is maintained by a third party does not require a warrant).

31 See Kyllo, 533 U.S. 27 (police used a thermal imaging device to "penetrate" the walls of a home to observe defendant growing marijuana prior to obtaining a search warrant; held, the thermal image was inadmissible). See also United States v. Hill, 459 F.3d 966 (9th Cir.
on the facilities of a service provider, Fourth Amendment protection arguably was precluded by the third-party doctrine articulated in *United States v. Miller*.32

In *Miller*, the Supreme Court found that a bank customer had no reasonable expectation of privacy in financial documents he had "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."33 Therefore, the government's compelled acquisition of information from the bank was not a "search" for Fourth Amendment purposes.34 Extending this rationale to communications services, it could be argued that an individual who sends communications over the facilities of a service provider, which then stores the communications, has "voluntarily conveyed" those communications to the service provider and to have lost her Fourth Amendment expectation of privacy in that information.35

The arguable absence of Fourth Amendment protection for communications stored with a service provider has important consequences. If the government's compelled acquisition of information is not a Fourth Amendment "search," then the government is not required to obtain a warrant based upon probable cause, but instead may proceed with a subpoena or similar process.36 Unlike warrants, subpoenas may be based upon a mere possibility that the items or information produced will be relevant to the subject matter of an investigation.37 Issuance of a subpoena does not require the government to make a showing of probable cause before a magistrate that the items or information produced are themselves connected with the commission of a crime.38

The 1986 *Senate ECPA Report* acknowledged that a communication


32 *See Miller*, 425 U.S. at 435.

33 *Miller*, 425 U.S. at 442-444.


35 *Miller*, 425 U.S. at 442.


38 As Orin Kerr has pointed out, some courts have suggested that even if the Fourth Amendment applies to a request for information stored with a third party service provider, the Fourth Amendment's requirement of reasonableness may be satisfied by a subpoena that seeks relevant information and is not overbroad. Kerr, *supra* note 31, at 1211-12. As Professor Kerr also points out, the Fourth Amendment does not restrain non-governmental service providers from conducting private searches and sharing the results with the government. *Id.*
“subject to control by a third party computer operator” might, like the bank
records in Miller, “be subject to no constitutional privacy protection.” At the
same time, Congress recognized that “[f]or the person or business whose
records are involved, the privacy or proprietary interest in that information
should not change” simply because the information is stored with a service
provider rather than on the premises of that person or business. Accordingly,
Congress concluded that some level of protection for stored communications
was appropriate. Therefore, Title II of ECPA added chapter 121, often referred
to as the Stored Communications Act.

Chapter 121 is comprised of three principal sections: section 2701 (unlawful
access to stored communications); section 2702 (disclosure of contents); and
section 2703 (requirements for governmental access). The following discusses
each of these sections in turn.

1. ECPA Section 2701: General Prohibition Against Unauthorized Access

Section 2701 of ECPA sets out a broad set of prohibitions against
unauthorized access to stored communications. Specifically, section 2701
makes it unlawful for any person to intentionally access, without authorization,
a facility through which an ECS is provided, and thereby obtain, alter, or
prevent authorized access to a wire or electronic communication while it is in
electronic storage on that system. It also is unlawful to intentionally exceed
an authorization to access a facility through which an ECS is provided, and
thereby obtain, alter or prevent authorized access to a wire or electronic
communication while it is in electronic storage on that system.

Section 2701 includes a number of exceptions to its unauthorized access
prohibition. Specifically, there is no liability for conduct that the person or
entity providing a wire or electronic communications service has authorized, or
for conduct that a user of that service has authorized with respect to a
communication of or intended for that user. There are also exceptions for

---

40 id.
508 (1986). The nomenclature of ECPA's various parts can be confusing. Chapter 121,
consisting of 18 U.S.C. §§ 2701-2709, sometimes is referred to as the Stored
Communications Act (“SCA”), but often is referred to simply as part of ECPA. This article
follows the convention of referring to the Stored Communications Act provisions as chapter
121 of ECPA.
43 id. § 2701(a)(1).
44 id. § 2701(a)(2).
45 id. § 2701(c).
46 id. § 2701(c)(1)-(2).
An ECPA for the 21st Century

2. **ECPA Section 2702: Voluntary Disclosures**

The Fourth Amendment does not restrict the ability of private parties to make voluntary disclosures of communications to the government, nor does it prevent service providers from disclosing the contents of customer communications and information to other private parties. To ensure some level of privacy protection for subscribers and customers against voluntary disclosures by service providers, Congress wrote section 2702 of ECPA. Unfortunately, the provisions of section 2702 require a service provider to sort through a tangle of categories, definitions, overlapping rules, and confusing exceptions in order to decide whether a particular disclosure of a communication or customer record is permitted. To illustrate these complexities, it might be helpful to examine a series of hypotheticals.

**a. Content Requests from a Private Party to a Provider of ECS to the Public**

Suppose an employer retains a large, commercial email service provider to furnish email service for the workplace use of his employees. The employer then asks the service provider to disclose the contents of an employee’s email messages to and from the employer’s competitor. The email provider consults section 2702 of the statute and discovers that, because it is a provider of ECS to the public, it may not divulge the contents of those messages unless the exceptions set out in that section apply. Those exceptions include the delivery to the intended recipients of those communications and other lawful

---

47 Id. § 2703.
48 Id. § 2704.
49 Id. § 2518.
52 See, e.g., 18 U.S.C. § 2702(b)(1)-(8) (listing eight exceptions for disclosure of communications); id. § 2702(c)(1)-(6) (listing six exceptions for disclosure of customer records); id. § 2710 (defining terms like “consumer,” “ordinary course of business,” and “personally identifiable information”); id. § 2711 (defining the terms used in the entire chapter, i.e., §§ 2701-12).
53 See id. § 2702(b)-(c) (detailing the exceptions for disclosure of communications and customer records, respectively). This only relates to the disclosures of the contents of communications—not disclosures of subscriber information or transactional records. We turn to those non-content items below.
purposes "necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service . . . "54

