Berkeley Technology Law Journal

Volume 18 | Issue 4 Article 1

September 2003

Electronic Evidence Compliance - A Guide for Internet Service Providers

Berkeley Technology Law Journal

ELECTRONIC EVIDENCE COMPLIANCE—A GUIDE FOR INTERNET SERVICE PROVIDERS

Prepared by the U.S. Internet Service Provider Association[†]

ABSTRACT

This Guide provides general guidelines for Internet service provider compliance with law enforcement and national security evidence gathering authorities. It is not intended to constitute or be a substitute for legal advice provided to individual clients on the basis of particular facts. In light of the law's complexity, Internet service providers should consult counsel regarding questions about the law.

TABLE OF CONTENTS

---

† Refer to Part 13 for contact information.

1 INTRODUCTION

Internet service providers ("ISPs") are increasingly being asked to provide assistance to government agencies in both criminal and national security investigations. The types of assistance being requested can take many forms, including:

- a request for *non-content records* (for example, billing records or transactional records);
- a request to *preserve* certain records or information;
- a request to implement a *pen register or trap and trace* surveillance;
- a request for *stored* electronic communications (for example, e-mail messages); or
- a request to *wiretap* a subscriber's communications.

Requests for assistance by the government are governed by a series of federal surveillance laws.[1] Assistance in criminal investigations[2] is governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968—better known as "Title III"[3]—and the Electronic Communications Privacy Act of 1986—known as "ECPA."[4] Assistance in national security investigations[5] is governed by the Foreign Intelligence Surveillance Act of 1978—better known as "FISA."[6]

Although a major purpose of these laws is to regulate how the government conducts electronic surveillance, these laws also impose obligations on private parties, including ISPs. This Guide is intended to provide an overview of the laws as they may apply to ISPs, especially after the

---

1. Most states have adopted surveillance laws that apply to state and local law enforcement agencies within their jurisdiction. These state laws generally follow the federal rules, although states have adopted more restrictive requirements in a few cases. As a result, this Guide focuses on the standard, federal rules.

2. *See* discussion *infra* Parts 8, 10.

3. Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2000 & Supp. 2003)).

4. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2232, 2510-2521, 2701-2711, 3117, 3121-3126 (2000 & Supp. 2003)).

5. *See* discussion *infra* Part 8.

6. Pub. L. No. 95-511, 92 Stat.1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-1811, 1822-1829, 1841-1846 (2000 & Supp. 2003)).

passage of the USA PATRIOT Act[7] anti-terrorism law in October of 2001 and the Homeland Security Act[8] in November of 2002. It is not meant to be a substitute for advice from a lawyer familiar with this often obscure area of the law and with the particular facts of an individual case. If in doubt, consult your own attorney.

The court's interpretation of these provisions has been disjointed due in large part to the complexity of the statutes. While the recent amendments introduced by the USA PATRIOT Act and the Homeland Security Act clarify how Title III and ECPA apply to ISPs, it may still be beneficial to interpret the laws' implications to the Internet by drawing analogies to the "plain old telephone system" and the early precursors to the Internet.

As summarized in the following chart, the surveillance laws make two general distinctions in criminal investigations. First, they distinguish between 1) historical information and 2) information acquired in real time. Second, they distinguish between 1) non-content records (such as subscriber or transactional information) and 2) the content of specific communications.

7. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C. and 50 U.S.C. (2000 & Supp. 2003)) [hereinafter USA PATRIOT Act].

8. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002) (codified as amended in scattered sections of 18 U.S.C. (2000 & Supp. 2003)).

	Historical Information	Real Time Acquisition
Non-Content Records (Subscriber or Transactional Data)	**Part 3: Customer Records** Requires subpoena (for basic subscriber information only), "section 2703(d)" court order (for other records), or consent.	**Part 4: Pen Register and Trap and Trace Devices** Requires pen register or trap and trace court order or consent
Content of Communications	**Part 5: Stored Electronic Communications** Generally requires warrant (for communications in storage less than 180 days), subpoena (more than 180 days), or consent	**Part 6: Interception of Electronic Communications** Generally requires Title III court order or consent

This Guide briefly discusses each of these categories beginning with non-content customer records (which are generally entitled to the least legal protection) and concluding with the real-time acquisition of the content of communications (which is entitled to the most legal protection). This Guide further discusses the government's authority to ask ISPs to preserve information in Part 7 and national security investigations in Part 8.

In applying the principles set forth in this Guide, ISPs must take into account their own particular technical structure. Not every ISP uses the same technology; indeed, there can be radical differences in technology that have a substantial impact both on what the law requires and on what the ISP can actually do. Thus, both ISPs and law enforcement agencies should be wary of the notion that the capabilities and obligations of one ISP can be applied freely to other ISPs with different technical structures.

2 WHICH ENTITIES ARE COVERED BY ECPA?

2.1 Provider of "Electronic Communication" or "Remote Computing" Services

ECPA addresses two types of entities: 1) providers of "electronic communication service," defined as "any service which provides to users

thereof the ability to send or receive wire or electronic communications," including electronic mail services;[9] and 2) providers of "remote computing service," which is defined as "the provision to the public of computer storage or processing services."[10] An ISP may qualify as either a provider of "electronic communication service" or "remote computing service"—or both. Take, for example, the case of a single e-mail received by an ISP for one of its customers. Before the recipient opens the e-mail, the ISP is providing "electronic communication service" because it is providing the user "the ability to . . . receive . . . electronic communications."[11] Once the e-mail has been opened, however, the electronic communication is complete. If the user does not immediately delete the e-mail, the ISP is now offering a "remote computer service." It is providing "computer storage" of the opened e-mail for the user.[12]

2.2 What Constitutes an "Electronic Communication"?

For purposes of ECPA, "electronic communication" is defined broadly to encompass a wide range of technologies. Specifically, ECPA defines an "electronic communication" 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 that affects interstate or foreign commerce[.]"[13] In the legislative history, Congress specifically identified non-voice communications consisting solely of data, communications transmitted only by radio, electronic mail, digitized transmissions, and video teleconferences as electronic communications.[14] While the statute sought to be comprehensive in the technologies it covered, it can be unclear what constitutes an "electronic communication" and what does not. In light of this ambiguity, ISPs should

---

9. 18 U.S.C. § 2510(15) (2000 & Supp. 2003).