Section 2702's exceptions also permit divulgence of the contents of communications with the lawful consent of "the originator or an addressee or intended recipient of such communication"—in this case, the employee or the person to whom the employee’s emails were sent or from which they were received.55 Accordingly, in the absence of consent by the employee or the employee’s correspondents, or unless one of the other statutory exceptions applies, the email provider must refuse the employer's request.56

Alternatively, suppose the employer brings litigation against the employee. Even if the employer were to later file suit against the employee and present the email provider with a civil subpoena demanding the contents of those same emails, none of the section 2702 exceptions would apply.57 As a result, the provider would be required to give the same, negative answer.

b. Content Requests from a Governmental Entity to a Provider of ECS to the Public

Varying the facts a bit, suppose the request for emails comes from the local sheriff pursuing an official investigation. The section 2702 exceptions do not permit voluntary disclosure to a governmental agency, except in narrow circumstances that presumably do not apply here.58 However, section 2702 permits disclosures authorized by section 2703, which outlines the means by which governmental entities may compel disclosures through warrants, subpoenas and other procedures.59 Accordingly, voluntary disclosure to the sheriff is not permitted, but compliance with a warrant or other process served by the sheriff is allowed.

54 Id. § 2702(b)(5).
55 Id. § 2702(b)(3). In the case of a remote computing service provider, the consent of the subscriber, rather than the originator or addressee, is necessary. Id.
56 If the employer’s request was instead directed to an entity classified as a provider of RCS to the public, the disclosure would be permitted with the consent of the employer as the service’s subscriber. Id. § 2702(b)(3). Consent of the employee or the employee’s correspondents would not be required. See discussion, infra Section IV.C.
57 Id. § 2702(b)-(c) (neither subpart’s exceptions covers subpoenas brought by non-governmental litigants).
58 Id. § 2702(b)(7)-(8). Among other exceptions, a service provider to the public "may divulge the contents of a communication to a law enforcement agency if the contents were inadvertently obtained by the service provider; and appear to pertain to the commission of a crime; or...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." Id.
59 Id. §§ 2702(b)(2), 2703(a)-(d) (2006).
c. **Content Requests from a Private Party to a Non-Public Provider of ECS**

Suppose instead that a private entity directs a request for some piece of stored information to another private entity that maintains a self-contained internal communications network. Section 2702 does not address the obligations of employers, private networks, and other entities that do not hold themselves out to serve the public. As a result, subject to any other privacy assurances the employer may have given, it is free to disclose the contents of its employee's emails to a private third party. The employer is also permitted to divulge the contents of those emails in response to a civil subpoena presented by the private third party.


d. **Content Requests from a Governmental Entity to a Non-Public ECS Provider**

What if the private company is asked to disclose the contents of an employee's communications voluntarily to a governmental entity? Again, because the non-public service provider is not subject to section 2702, it is not required to apply the exception permitting disclosures that are authorized by section 2703 when it deals with a governmental entity. The company/employer may turn over the emails to the governmental entity voluntarily. However, the governmental entity cannot compel it to do so except pursuant to the procedures described in section 2703. This is because the employee's emails, whether held on a private or public service, enjoy the privacy interests recognized by section 2703 when it imposes constraints on governmental access to stored electronic communications.

e. **Non-Content Requests**

It is also important to consider disclosures of customer or subscriber records that do not include the contents of communications. Under section 2702(a)(3), any RCS or ECS provider "shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity." This rule is reinforced by section 2702(c), which expressly states that an ECS or RCS provider "may divulge a record or other

---

60 *Id.* § 2702. This section only applies to public and commercial entities. *Id.*
61 Kerr, supra note 31, at 1223 ("Nonpublic providers can disclose without restriction.").
62 *Id.*
63 *Id.*; 18 U.S.C. § 2703(c).
information pertaining to a subscriber to or a customer of such service . . . to any person other than a governmental entity." Accordingly, "non-content records can be disclosed to non-government entities without restriction." 

Again, as in the case of ECS and RCS providers to the public, the private entity's disclosure of various customer records to governmental entities may be compelled only in accordance with the process described in section 2703. 

f. Putting the Voluntary Disclosure Rules Together

The complex statutory language in ECPA yields the following rules:
1. A public ECS or RCS provider may disclose the contents of a communication stored on its service to a governmental or non-governmental entity only where an exception—such as the consent of a party or subscriber or service of process by a governmental entity—applies.
2. A public ECS or RCS provider may disclose non-content customer information to any non-governmental entity. Disclosures of such information to governmental entities may be made only where an exception—such as consent of a party or subscriber or service of process by the governmental entity—applies.
3. A non-public ECS or RCS provider may voluntarily disclose the contents of a communication stored on its service to a private or governmental entity but may be compelled to do so only upon service of process.
4. A non-public ECS or RCS provider may disclose non-content customer information to any private or governmental entity but may be compelled to do so only upon service of process.

3. ECPA Section 2703: Compelled Governmental Access

Section 2703 defines the circumstances under which service providers may be compelled to disclose customers' communications and subscriber information to governmental entities. Because of the unique potential of governmental surveillance to undermine civil liberties, Section 2703 has become the main focus of the present ECPA reform effort.

---

66 Id. § 2702(c)(6).
67 Kerr, supra note 31, at 1222.
68 18 U.S.C. § 2703(c)(1). This section applies to both public and nonpublic companies.
Kerr, supra note 31, at 1222.
69 See supra Section II.B.
70 18 U.S.C. § 2702(c).
71 Id. §§ 2702(c)(6), 2703(c)(1).
72 Id. § 2703(c)(1).
73 Id. §§ 2702(c)(1), (4), (6), 2703(c)(1).
74 Id. § 2703.
75 See Appellate E-Communication Privacy Rulings Lend Impetus to Push for Reforms to ECPA, 16 ELECTRONIC COM. L. REP. 129 (Jan. 26, 2011); 2010 ECPA Hearing, supra note
Section 2703 creates an intricate set of requirements for governmental access to stored communications and subscriber information. Whether a governmental entity must obtain a probable-cause warrant or a less demanding form of process in order to compel disclosure of stored information depends upon three sets of distinctions: (1) the distinction between the contents of a communication and non-content information; (2) the distinction between an ECS and an RCS; and (3) the distinction between communications stored with an ECS for 180 days or less and communications stored for more than 180 days. The interplay of these classifications produces different levels of protection for different types of information. In some circumstances a warrant is required; in other circumstances, disclosure of the requested information may be compelled upon service of a subpoena or of a specific type of court order, not based upon probable cause, which is authorized by section 2703(d). The following describes these circumstances, and the types of process involved, in more detail.