10. 18 U.S.C. § 2711(2). Providers of electronic communication service are in turn divided into those who provide service to the public and those who do not, with different rights and responsibilities. For example, a company that runs an internal data network is a provider of electronic communication service to itself, but is not a provider "to the public." By definition, the term "remote computing service" only applies to those who provide such service to the public.

11. 18 U.S.C. § 2510(15).

12. Messages that are sent to group message boards or private fora present a unique problem. It is often difficult, if not impossible to determine if all members of a group have read the message. Thus, for some members the ISP is merely providing storage while for others the ISP is still in the process of delivering the message. How to treat such group message boards thus presents difficult legal and technical questions.

13. 18 U.S.C. § 2510(12).

14. *See* S. REP. NO. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

contact legal counsel when there is a question about whether a service could potentially qualify as an "electronic communication."

3 NON-CONTENT CUSTOMER RECORDS

Customer records include historical, non-content records such as basic subscriber information that identifies a customer's name and address and transactional information about the customer's use of a service. ECPA sets forth different standards for disclosing such non-content records depending on whether a provider is disclosing the records to a non-governmental entity or the government.

3.1 Voluntary Disclosure to Non-Governmental Entities

As discussed below, a public provider of electronic communication service or remote computing service may generally not disclose the *contents* of customers' electronic communications[15] to any third party, whether governmental or non-governmental. However, ECPA does not in any manner restrict a public provider from disclosing *records* about a customer (for example, customer user names, other identification information, and transactional records related to the account) to any entity other than a governmental entity.[16]

Therefore, a provider is not restricted by ECPA from providing records to non-governmental entities. However, to better protect customer privacy, an ISP may set standards on its own for when records will be disclosed to non-governmental entities. Although disclosure of customer records is generally not restricted by ECPA, other legal limitations may apply. Disclosures that are not in accord with the ISP's privacy policy, for example, may lead to private or Federal Trade Commission actions.

3.2 Disclosure to Government Entities

Generally, a public provider may only disclose customer records to the government either in response to compulsory process such as a subpoena or court order under § 2703 or pursuant to an exception, such as customer

15. *See infra* Parts 4, 6.

16. 18 U.S.C. §§ 2702(a)(3), (c)(6) (2000 & Supp. 2003). Although disclosure of customer records is generally not restricted by ECPA, it is important to emphasize that other legal limitations may exist. For example, the Federal Trade Commission has promised to pursue civil sanctions against companies that disclose customer records in violation of their stated privacy policies.

consent.[17] Note that in the latter case (exceptions where compulsory process is not required), disclosure is generally permissive: that is, a provider may disclose the pertinent records, but is not required to do so.

The governmental entity obtaining the records or other customer information must reimburse the provider for its "reasonably necessary" costs for assembling and providing such information.[18] Typically, a warrant or "section 2703(d)" court order will instruct the provider not to disclose the existence of the warrant or order.[19]

3.2.1 Government-Compelled Disclosure

When the government wishes to compel the production of customer non-content records, the type of legal process required depends on the type of records sought. As discussed below, non-content customer records fall into two general categories—basic and transactional.

3.2.1.1 Basic Subscriber Information

Basic information about customers is available in response to an administrative, grand jury, or trial subpoena.[20] Of course, a subpoena is not the only way the government may obtain basic information. The government may also opt to use any of the other forms of process (court order, warrant) discussed below.[21] But subpoenas are easy for investigators to obtain. They require no judicial oversight and no particular showing in terms of evidence. Congress has expanded the category considerably.[22] ECPA now mandates disclosure of the following basic information: "the (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and 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; and (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber . . . when the governmental entity uses an administrative

17. A little-used exception also allows the government to access, with a mere written request, the name, address, and place of business of a customer engaged in telemarketing fraud (as defined in 18 U.S.C. § 2325). 18 U.S.C. § 2703(c)(1)(D).

18. 18 U.S.C. § 2706(a).

19. 18 U.S.C. § 2705(b).

20. *See* 18 U.S.C. § 2703(c)(2).

21. *See id.* (noting that basic subscriber information may be compelled by "any means available under paragraph (1)" of 18 U.S.C. § 2703(c)).