a. When Section 2703 Requires a Probable-Cause Warrant

Section 2703 requires a probable-cause warrant only in a narrow set of circumstances: when the government seeks to compel disclosure of (1) the contents of a communication (2) that has been in electronic storage (3) with an ECS (4) for 180 days or less. Each of these four predicates for the warrant requirement requires some explanation.

i. The Content-Noncontent Distinction

The distinction between content and non-content information is fundamental. When the government seeks access to the “contents of an electronic communication that is in electronic storage,” it may be required to obtain a probable-cause warrant. However, a warrant is never required—although one may be used—for compelled governmental access to non-content information.

Fortunately, “contents” is a defined term in ECPA. “[W]hen used with respect to any wire, oral, or electronic communication, [contents] includes any

---

3, at 8 (statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy & Technology), http://judiciary.house.gov/hearings/pdf/Dempsey100505.pdf; id. at 3 (statement of Marc J. Zwillinger, Adjunct Professor, Georgetown University Law Center), http://commcns.org/sGqzzL.

76 18 U.S.C. § 2703 (2006). This discussion of section 2703 describes the section in effect today, including amendments made to that section since 1986. The discussion of sections 2702 and 2701 also refers to the current versions of those sections.

77 Id. § 2703(c)(2).
information concerning the substance, purport, or meaning of that communication.” Accordingly, any information that assists with the routing or addressing of a communication, identifies the time of the communication, or conveys information about a subscriber other than the contents of the subscriber’s communications, falls outside the contents category.

ii. Electronic Storage

Electronic storage is defined as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and . . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” Although this seems straightforward enough, application of this definition has proved confusing in practice.

The principal confusion about “electronic storage” involves emails that have been delivered and opened by their recipients and that remain in “post-transmission” storage on the service provider’s facilities. In Fraser v. Nationwide Mutual Insurance Company, a federal judge in Pennsylvania found that emails stored on a service after the recipient had opened them were neither in “temporary, intermediate storage” nor in “backup storage.” Therefore, they were not protected by ECPA. However, in 2003 the Ninth Circuit took the opposite view, finding that post-transmission storage of emails served a backup function for purposes of the electronic storage definition, and that those emails therefore were protected by ECPA. As discussed below, the United States Department of Justice prefers the Fraser position.

iii. The ECS-RCS Distinction

The level of protection for stored communications also varies according to whether the service on which the communication is stored is an ECS or RCS. As noted earlier, ECPA defines an ECS as “any service which provides to users thereof the ability to send or receive wire or electronic

---

78 Id. § 2510(8).
79 Id. § 2510(17).
81 Id.
82 Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003).
83 See discussion, infra Part III.A.
84 CONG. RESEARCH SERV., RL 34693, ONLINE DATA COLLECTION AND DISCLOSURE TO PRIVATE ENTITIES: SELECTED FEDERAL LAWS AND SELF-REGULATORY REGIMES 8 (2011).
communications. An RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." In 1986, most communications services and remote computing services could readily be classified in one or the other of these categories. However, more recent technologies, such as social networks and interactive websites, have put these classifications under considerable strain.

iv. "Time-in-Storage" on an ECS

Chapter 121 gives the contents of communications stored on ECS facilities for 180 days or less greater protection than communications stored for more than 180 days. While governmental access to the contents of communications stored by an ECS for 180 days or less will require a warrant, access to contents of communications stored for more than 180 days may be obtained with only an administrative subpoena, a grand jury subpoena, or a 2703(d) order.

The rationale for these "time-in-storage" distinctions appear to be based on the limitations of 1986-era technology and the expectations those limitations created. When ECPA was enacted, email service providers lacked the storage capacity to maintain customers' emails on their servers for long periods of time. ECPA's drafters likely assumed that any email stored in a provider's server for more than 180 days had never been retrieved by the customer, giving that customer a weak or nonexistent expectation of privacy in the contents of the message. The result is a statutory scheme in which emails stored on the customer's own computer are protected by a warrant requirement regardless of time spent in storage, but access to emails in remote storage on an ECS may or

---

86 Id. § 2711(2).
87 Compare 18 U.S.C. § 2703(a) (requiring a warrant for disclosure of contents of communications stored on an ECS for 180 days or less), with 18 U.S.C. § 2703(b) (requiring a type of subpoena or a 2703(d) order for disclosure of contents of communications stored on an RCS).
88 Id. § 2703(a).
89 Id. § 2703(b).
92 See Oza, supra note 91, at 1072.
may not require a warrant, depending upon how long they have been stored.93

b. When Section 2703 Does Not Require a Warrant: Lesser Forms of Process

When the circumstances of a governmental request for information do not trigger ECPA’s warrant requirement, a number of other types of process may come into play.

In many cases, disclosure will be demanded under a special process defined in section 2703(d) of ECPA. These so-called “2703(d) orders” require the requesting governmental entity to offer a court “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.”94 The statute permits the use of 2703(d) orders for access to the contents of communications stored with an ECS for 180 days or less, or for access to the contents of communications stored with an RCS.95 These orders also may be used to gain compelled access to subscriber records.96 Use of the section 2703(d) process, unlike a warrant, typically will require prior notice to the affected customer or subscriber; however, delayed notice may be given in certain circumstances.97

Governmental access to information may, in some cases, be based upon an administrative, grand jury, or trial subpoena. Subpoenas are sufficient to acquire information stored with an RCS or with ECS for 180 days or less.98 Subpoenas also are sufficient to compel disclosure of name, address, local and long distance telephone billing records, telephone number or other subscriber number or identity, length of service and certain other information of a customer or subscriber.99 Disclosure of certain subscriber information may be compelled pursuant to written request, in support of an investigation for telemarketing fraud.100