22. *See* USA PATRIOT Act § 210 (codified as amended at 18 U.S.C. § 2703(c)(2) (2000 & Supp. 2003)).

subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena."[23]

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."[24] The list of subscriber information in 18 U.S.C. § 2703(c)(2) includes Internet Protocol ("IP") address information[25] and billing information (billing name, address, credit card, and/or bank account number) if the service provider is charging the subscriber for services.[26]

The last two items on the list are also the two most interesting and occasionally difficult provisions. First, the credit card number used by a subscriber to pay for Internet access is properly treated as basic information subject to subpoena. But when a credit card is used to buy other goods or services, its number is transactional information and may be obtained only with a court order under 18 U.S.C. § 2703(d), known as a "section 2703(d)" court order.[27]

Second, there is a question whether the government may use a subpoena to obtain a list of all dynamically assigned IP addresses used by a subscriber. The statute calls for production of "any temporarily assigned

---

23. 18 U.S.C. § 2703(c)(2). Note that some states require ISPs to notify customers when they receive civil subpoenas for identifying information about the customer. *See, e.g.*, VA. CODE ANN. § 8.01-407.1(A)(3) (Michie Cum. Supp. 2003), *available at* http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+8.01-407.1 (last visited on Nov. 15, 2003). California is also considering such a measure, the Internet Communications Protection Act. *See* A.B. 1143, 2003 Leg., 2003-04 Reg. Sess. (Cal. 2003).

24. ORIN KERR, DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § III.C.1, at 90 (2002) [hereinafter KERR, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS], *at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf; *see also* Jessup-Morgan v. Am. Online, Inc., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998). The court in *Jessup-Morgan* stated that

> 18 U.S.C. § 2510 states that "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication," [not information concerning the identity of the author of the communication]. 18 U.S.C. § 2510(8). The "content" of a communication is not at issue in this case. Disclosure of information identifying an AOL electronic communication account customer is at issue. In 18 U.S.C. § 2703(c)(1)(C) this identifying information is specifically acknowledged as separate from the "content" of electronic communications.

Id.

25. 18 U.S.C. §§ 2703(c)(2)(C), 2703(c)(2)(E).

26. *See* 18 U.S.C. § 2703(c)(2)(F).

27. *See infra* Part 3.2.1.2.

network address."[28] The Department of Justice has correctly concluded that this "list does not include other, more extensive transaction-related records, such as logging information revealing the e-mail addresses of persons with whom a customer corresponded during a prior session" and that "these records include the IP address assigned by an Internet service provider to a customer *for a particular session*."[29] A complete list of all dynamic IP addresses that have been assigned to a subscriber can be a large and sensitive body of data. The statute plainly allows disclosure of at least one such address, but it is not clear that it calls for disclosure of multiple addresses. For dial-up ISPs, in particular, one such address is usually sufficient to identify the subscriber, while a complete list may be more sensitive. For portals and free e-mail services, however, the IP address may be the only available method of identifying the subscriber accurately at any particular time, so a more complete list of IP addresses may be needed to provide a user's identity. In short, this is an area of considerable uncertainty.

3.2.1.2 Transaction and Other Account Records

For all other non-content customer records, the government must obtain a "section 2703(d)" court order[30] or a search warrant.[31] Examples of such customer records include transactional records, such as addresses of web sites visited by the customer and e-mail addresses of other individuals with whom the account holder has corresponded.[32] In practice, the re-

---

28. 18 U.S.C. § 2703(c)(2)(E) (2000 & Supp. 2003).

29. KERR, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, *supra* note 24, § III.C.1, at 90 (emphasis added). While this issue has yet to be addressed by a court, a broader reading of the statute, permitting government entities to obtain a log record of session times and durations with a mere administrative subpoena would eviscerate 18 U.S.C. § 2703(d), which requires a court order for information not specifically listed in 18 U.S.C. § 2703(c)(2). Since 18 U.S.C. § 2703(c)(2)(E) specifies "any temporarily assigned network address," with "address" in the singular, "temporarily" reasonably relating to a specific incident, and making no use of the term "any and all," there is a strong argument for limiting the information produced in response to administrative subpoenas to a single IP address for identification purposes.

30. In order to obtain a "section 2703(d)" court order (also known as a "specific and articulable facts" order), the government must present to a court "specific and articulable facts showing that there are reasonable grounds to believe that [the specified records] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). This "specific and articulable facts" standard is a lower standard than the "probable cause" standard the government must show to obtain a warrant.

31. 18 U.S.C. § 2703(c)(1)(B).

32. KERR, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, *supra* note 24, § III.C.2, at 90-91.

quirement for a court order or warrant for this data occasionally trips up state and local law enforcement. Because of the sharp distinction drawn by the statute between subpoenas under § 2703(c) and court orders under § 2703(d), ISPs often refuse to provide transactional data in response to court orders that are labeled "subpoenas," as may happen in some states. Law enforcement should recognize the risk that any document labeled a subpoena will be handled under § 2703(c) and not under § 2703(d), thus limiting the data available.

Similarly, some states issue court orders for discovery that do not meet the requirements of § 2703(d). These requirements include "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation."[33] A state court order that does not specify these findings will typically be rejected by cautious ISPs, or ISPs will limit disclosure to basic subscriber data.

3.2.1.3 Presence of Officer Not Required

A relatively new provision of the statute makes clear that a law enforcement officer need not be present during the service and execution of a search warrant for the purposes of obtaining customer records.[34] This provision overturns the lower court's decision in *United States v. Bach*, which held that federal law requires a law enforcement officer who obtains a warrant to search a suspect's e-mail account to be "present" when the ISP's employees retrieve the information.[35] The decision has now been overruled twice—once by Congress as set forth above and again by the Eighth Circuit, which held that allowing ISP employees to conduct a search and seizure without the supervision of an officer was not a violation of the Fourth Amendment.[36] The provision allows ISPs to accept service of warrants by fax and to extract records without the distraction and privacy risk of an investigator observing the process.[37] Many ISPs do not permit investigators to participate while technicians are examining and extracting data from their systems.

---

33. 18 U.S.C. § 2703(d).