---

93 Kerr, supra note 31, at 1216-1219. See also Leonard Deutchman & Sean Morgan, The ECPA, ISPs & Obtaining E-mail: A Primer for Local Prosecutors, BUREAU OF JUSTICE ASSISTANCE, AMERICAN PROSECUTORS RESEARCH INSTITUTE 1, 14-15 (July 2005).
95 Id. §§ 2703(a), (b).
96 Id. § 2707(b)(2)(B).
97 Id. § 2705.
98 Id. § 2703(b).
99 Id. § 2703(c)(2).
100 Id. § 2703(c)(1)(D).
III. AFTER 1986: NEW TECHNOLOGIES AND NEW CONFUSION

As the discussion of ECPA's origins shows, the 1986 statute was a response to technological developments—such as email and mobile telephone service—that were not anticipated when Congress drafted Title III in 1968.101 If anything, the years since ECPA's enactment have seen an even greater number of dramatic, disruptive developments in the technologies and services available to users of electronic communications.102 Those developments include cloud computing, searches conducted on the World Wide Web, social networking, mobile geolocation technologies, and the enactment of various privacy laws that are in some ways inconsistent with ECPA.103 Before discussing the ECPA reform effort, it is helpful to describe each of these developments.

A. Remote Communications Storage and Cloud Computing

ECPA was enacted before the creation of the publicly accessible Internet and World Wide Web.104 To the extent computer networks existed in 1986, business and government agencies tended to operate them over proprietary facilities, rather than over systems controlled by third-party vendors.105 Remote data processing was an important method of sharing mainframe computer resources among multiple users but was not yet a pervasive method of electronic communication and information exchange.106

In that environment, ECPA's complex and inconsistent standards for governmental access to stored communications made some sense. When email

---


104 *Tim Berners-Lee Bio*, supra note 103.


106 Mulligan, supra note 2, at 1557, 1560-61 (asserting that commercial electronic mail and commercial data processing centers services were emerging in 1986 but both primarily served the business community).
server memory was scarce and service providers did not retain opened messages, it could be assumed that an email message stored on a service provider’s server for more than 180 days effectively had been abandoned by its intended recipient. Therefore, it might have been appropriate to permit governmental access to those communications upon presentation of less than a probable-cause warrant. Similarly, at a time when businesses did not extensively use third-party vendors to store confidential, digitized communications, ECPA’s differential treatment of information stored on a business’s own computers and that same information stored with a remote vendor did not have dramatic consequences.

In the years after 1986, the technical and business environment changed substantially. Email providers’ storage capacity increased as the cost of computer memory declined, allowing them to offer enormous storage capacity to their customers. As a result, customers and businesses increasingly took advantage of the growing efficiencies of remote storage and management of their electronic communications and records. Most recently, “cloud computing” has made the physical location of data obsolete as a factor in the choice of vendors and service architectures.

At the same time, ECPA’s increasingly artificial distinctions have resulted in diverging interpretations of different categories of stored data. For example, courts and law enforcement agencies have differed on the meaning of “electronic storage” under ECPA. The Department of Justice maintains that “electronic storage” refers only to “temporary storage in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity,” but “does not include post-transmission storage of communications,” such as when an email customer keeps an opened email in his or her inbox. The result is

107 Kerr, supra note 31, at 1234.
108 Julie J. McMurry, Privacy in the Information Age: The Need for Clarity in the ECPA, 78 WASH. U. L. QUARTERLY 597, 617-18 (2000) (asserting that when Congress adopted ECPA in 1986, the narrow scope was adequate to protect electronic privacy in the much smaller electronic communications systems because of the technology available at the time).
112 NEWTON’S TELECOM DICTIONARY 286 (25TH ANNIVERSARY ED. 2009).
that the Justice Department believes that it may obtain opened emails from a service provider without serving a probable-cause warrant, regardless of the message’s time in storage. However, the United States Court of Appeals for the Ninth Circuit disagrees with the Justice Department’s interpretation. If ECPA treated all stored messages the same regardless of the information requested, the type of provider, and whether storage exceeds 180 days, disputes of this kind would be moot. Even more dramatically, the Sixth Circuit ruled that the Fourth Amendment precluded the government from obtaining a criminal suspect’s emails from storage on a service provider’s facilities without a probable-cause warrant, regardless of the messages’ time in storage. The court expressly distinguished the circumstances of Miller on the ground that that case involved “simple business records” rather than the “potentially unlimited variety of confidential communications” obtainable from the appellant’s email account. The court also found that the commercial Internet service provider holding the appellant’s e-mails was an intermediary rather than an intended recipient of the information, like the bank in Miller. In the view of the Sixth Circuit, therefore, “to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.” This decision increases the pressure to reform the variable treatment of different stored communications in section 121.

B. Mobile Device Geolocation Data

Mobile telephones using cellular technology were used in 1986—in fact, one of ECPA’s purposes was to extend privacy protection to conversations carried over those new devices. The mobile telephones of that era also generated geolocation data, when they exchanged non-voice signals with local cell sites for the purpose of setting up calls and handing off those calls from one cell site to another.

114 Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004).
115 Id.
116 Id. at 1076-1077.
118 Id. at 288.
119 Id. at 286.
120 Id. at 288. “SCA” is a common abbreviation for the Stored Communications Act, which is another way of referring to chapter 121 of ECPA. Id. at 282.
122 Carlo Ratti et al., Mobile Landscapes: Using Location Data from Cell-phones for Urban Analysis, SENSEABLE CITY LABORATORY, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 1, 9-10 (2006), http://commens.org/sx1ZTC.
However, Congress did not anticipate in 1986 that mobile telephone geolocation data would become a target of governmental surveillance, and ECPA sets no standard for governmental access to that data. In recent years, as the mobile networks' own geolocation information technology has improved, and as precise global positioning system technology has been implemented on smartphones and applications, law enforcement has increasingly sought access to historical and real-time mobile device geolocation data.