34. 18 U.S.C. § 2703(g) (2000 & Supp. 2003). This section reflects the amendment introduced by the 21st Century Department of Justice Appropriations Authorization Act, Pub. L. No. 107-273, § 11010, 116 Stat. 1812, 1822 (2002).

35. No. 01-221, 2001 U.S. Dist. LEXIS 21853, at *10 (D. Minn. Dec. 14, 2001).

36. United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002), *cert. denied*, 123 S. Ct. 1817 (2003).

37. 18 U.S.C. § 2703(g).

3.2.2 Voluntary Disclosure of Non-Content Customer Records to the Government

ECPA allows for the voluntary disclosure of a public provider's non-content subscriber information to the government in three circumstances:

- with the customer's consent;[38]
- where the disclosure is necessary to protect the provider's rights or property;[39] and
- "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."[40]

Disclosure of the contents of subscriber communications in an emergency is discussed in Part 4.3, which should be read in conjunction with this Part. It is worth reiterating that under these provisions, service providers are under no obligation to disclose customer records to law enforcement entities absent legal process issued pursuant to § 2703. In short, a provider *may* disclose records to the government under these circumstances, but that decision is committed to the sole discretion of the service provider.

4 PEN REGISTERS AND TRAP AND TRACE DEVICES

Subject to certain exceptions discussed below, ECPA prohibits the installation of either pen registers or trap and trace devices without a court order.[41]

A pen register records the telephone numbers dialed on outgoing calls, while a trap and trace device records the telephone numbers identifying the origin of incoming calls. Neither mechanism records the *content* of a communication (which is covered by a more rigorous set of restrictions, discussed in Parts 5 and 6).[42] In the context of e-mail communications, of course, the distinction between content and non-content is not as plain as in the telephone context. In addition to subject lines, which plainly contain

38. 18 U.S.C. § 2702(c)(2).
39. 18 U.S.C. § 2702(c)(3).
40. 18 U.S.C. § 2702(c)(4) (2000 & Supp. 2003). The emergency/voluntary disclosure amendments to ECPA, added by the USA PATRIOT Act, are currently set to expire on December 31, 2005. USA PATRIOT Act § 224 (codified as amended at 18 U.S.C. § 2510 note (2000 & Supp. 2003))
41. 18 U.S.C. § 3121(a).
42. 18 U.S.C. § 3127(3)-(4).

content, even the "To" and "From" lines can contain aliases and "Send As" names that may be considered content.

Law enforcement may also use pen register and trap and trace orders to trace communications on the Internet and other computer networks. Orders for the installation of a pen register or trap and trace device may obtain any prospective non-content information associated with communications—including all "dialing, routing, addressing, [and] signaling information"[43]—utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen register and trap and trace orders cannot, however, authorize the interception of the content of a communication, such as words in the subject line or the body of an e-mail.[44]

Further, because the pen register or trap and trace "device" often cannot be physically "attached" to the target facility, 18 U.S.C. § 3123 was recently amended by the USA PATRIOT Act to allow law enforcement agencies to use software instead of physical mechanisms to collect relevant pen register or trap and trace information.

4.1 Exceptions to Prohibition Against Installing Pen Registers and Trap and Trace Devices

The prohibition against installing pen registers and trap and trace devices does not apply to devices (or software) used by electronic communication service providers:

- in relation to the operation, maintenance, and testing of their communication service;
- to protect the rights or property of the provider (for example, to bill or to detect hacking);
- to protect users of the service from fraudulent, unlawful, or abusive use of the service; or
- with the consent of the user of the service.[45]

---

43. 18 U.S.C. § 3127(3).

44. The Justice Department takes the view that the subject line of an e-mail constitutes *content* that may, along with the body of the e-mail, properly be captured only with a valid court order or other legal authority under the wiretap statute. KERR, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, *supra* note 24, § III.C.3, at 91.

45. 18 U.S.C. § 3121(b).

4.2 Law Enforcement's General Ability to Use Pen Registers and Trap and Trace Devices

Except in the very limited emergency situations set forth below, law enforcement must obtain a court order before it can lawfully install a pen register or trap and trace device.[46] An order may only authorize the installation and use of a pen register or trap and trace device for up to 60 days, but law enforcement may obtain an unlimited number of extensions, each of 60-day duration.[47] Because a court order is available to law enforcement based on its own certification (without independent evaluation by a court of the facts and circumstances supporting the application), the requirements for a pen register or trap and trace order are considerably less stringent than those for interceptions of the contents of electronic communications, discussed below.[48]

4.3 Emergency Law Enforcement Use of Pen Registers and Trap and Trace Devices

Certain specially designated law enforcement officers may authorize the installation and use of a pen register or trap and trace device before obtaining a court order if they 1) determine that an emergency situation exists involving either an immediate danger of death or serious injury or organized crime activities, and 2) subsequently obtain a court order within 48 hours.[49] Even in this type of emergency situation, the law enforcement agency must stop using the pen register or trap and trace device after 48 hours (at the latest) if it subsequently fails to obtain a court order.[50]

4.4 A Provider's Obligations to Provide Assistance

An order authorizing the installation of a pen register or trap and trace device may direct a provider to furnish the government "forthwith all information, facilities and technical assistance necessary to accomplish the installation."[51] Law enforcement must reimburse a provider for its "rea-

46. 18 U.S.C. §§ 3121(a), 3125 (2000 & Supp. 2003).

47. 18 U.S.C. § 3123(c). Note, national security-related pen registers and trap and trace devices are installed under slightly different standards, pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-11, 1822-29, 1841-46). FISA-authorized pen registers and trap and trace devices can last up to 90 days, with renewals for up to 90 days at a time. 50 U.S.C. § 1842(e).

48. *See infra* Part 6.

49. 18 U.S.C. § 3125(a).

50. 18 U.S.C. § 3125(b).

51. 18 U.S.C. § 3124(a)-(b).

sonable expenses" in providing such assistance.[52] As a general rule, the only assistance required in response to such an order is the assistance that can be provided by an ISP's existing personnel and technology. The principal exception arises in the context of pen registers, where ISPs that cannot carry out the order using their own equipment may be required to install a device (such as Etherpeek or the FBI's DCS1000) to collect the information. This is because, somewhat anomalously, the pen register provision speaks in terms of authorizing "the installation and use" of a "device." But extracting data from a complex ISP network is far more complex than attaching one of the old phone line pen registers. Few ISPs are willing to permit the use of foreign equipment on their networks in order to preserve the proper functioning of these complex systems. As a result, ISPs tend to insist on developing their own pen register tools rather than allowing the installation of other equipment for all but the simplest networks.

When a pen register "device" is installed, the law enforcement agency is required to provide to the court under seal within 30 days: 1) the identity of the officers who installed or accessed the device; 2) the date and time the device was installed, accessed, and uninstalled; 3) the configuration of the device at installation and any modifications to that configuration; and 4) the information collected by the device.[53]

Typically, an order will instruct the provider not to disclose the existence of the pen register or trap and trace device.

As a result of the passage of the USA PATRIOT Act, ECPA was amended to include two new provisions in 18 U.S.C. § 3123 that are worth highlighting. The first gives federal courts the authority to issue pen register and trap and trace orders effective outside the district of the issuing court.[54] The second provides that law enforcement authorities must file a special report with the court whenever they use a pen register or trap and trace order to install their own monitoring device (such as the FBI's DCS1000) on computers belonging to a public provider.[55]

As amended, 18 U.S.C. § 3123(a)(1) gives federal courts the authority to compel assistance from any provider of communication services in the United States. This allows a law enforcement agency to serve one order on multiple ISPs. Thus, a prosecutor's application and the resulting order will not necessarily name all providers in a communications chain. This provi-

52. 18 U.S.C. § 3124(c) (2000 & Supp. 2003).
53. 18 U.S.C. § 3123(a)(3).
54. 18 U.S.C. § 3123(a)(1).
55. 18 U.S.C. § 3123(a)(3).

sion specifies that, when a provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider.

This section also empowers courts to authorize the installation and use of pen registers and trap and trace devices in other districts. Thus, for example, if a federal terrorism or other criminal investigation based in Virginia uncovers a conspirator using an Internet account in New York, the Virginia federal court can compel communications providers in New York to assist investigators in collecting information under its pen register or trap and trace order. Consistent with this, 18 U.S.C. § 3123(b)(1)(C) does not require that federal pen register or trap and trace orders specify their geographic limits. However, since the law gives out-of-district effect to federal pen register or trap and trace orders, 18 U.S.C. § 3127(2)(A) imposes a "nexus" requirement: the issuing court must have jurisdiction over the particular crime under investigation.

5 VOLUNTARY AND COMPELLED DISCLOSURE OF STORED ELECTRONIC COMMUNICATIONS

ECPA generally prohibits unauthorized access to and disclosure of the contents of electronic communications in *electronic storage*.[56] ECPA defines "electronic storage" as: "[A]ny 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."[57]

18 U.S.C. § 2510(17) makes it clear that electronic communications in electronic storage includes unopened e-mail that is less than 180 days old.[58] E-mail that had been opened and retained on the service was thought not to be in electronic storage because it was not retained "incidental to

56. 18 U.S.C. § 2701(a).

57. 18 U.S.C. § 2510(17). The courts have not found the concept of storage easy to capture. In *United States v. Councilman*, the U.S. District Court of Massachusetts managed to characterize almost all electronic communications as "stored communications" rather than as communications in transit when it concluded that an electronic communication is in electronic storage even when it is in storage for a mere "nano-second juncture." 245 F. Supp. 2d 319, 320-21 (D. Mass. 2003). If this view stands it would mean that virtually all electronic communications would be treated as stored (and thus subject to seizure with a search warrant) rather than in transit (and thus subject to seizure only with an intercept order). Seizure by intercept order is a far more onerous process.

58. *See* KERR, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, *supra* note 24, § III.B, at 86-87.

. . . transmission."[59] However, in *Theofel v. Farey-Jones*,[60] the Ninth Circuit held that electronic communications that had been opened and were kept by the Internet service provider merely for the convenience of the customer were still in electronic storage because they were kept for purposes of backup protection and covered by 18 U.S.C. § 2510(17)(B). This has potentially far-reaching implications because governmental entities may obtain communications that are no longer in electronic storage by subpoena with notice, or by court order pursuant to 18 U.S.C. § 2703(d).[61] The holding in *Theofel* means the government must get a search warrant in order to obtain the contents of any electronic communication that has been stored by an ISP for less than 180 days.

Whether the holding in *Theofel* will ultimately be proven correct is open to some question. The opinion was issued just before this Guide went to press and petitions for rehearing have been filed. Moreover, this is the first appellate interpretation of this particular provision and other circuits may come to different conclusions on the meaning of the language in the statute. However, for the present time this opinion is controlling in the Ninth Circuit and represents the only circuit court opinion interpreting 18 U.S.C. § 2510(17).