The legal picture is critically confused because ECPA offers no guidance on these law enforcement requests. Until 1994, requests for geolocation data were made under the trap/trace statute, which requires only a showing of relevance to an ongoing investigation. In 1994, the Communications Assistance for Law Enforcement Act effectively prevented governmental access to geolocation data “solely pursuant” to a pen register or trap/trace order, and law enforcement responded by combining trap/trace requests with requests under chapter 121. These “hybrid” requests were not supported by a showing of probable cause.

Beginning with a decision entered in 2005, a number of courts have taken the position that government may not compel disclosure of geolocation data without first obtaining a probable-cause warrant. These decisions create

---

125 See Electronic Communications Privacy Act, 100 Stat. 1848. As the Third Circuit recently observed, the courts “are stymied by the failure of Congress to make its intention clear” on the matter of governmental access to geolocation data. In re Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 319 (3d Cir. 2010).
128 See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005).
129 Id.
130 See In re Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304 (3d Cir. 2010) (remanding government request for historical cell site data to district court to resolve possible encroachment on customer’s reasonable expectation of privacy); United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), cert. granted sub nom. United States v. Jones, 131 S. Ct. 3064 (2011) (prolonged GPS surveillance implicates a person’s reasonable expectation of privacy); In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d 578 (E.D.N.Y. 2010) (holding that government may not obtain two months’ cell phone tracking data without a warrant); In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005).
considerable pressure for an amendment to the statute that clarifies the applicable standard.

C. Transactional Data Requests and Web Searches

One of ECPA’s most important elements is the distinction between the acquisition of the contents of communications and the acquisition of non-content information concerning the circumstances of communications.\(^{131}\) The latter category is often referred to as “transactional” data.\(^{132}\) Content information is anything that discloses the “substance, purport, or meaning” of a communication; everything else associated with the communication—including the telephone numbers dialed, email addresses, and signaling transmissions—is non-content transactional information.\(^{133}\)

Compelled governmental access to content, if accomplished simultaneously with its transmission, requires a superwarrant as prescribed by Berger. Alternatively, compelled governmental access to content stored with an ECS may be supported by a warrant or, if notice is given to the subscriber, with lesser process. However, compelled governmental access to transactional data may be obtained under the pen/trap statute, requiring only a showing of relevance.\(^{134}\) If the law enforcement agent requesting the transactional information has made the required claim of relevance, the court must issue the order and is not authorized to make an independent assessment of the basis for the law enforcement agent’s claim.\(^{135}\)

The World Wide Web brought new kinds of communications that could not be as readily classified as “content” and “non-content” data. One of the most important “communications” is the Web search, which includes search terms, the URLs returned as search results, and the URLs of places visited on the Web.\(^{136}\) A URL is like a telephone number because it points to a location, but when associated with the identity of a website or the information it contains, the URL can furnish content information.\(^{137}\) Similarly, search terms typed into

\(^{131}\) See discussion, supra Section II.A.


\(^{133}\) Id.


\(^{135}\) 18 U.S.C. § 3123(a) (“[u]pon an application made under section 3122 (a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”).


\(^{137}\) Id. at 265.
a browser are queries, the content of which can be as expressive as a phrase spoken on a telephone or text placed in an email message. The URLs of the sites a person visits, as well as the search terms a person enters, may reveal a great deal about that person's interests and activities and could provide evidence of criminal intent or motive.

Thus far, there are few reported decisions in which courts have attempted to distinguish content from non-content components of these newer types of communications. However, the few decisions that are available reflect a great deal of judicial confusion. For example, one court suggested that when a URL includes a search phrase, it crosses the boundary dividing a mere Internet address (the primary function of a URL) from the content of a communication. Another court, in considering a Fourth Amendment claim, found that Internet users have no reasonable expectation of privacy in the IP addresses of websites they visit, but stated that governmental access to the “the [URLs] of the pages visited might be more constitutionally problematic” because it can point to specific documents on a website.

As new technologies and services continue to diverge from the clear content-transactional data dichotomy of traditional telephone and email services, the need for legislative guidance will grow.

D. Blurring of the ECS/RCS Boundary

The ease with which government may compel disclosure of stored information varies according to whether the service provider is an ECS or RCS. However, the application of ECPA's definitions of ECS and RCS was and is not always obvious, even for electronic services of its era. For example, when an email or text messaging service stores messages that have been retrieved by their recipients, does the service become an RCS rather than an ECS with respect to those messages? Recently, one district court concluded that the function of storing retrieved messages was an RCS rather than an ECS function, and accordingly concluded that the service provider could disclose

---

138 Id.
139 Patricia L. Bellia, Spyware and the Limits of Surveillance Law, 20 BERKELEY TECH. L.J. 1283, 1311-1312 (2005); Goldberg, supra note 136, at 265.
140 Compare Application of the United States of America for the Use of a Pen Register and Trap on Internet Service Account/User Name, 396 F. Supp. 2d 45, 49 (D. Mass. 2005), with United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007) (demonstrating different approaches used to distinguish content from non-content information).
142 United States v. Forrester, 512 F.3d 500, 510 n.6 (9th Cir. 2007).
143 See discussion, supra Part II.B.3.a.
the contents with the permission of the subscriber to the service, even in the absence of consent by the senders or intended addressees of those messages.144 The appellate court disagreed, finding that the service provider remained an ECS even after the stored messages had been retrieved.145

Newer-generation services present even more difficult cases. An example cited by Professor Orin Kerr questions whether eBay provides a data processing (RCS) service when it takes in bids for an item, calculates which bid is highest, and accepts the highest bid.146 Another unanswered question is how a social networking site should be classified when it stores and processes customers’ profile information (which looks like an RCS function) and also permits communication among customers and their “friends” (which might be considered an ECS function).147 Given the different protections afforded to ECS and RCS communications under ECPA, the answers to these questions have consequences.148

ECPA’s lesser level of protection for information stored on RCSs threatens to disincentivize businesses and individuals from migrating to cloud computing applications.149 As ECPA is written, communications stored on an ECS are protected by a probable-cause warrant requirement if they are unopened or stored for less than 180 days.150 Communications stored on an RCS are never protected by a probable-cause warrant requirement.151 Proprietary and confidential records stored with an RCS can be fully as sensitive and valuable as emails stored with an ECS. Unfortunately, the ECS-RCS dichotomy fails to recognize this reality.152 A business’s decision to take advantage of, or forego,
the efficiencies of cloud computing should not turn upon these statutory distinctions.

E. Effects of Other Privacy Laws

When ECPA was enacted in 1986, only a small number of sector-specific laws protected the privacy of personal information entrusted to third parties. The ensuing years have brought a number of such laws with obligations and protections that are more strongly imposed than those of ECPA, albeit in more specific contexts. The result is that a customer's personal information might have weak protections when the entity holding that information is subject only to ECPA and stronger protections when other laws apply.

A recent case illustrates the danger. The Internal Revenue Service ("IRS") issued an advice memorandum in response to an unnamed cable company's objection to an IRS summons that requested the disclosure of subscriber records. While the IRS conceded that disclosure of personal information concerning a cable subscriber could not be made pursuant to a summons under the privacy provisions of the Cable Act, it pointed out that the cable company also provided Internet access and telephone service. To that extent, the company was considered an ECS under ECPA. As a result, the cable company could disclose the subscriber's personal information because the Cable Act contains an exception for disclosure of subscriber information and because ECPA, unlike the Cable Act, permits disclosure of subscriber

---


Id. at 4.
information pursuant to an administrative subpoena. Although ECPA was intended as a state-of-the-art privacy statute, this case illustrates the shortcomings of both statutes.

More generally, ECPA’s voluntary disclosure provisions are making the statute an outlier in an increasingly privacy-conscious legal environment. Existing statutes in the financial services, health care, and other industries are making notice-and-consent the norm for disclosures of consumers’ information, and Congress is considering legislation that will extend that model to all sectors of the economy. At the same time, the Federal Trade Commission’s enforcement priorities emphasize the importance of adherence to privacy policies that limit companies’ discretion to collect and share personal information. In this environment, ECPA’s failure to impose similar, uniform protections for communications covered by chapter 121 on ECSs and RCSs is increasingly anomalous.

IV. THE CURRENT STATE OF ECPA REFORM

As ECPA’s inconsistency with emerging technological reality has become more apparent, a number of public and private actors have sought reform of the statute. The most notable of these initiatives are the work of the Digital Due Process Coalition and Senator Leahy of the Senate Judiciary Committee.

A. Digital Due Process Coalition Proposal

In the spring of 2010, a broad coalition of civil liberties groups, technology companies, academics, and individuals joined to take up the task of recommending reforms to ECPA. The goal of the newly formed Digital Due Process Coalition (“DDP”) was to improve ECPA’s protections for individual rights, remove uncertainties that were hindering the adoption of new technologies and economic progress, and preserve the ability of law enforcement to use legitimate surveillance and information-gathering.

158 Id.
techniques. ¹⁶²

DDP has not attempted to completely reform ECPA. Notably, DDP’s recommendations do not address foreign intelligence surveillance or the voluntary disclosure provisions of ECPA.¹⁶³ Rather, DDP’s focus is on when and how the government may compel the disclosure of communications, transactional data, and customer information transmitted and maintained by service providers during the course of criminal investigations.¹⁶⁴ DDP has announced four “consensus principles” that it believes should guide legislators as they consider amendments to ECPA.¹⁶⁵

First, the government should be required to obtain a search warrant based on probable cause before it can compel a service provider to disclose a user’s private communications or documents stored online.¹⁶⁶ Adoption of this principle would eliminate ECPA’s present distinction between private content stored on ECSs and similar content stored on RCSs.¹⁶⁷ It also would eliminate time-in-storage as the boundary between stored content subject to a probable-cause warrant requirement and content that the government may obtain with lesser process.¹⁶⁸ Furthermore, this principle would apply to all private users’ content, not just traditional “communications” such as email messages.¹⁶⁹ The probable-cause warrant requirements would apply to “word processing documents and spreadsheets, photos, Internet search queries and private posts made over social networks.”¹⁷⁰

Second, the government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.¹⁷¹ Doing so would resolve the ongoing confusion concerning governmental access to “data based on the location of cell phones, laptops and other mobile devices.”¹⁷² It would require a probable-cause warrant for real-time and historical data stored on mobile devices and on the facilities of service providers.¹⁷³

¹⁶³ Id.
¹⁶⁴ Id.
¹⁶⁶ Our Principles: Background, supra note 162.
¹⁶⁷ See discussion, supra Part II.
¹⁶⁸ Id.
¹⁶⁹ Id.
¹⁷⁰ Our Principles: Background, supra note 162.
¹⁷¹ Id.
¹⁷² Id.
¹⁷³ Id.
Third, before obtaining transactional, non-content data in real time about when and with whom an individual communicates using any communications technology, the government should demonstrate to a court that such data is relevant to an authorized criminal investigation.\textsuperscript{174} There is considerable uncertainty about the status of web search terms and other information under ECPA.\textsuperscript{175} When a court classifies that information as mere transactional data rather than as the content of a communication, it will uphold the use of a pen register and trap/trace as the government’s method of compelling access to that information.\textsuperscript{176} DDP does not propose legislation that attempts to resolve the content/transactional dichotomy for all foreseeable types of data transmission and does not favor imposing a warrant requirement for access to information that is properly classified as transactional.\textsuperscript{177} However, this third principle would reform the present trap/trace statute so that courts will have discretion to reject applications for those orders that do not meet the present statutory standard of reasonable grounds to believe that the information sought is relevant to a crime being investigated.\textsuperscript{178} The present pen/trap statute appears to deny courts that discretion.\textsuperscript{179}

Finally, before obtaining transactional data about multiple unidentified users of communications or other online services when trying to track down a suspect, the government should first demonstrate to a court that the data is needed for its criminal investigation.\textsuperscript{180} DDP does not propose to raise the standard the government must meet when it seeks compelled access to non-content information about individuals’ Internet activity.\textsuperscript{181} The principle is designed to address the concern about "bulk requests for information about everyone that visited a particular web site on a particular day, or everyone that