5.1 Voluntary Disclosure of Stored Electronic Communications

Subject to certain exceptions, providers of electronic communication service or remote computing service *to the public* are prohibited from knowingly divulging the contents of any customer communication (those who provide private communications and storage services are not so regulated).[62] Disclosure of the contents of a communication is permitted, however, in the following circumstances:

- to an addressee or intended recipient of the communication (or his agent);
- as otherwise authorized by a court order or some other legal authorization;
- "with the lawful consent of the originator or an addressee or intended recipient of such communication or the subscriber in the case of a remote computing service;"

---

59. 18 U.S.C. § 2510(17)(A) (2000 & Supp. 2003).
60. 341 F.3d 978, 984-85 (9th Cir. 2003).
61. 18 U.S.C. § 2703(a)-(b).
62. 18 U.S.C. § 2702(a).

- for the purpose of forwarding a communication to its destination;
- if necessary to provide the service or to protect the rights or property of the provider;
- to law enforcement, "if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"
- "to a Federal, State, or local 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[;]" or
- if the ISP has knowledge of child pornography, required by 42 U.S.C. § 13032 (where violation of child pornography laws is apparent).[63]

For any other disclosures to the government, the government must obtain a warrant, court order, or subpoena, depending on the age or type of the communication, as described below.

Law enforcement agencies sometimes invoke the "emergency" provision in an effort to avoid the necessity of a subpoena or other process. ISPs often must be firm in pointing out that this provision gives the ISP, *not* law enforcement, authority to decide whether or not to provide information. There is never an "emergency" obligation on an ISP to disclose under § 2702(b)(7). In a true emergency, ISPs are usually ready to respond, but they typically insist that investigators provide a clear basis on which the ISP can conclude that an emergency meeting the statutory criteria exists. The law requires that the ISP reasonably "believe[] that an emergency involving danger of death or serious physical injury to any person requires disclosure [of the information] without delay . . . ."[64]

Because of the intense interest of agencies in this exception, it is prudent for an ISP to adopt clear procedures for its use, and to require all government agencies to adhere to the procedures. Some ISPs provide forms to be filled out by investigators, sometimes under penalty of perjury. These forms can help to focus investigators by requiring the information needed to satisfy the statute (for example, "What is the danger of death or serious physical injury?" and "Is the danger immediate?"). Transmitted along with a cover letter on the letterhead of a law enforcement agency, such docu-

63. 18 U.S.C. § 2702(b).
64. 18 U.S.C. § 2702(b).

ment agency, such documentation provides a useful backup in case the ISP's decision to release information voluntarily is ever questioned.

5.2 Law Enforcement's Ability to Compel Production of the Content of Stored Electronic Communications

Although ECPA does not on its face draw a distinction between opened and unopened e-mail, this is a central dividing line in practice. ECPA provides heavy protection for communications while they are in the process of transmission (for example, an unopened e-mail).[65] As long as the e-mail remains in "electronic storage" (for example, unopened in an inbox), it is protected quite heavily for 180 days. After electronic communications in "electronic storage" have remained undelivered for 180 days, law enforcement may access the contents under less rigorous legal authorizations, including an administrative, grand jury, or trial subpoena.[66] But all of that depends on the communication remaining undelivered. Once an electronic communication has been opened by its recipient, it is no longer in transmission. The ISP is no longer providing "electronic communication service" but is now providing a "remote computing service." The communication is protected only as a stored communication and is accessible under the less rigorous legal authorizations of 18 U.S.C. § 2703(b).[67]

When a governmental entity obtains the content of electronic communications that have been in electronic storage more than 180 days with process other than a search warrant, the government (not the ISP) is required by law to give prior notice to the customer.[68] However, the government may delay notification for up to 90 days if there is reason to believe that notification would result in: 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) otherwise seri-

---

65. 18 U.S.C. § 2510(17) (2000 & Supp. 2003).

66. 18 U.S.C. § 2703(b). These requirements apply to a remote computing service provider to the extent that

> any wire or electronic communication . . . is held or maintained on [its] service—(A) on behalf of, and received by means of an electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service.

18 U.S.C. § 2703(b)(2).

67. *See supra* Part 2.1.

68. 18 U.S.C. § 2703(b).

ously jeopardize an investigation.[69] The government may obtain subsequent extensions of this delay in providing notice.

5.3 A Provider's Obligations to Provide Assistance

A provider must comply with an appropriate legal authorization to provide the government with access to the stored communications identified in the order. The governmental entity obtaining the contents of such stored communications, however, must reimburse the provider for its "reasonably necessary" costs directly incurred for assembling and providing such information.[70]

5.4 Back-up Copies

Under a very rarely used provision, if a governmental entity determines (at its discretion) that there is reason to believe that prior notification to the customer of the existence of a court order or subpoena may result in destruction of or tampering with stored communications, it may require that the provider create a back-up copy of the contents of the electronic communications at issue before such notice is provided to the customer.[71]

Without notifying the customer, the provider must create a back-up copy within two days of receipt of the order.[72] The provider must not destroy this back-up copy until the later of: 1) its delivery to the governmental entity, or 2) the resolution of any proceedings concerning the court order or subpoena.[73] Note, unlike the preservation requirement[74] (which predates a court order and applies to stored communications as well as customer records), the obligation to create back-up copies applies after a court order or subpoena is served and applies only to stored communications (not customer records).