\textsuperscript{174} \textit{Id.}
\textsuperscript{175} See discussion, \textit{supra} Part III.C.
\textsuperscript{176} See discussion, \textit{supra} note 134.
\textsuperscript{177} \textit{Compare Our Principles: Background, supra} note 162, \textit{with discussion, supra} Part III.3. \textit{But see Our Principles: About the Issue, DIGITAL DUE PROCESS COALITION, http://commcns.org/uRCWeq (last visited Dec. 15, 2011) (guiding principles for ECPA reform are not intended to solve everything).}
\textsuperscript{178} \textit{Our Principles: Background, supra} note 162.
\textsuperscript{179} Specifically, the federal pen/trap statute states that upon receiving an application containing the representations required by the statute, a court “shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device . . .” 18 U.S.C. § 3123(a) (emphasis added). By imposing this “shall issue” requirement rather than a “may issue” provision, the pen/trap statute appears to deprive the court of authority to assess the credibility of the statements made in the application.
\textsuperscript{180} \textit{Our Principles: Background, supra} note 162.
\textsuperscript{181} \textit{Compare Our Principles: Background, supra} note 162, \textit{with discussion, supra} Part I.A. \textit{But see Our Principles: About the Issue, DIGITAL DUE PROCESS COALITION, http://commcns.org/uRCWeq (last visited Dec. 15, 2011) (guiding principles for ECPA reform are not intended to solve everything).}
used the Internet to sell products in a particular jurisdiction."\(^{182}\) For such requests, the government would be required to show that such bulk data is relevant to an investigation.\(^{183}\)

Adoption of the DDP principles in a reformed ECPA would represent a significant step forward. Notably, ECPA's artificial distinctions concerning the status of stored data would be resolved, eliminating a needless complication to the deployment of cloud computing services.\(^{184}\) Also, mobile device geolocation data would be put on par with other, equally sensitive information that already is protected by a warrant requirement.\(^{185}\) Compelled governmental access to transactional data, while still available upon a showing of less than probable cause, would be subject to meaningful judicial oversight. Lastly, blanket requests for records of online behavior would require a showing of relevance.\(^{186}\)

B. Congressional Efforts to Reform ECPA

The above principles already have influenced a reform initiative on Capitol Hill.\(^{187}\) On May 17, 2011, Senator Patrick Leahy (D-VT) introduced S. 1011, the Electronic Communications Privacy Act Amendments Act of 2011, which incorporates some of the DDP's principles.\(^{188}\)

The bill's most important provisions concern two subjects: (1) governmental access to customer communications, such as emails, that are stored on the facilities of the customers' service providers,\(^{189}\) and (2) government access to geolocation data obtained from mobile devices and service providers.\(^{190}\) While the bill would not satisfy all parties with a stake in these issues, it would clarify and simplify ECPA's treatment of these questions considerably.

On the first point, Senator Leahy's response is straightforward. Under the proposed bill, a government entity would be able to compel disclosure of the contents of a stored communication only if that entity obtained a warrant directing that disclosure.\(^{191}\) The warrant requirement applies regardless of whether the service provider was classified as an ECS or RCS under ECPA.

\(^{182}\) Our Principles: Background, supra note 162.

\(^{183}\) Id.

\(^{184}\) Id.

\(^{185}\) Id.

\(^{186}\) Id.

\(^{187}\) Id.


\(^{189}\) Id. § 3.

\(^{190}\) Id. § 5.

\(^{191}\) Id. § 3.
and regardless of the length of time the communication had been in storage.\textsuperscript{192} Similarly, and subject to some exceptions based on emergency circumstances, threats to national security, or consent of the owner or user of a device, the government must use a warrant to acquire geolocation information from a device.\textsuperscript{193} A warrant also would be required where the governmental entity wants to obtain contemporaneous or prospective geolocation information from an ECS or RCS.\textsuperscript{194} However, if the governmental entity wants only to obtain \textit{historical} geolocation information from a service provider pertaining to a subscriber or customer, process based upon less than a showing of probable cause would suffice.\textsuperscript{195}

The proposed bill includes a number of other provisions, including a clarification of the types of non-content records that law enforcement may obtain with an administrative or grand jury subpoena.\textsuperscript{196} The bill also would (1) modify ECPA’s current provisions for delayed notice to individuals concerning governmental access to their communications; (2) permit service providers to disclose communications contents that are pertinent to responding to a cyberattack; and (3) require the Attorney General and Secretary of Homeland Security to report annually to Congress on voluntary disclosures received under the “cyberattack” exception.\textsuperscript{197} Finally, it would clarify the kinds of subscriber records that the Federal Bureau of Investigation may obtain from service providers for counterintelligence purposes.\textsuperscript{198}

C. Additional Necessary ECPA Reforms

The Electronic Communications Privacy Act Amendments Act of 2011 may not become law as written and it certainly does not please everyone in the affected civil liberties, corporate, and law enforcement communities.\textsuperscript{199} However, the fact that Senator Leahy has put his considerable prestige behind ECPA reform is most encouraging.\textsuperscript{200} That said, the reforms under consideration today do not begin to exhaust the need for improvement in the

\textsuperscript{192} Id.
\textsuperscript{193} Id. § 5.
\textsuperscript{194} Id. § 6.
\textsuperscript{195} Id.
\textsuperscript{196} Id. § 3.
\textsuperscript{197} Id. §§ 4, 7.
\textsuperscript{198} Id. § 8.
federal statutory framework for electronic surveillance and information gathering. There are a number of future reforms that must be explored in order to bring ECPA fully in line with the changed circumstances.

ECPA currently permits ECSs and RCSs to disclose information concerning their subscribers, except the contents of communications, to non-governmental parties without limitation. This latitude is inconsistent with obligations to which those same service providers may be subject under other laws, such as the customer proprietary network information ("CPNI") provisions of the Communications Act and the subscriber privacy provisions of the Cable Act. Additionally, it runs contrary to the ongoing trend of privacy law in the United States, which is toward greater protection for personal information across all sectors of the economy. Reform of the voluntary disclosure provisions of ECPA should be a priority in the coming years.