5.5 Civil Requests for E-mail Content

Most ISPs receive discovery requests in civil matters on a routine basis. These requests may not be as numerous as criminal requests, but responding is often more complicated and time consuming. First, the sources of civil requests—federal enforcement agencies such as the Securities and Exchange Commission ("SEC") or the Federal Trade Commission

69. 18 U.S.C. § 2705(a)(1)-(2).
70. 18 U.S.C. § 2706(a).
71. 18 U.S.C. § 2704(a)(5) (2000 & Supp. 2003).
72. 18 U.S.C. § 2704(a)(1).
73. 18 U.S.C. § 2704(a)(3).
74. *See* discussion *infra* Part 7.

("FTC"), and private litigants—are often not familiar with the technology or legal constraints related to subscriber data held by ISPs. Second, the legal framework that allows government entities access to subscriber data does not provide helpful guidance on the appropriate mechanisms for private entities to compel production of records. Third, unlike in the criminal context where ISPs are unlikely to provide notice to subscribers, in the civil context many ISPs seek to give their subscribers notice of requests for their account data. Indeed, in certain jurisdictions ISPs may be required to provide notice.[75]

While ISPs are free, subject to their privacy policies, to provide identity and other non-content information to civil litigants (or, indeed, to other private parties), they are more restricted in divulging content. Section 2702(a) prohibits an ISP (either a provider of "electronic communication service" or a "remote computing service") from divulging "the contents of a communication." Section 2702(b) offers several exceptions to the prohibition, but none of them expressly permits disclosure pursuant to a civil discovery order unless the order is obtained by a government entity. This issue has not been litigated to our knowledge, but in some cases courts have managed to avoid the issue by ordering the subscriber to give consent to the disclosure of the contents of his or her e-mail, a compromise that only works when the subscriber is subject to the court's jurisdiction. Thus, the federal prohibition against divulging e-mail contents remains stark, and there is no obvious exemption for a civil discovery order on behalf of a private party. ISPs can, of course, voluntarily preserve the contents of an account pending receipt of a court order, if such an order can be obtained.

6 INTERCEPTION OR DISCLOSURE OF ELECTRONIC COMMUNICATIONS

Subject to certain exceptions discussed below, ECPA prohibits the intentional "interception" of any electronic communication, or the intentional disclosure or use of the contents of an intercepted electronic communication.[76] This prohibition applies to everyone, not just government officials; however, a violation of this statute occurs only when one "intentionally" intercepts an electronic communication or intentionally uses or divulges such an intercepted communication.

---

75. VA. CODE ANN. § 8.01-407.1(A)(3) (Michie Cum. Supp. 2003). Other states have also considered notice requirements. *See, e.g.*, H.B. 2203, 84th Gen. Assem., Reg. Sess. (Ark. 2003); A.B. 1143, 2003 Leg., 2003-04 Reg. Sess. (Cal. 2003).

76. 18 U.S.C. § 2511(1).

6.1 What Constitutes an "Interception"?

An "interception" of an electronic communication (such as an e-mail message) occurs when someone other than the intended recipient gains access to the communication during the *transmission* phase.[77] Technically, ECPA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[78] As previously discussed, access to communications that are in *electronic storage* is governed by separate rules.[79]

6.2 Exceptions to Prohibition Against Intercepting Electronic Communications

The prohibition against intentionally intercepting electronic communications is subject to the following notable exceptions:

- **"Normal Course of Business"**: A provider whose facilities are used in the transmission of an electronic communication may intercept, disclose, or use that communication in the "normal course of business" if necessary to provide the service or to protect the rights or property of the provider.[80] For example, caching and temporary buffering of messages during communication fall under this exception. While this exception is fairly broad, it may not apply to malicious acts committed by an employee of the provider.

- **Compliance with Lawful Court Order**: A provider is authorized to provide information, facilities, or technical assistance to law enforcement when the provider has been served with a court order or other appropriate legal authorization.[81]

- **Consent of Party to Communications**: Any private citizen may give consent to the interception of an electronic communication where that person is a party to the communication.[82] Consent may

77. *See* United States v. Smith, 155 F.3d 1051, 1056-58 (9th Cir. 1998); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460-62 (5th Cir. 1994); Wesley Coll. v. Pitts, 974 F. Supp. 375, 385-86 (D. Del. 1997).

78. 18 U.S.C. § 2510(4) (2000 & Supp. 2003).

79. *See* discussion *supra* Part 5.

80. 18 U.S.C. § 2511(2)(a)(i).

81. 18 U.S.C. § 2511(2)(a)(ii).

82. 18 U.S.C. § 2511(2)(d). This "one-party consent" rule is the Federal rule. The law of some states establishes a more stringent "all party consent" rule, which makes it illegal under state law to intercept a communication without consent of all parties to the communication. Note, however, that it is not an "interception" for the sender or recipient

be explicit or implied, as is the case with "logon banners" displayed when logging onto many governmental networks, which state that by using the system one consents to monitoring by the entity administering the system.

- **Fraudulent, Unlawful, or Abusive Use of Service**: A provider may record the fact that an electronic communication was initiated or completed in order to protect itself, another provider furnishing service to the communicating parties, or a user of the provider's service from fraudulent, unlawful, or abusive use of the service.[83] An example from traditional telephony is when a carrier traces harassing phone calls.

- **Interception of Computer Trespasser Communications**: The owner or operator of a computer who is the victim of an attack by a trespasser may authorize law enforcement to intercept the trespasser's communications on the protected computer.[84] Service providers are not *required* to invite law enforcement to monitor such trespasser communications but, if they wish to do so, 18 U.S.C. § 2511(2)(i) provides an exception to the general prohibition on intercepting electronic communications. A "computer trespasser" includes anyone who accesses a protected computer without authorization, but specifically excludes someone who has a contractual relationship with the computer owner/operator for access to all or part of the computer, for example, an authorized user who is merely violating the service provider's terms of service.[85] The statute provides immunity from liability for all claims against service providers who invoke this provision.[86]

6.3 Exceptions to Prohibition Against Divulging Contents of Electronic Communications

As noted above, a provider of electronic communication service is generally prohibited from divulging the contents of such communications.[87] However, that prohibition is subject to the following exceptions:

---

of an e-mail to disclose the contents to someone else, either to a private individual or to the government.