Furthermore, providers of ECS and RCS to the public are generally prohibited from disclosing the contents of communications stored on their services to others, subject to a list of exceptions. Those exceptions do not include disclosures to civil litigants in response to civil subpoenas. Accordingly, disclosures in response to civil subpoenas can put service providers at risk of violating ECPA. This prohibition is a glaring exception to the scope of permitted discovery under the Federal Rules of Civil Procedure and counterpart state rules, which give civil litigants broad rights to obtain information that may lead to the discovery of material and relevant evidence. This exception has been persuasively criticized and is the subject of a number of suggestions for reform. Future reform efforts should explore

---

201 See discussion, supra Part II.B.2.e.
202 See 47 U.S.C. §§ 222, 551 (2006). The CPNI provisions require telecommunications carriers to obtain subscribers' approval before sharing certain subscriber information for the purpose of marketing services not already used by the subscriber, and before sharing such information with joint venture partners, contractors and other third parties. The Cable Act privacy provisions prohibit cable operators from using their cable systems to collect personally identifiable information of subscribers, or disclosing personally identifiable information of subscribers to others.
203 See discussion, supra Part IV.B.
204 See discussion, supra Part II.B.
206 Id. at 609.
the possibility of permitting disclosures of communications pursuant to civil discovery.

One of the most important exceptions to ECPA’s prohibition on interceptions of wire, oral, and electronic communications is for interceptions made with the prior consent of a party to the communication. ECPA does not define the form that such consent must take, requiring courts to supply the answer. For example, employers commonly seek the benefit of this exception by including it in employee handbooks. The theory behind this approach, which courts seem to have accepted, is that if such notice is clear and prominent, the employee’s decision to use the employer’s communications facilities after receiving the notice demonstrates consent to eavesdropping. However, one recent court decision has shown that employers must be careful not to make statements or engage in behavior that might suggest a withdrawal of the notice or a waiver of the right to monitor. ECPA should do more to define the conditions that constitute adequate notification.

New methods of capturing the contents of communications for commercial purposes raise questions about the form and sufficiency of user consent. Notably, an email service might scan the contents of customers’ email messages for content that suggests an interest in certain products and may provide that information to behavioral advertising agencies that create consumer databases and feed online ads on behalf of their clients. Under ECPA, those service providers have violated the law if they have not obtained user consent for those practices. Unfortunately, ECPA’s failure to define

\[\text{References}\]


211 See Quon, supra note 144, at 1123-24.


213 See, e.g., Quon, supra note 144, at 1144 (discussing employer statements establishing a reasonable expectation of privacy for Fourth Amendment purposes), aff’d in part, rev’d in part, 529 F.3d 892, 907 (9th Cir. 2008) (concurring with the district court), rev’d sub nom. on other grounds City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2630 (2010) (declining to decide whether the expectation exists but assuming arguendo that the expectation existed).

214 Compare Rittweger, 258 F. Supp. 2d at 346 (recordings of telephone conversations) and Quon, supra note 144, at 1126 (employer review of employees’ pager text message transcripts), with Ads in Gmail and Your Personal Data, GOOGLE (May 20, 2011), http://commcns.org/riRlc8 (email service provider scanning personal email content for targeted advertisement delivery purposes).

215 Ads in Gmail and Your Personal Data, supra note 214 (“Google does not and will never rent, sell or share information that personally identifies you for marketing purposes without your express permission.”)(emphasis added).

consent leaves users and service providers without guidance on this point. Is a consumer's decision to use a monitored email service, after being given an opportunity to read a privacy policy, sufficient to indicate consent? Or should explicit opt-in consent, pursuant to conspicuous notice, be required? These questions are the subject of inquiries by the Federal Trade Commission and are addressed with varying specificity in pending privacy legislation, but are also properly within the realm of ECPA reform efforts.

Furthermore, employers often wish to acquire the contents of emails and other electronic communications from storage on communications facilities furnished by the employer. The right of an employer to acquire such communications is clear when the service is provided by the employer's own facilities. In such a case, the acquisition of the stored communications is conduct authorized by the service provider for purposes of section 2701 of ECPA because the service is not offered to the public.

However, if the employer has outsourced a communications service to a third-party vendor, that vendor is subject to the constraints of section 2702 as a provider of ECS or RCS to the public. If the outside vendor is providing an RCS to the employer, then it may divulge contents of communications with the consent of the employer. Alternatively, if the outside vendor is classified as an ECS under ECPA, the vendor may divulge employee communications to the employer only with the permission of a party to those communications. Accordingly, employers that outsource electronic communications service to vendors must consider how they will preserve their right to access and review their employees' communications stored on those services. This concern

---

217 Id. § 2510 (failing to provide a definition for the term "consent").
220 See, e.g., Bohach, 932 F. Supp. at 1236.
221 See, e.g., id. See also 18 U.S.C. § 2701 (c)(1).
223 18 U.S.C. § 2702 (b)(3) ("A provider...may divulge the contents of a communication...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. (emphasis added)).
225 Compare Bohach, 932 F. Supp. at 1236 (employer who is provider of electronic communication services may "do as they wish when it comes to accessing communications in electronic storage"), with Quon, 529 F.3d at 900 (ECS subscriber cannot access communications).
impedes employers’ decisions to outsource email services and implicates employee privacy.

Finally, the pending reform effort has concentrated on ordinary criminal investigations, largely ignoring the parallel universe of national security surveillance. The foreign intelligence issues are murkier than those associated with criminal investigations, primarily because the Fourth Amendment baseline for national security investigations is less certain and unquestionably lower than the recognized constitutional protections for targets of domestic criminal surveillance. However, the reform of investigations conducted under the Foreign Intelligence Surveillance Act is just as important as ECPA reform and raises many of the same concerns.

V. CONCLUSION

Although ECPA’s age is showing, its enactment was a forward-looking legislative effort that has served remarkably well through some of the most crowded decades in the history of technology. New technologies and services, however, have strained ECPA’s definitions and distinctions to the point of unsustainability. As a matter of immediate concern, the public interest requires Congress to clarify the privacy protections that individuals can expect with respect to their nonpublic, stored information, regardless of the type of service on which that information is stored or the time it has been in storage. Congress also must create rules for governmental access to geolocation data and transactional data, and begin the process of collecting public input on other reforms discussed in this article that cannot be indefinitely deferred.