83. 18 U.S.C. § 2511(2)(h)(ii).
84. 18 U.S.C. § 2511(2)(i) (2000 & Supp. 2003).
85. 18 U.S.C. § 2510(21).
86. H.R. REP. NO. 107-236, pt. 1, at 58 (2001).
87. 18 U.S.C. § 2511(3)(a).

- if either the "normal course of business" or "pursuant to lawful court order" exceptions discussed above in Part 6.2 apply;
- with the lawful consent of the originator or any addressee or intended recipient of the communication (this could include consent provisions that are part of the provider's standard terms of service);
- to a person employed, or whose facilities are used, to forward the communication to its destination (for example, another ISP);
- to law enforcement, if the communication was inadvertently obtained by the provider and appears to pertain to the commission of a crime;[88] or
- as may be necessarily incident to the rendition of services or the protection of the rights or property of the service provider.[89]

6.4 Law Enforcement's Ability to Intercept Electronic Communications

Law enforcement must meet a fairly stringent set of requirements for authorization to intercept electronic communications in *transmission* (although, access to communications in *electronic storage* is governed by a different set of standards discussed in Part 5 above).

Except in the very limited emergency situations set forth below, a governmental entity must obtain a court order before it can lawfully conduct an interception.[90] ECPA limits the duration of the interception to 30 days (although the order can be renewed in 30-day increments on application to the issuing court).[91]

6.4.1 Law Enforcement Interception of Electronic Communications in Emergency Situations

Certain specially-designated law enforcement officers may authorize the interception of electronic communications before obtaining a court order if they 1) determine that an emergency situation exists involving an immediate danger of death or serious injury, activities that threaten national security, or organized crime activities, and 2) apply for a court order within 48 hours.[92] Even in this type of emergency situation, law enforce-

88. 18 U.S.C. § 2511(3)(b)(i)-(iv); 18 U.S.C. § 2702(b)(1)-(4).
89. 18 U.S.C. § 2702(b)(5).
90. 18 U.S.C. §§ 2516, 2518 (2000 & Supp. 2003).
91. 18 U.S.C. § 2518(4)-(5).
92. 18 U.S.C. § 2518(7).

ment must stop conducting the interception when the communication sought is obtained or when the application for an order is denied, whichever is earlier. If the application is denied, the contents of any communications already intercepted are likely to be viewed as having been obtained in violation of ECPA. Hence it is both prudent and a common practice among ISPs to obtain either a court order or a certification in writing that an emergency situation exists and that no court order is required before conducting an interception of a communication.

6.5 A Provider's Obligation to Provide Assistance

An order authorizing the interception of electronic communications may direct a provider to furnish "forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively."[93] Although the scope of this assistance is not defined in the statute, such an order would, at least under most circumstances, require a provider to promptly use its equipment or facilities to accomplish the interception unobtrusively. On the other hand, the Supreme Court has held that "the power of federal courts to impose duties upon third parties is not without limits; unreasonable burdens may not be imposed."[94]

A governmental entity must reimburse a provider for its "reasonable expenses" in providing interception assistance.[95] Typically, an order will instruct the provider not to disclose the existence of law enforcement's interception.

7 PRESERVATION REQUESTS

7.1 Preservation

The government may request that a provider *preserve* stored electronic communications, customer records, and other evidence in its possession, without turning them over to the government, pending the issuance of a legal process.[96]

The federal government has informally taken the position that, because the statute does not explicitly require a written request, the obligation to

---

93. 18 U.S.C. § 2518(4).

94. United States v. N.Y. Tel. Co., 434 U.S. 159, 172 (1977).

95. 18 U.S.C. § 2518(4).

96. 18 U.S.C. § 2703(f) (2000 & Supp. 2003). Note that this provision has a limited effect because "no law regulates how long network service providers must retain account records in the United States." KERR, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, *supra* note 24, § III.G.1, at 104.

preserve evidence attaches when the ISP receives a preservation request by telephone. However, an ISP that receives a telephone preservation request should request a confirmation letter for its own protection. Preservation requests only apply to stored communications and records that the provider has in its possession at the time of the request.[97] Preservation requests potentially can be burdensome, but the government has sometimes been willing to negotiate the scope of the request in order to reduce the burden on companies that receive a large number of such requests.

7.2 Nondisclosure

It is common for law enforcement agencies to instruct an ISP not to disclose to its subscriber the fact that a subpoena or other process targeting the subscriber has been served on the ISP. 18 U.S.C. § 2705(b) provides a basis and a procedure for nondisclosure orders:

> A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—
>
> (1) endangering 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) otherwise seriously jeopardizing an investigation or unduly delaying a trial.[98]

---

97. The Justice Department has taken the position that under § 2703(f), a law enforcement agent "can order a provider to preserve records that have already been created, but cannot order providers to preserve records not yet made." While other provisions in ECPA permit prospective orders, § 2703(f) does not, because law enforcement officers must comply with electronic surveillance statutes to obtain prospective communications. KERR, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, *supra* note 24, § III.G.1, at 105.

98. 18 U.S.C. § 2705(b).

This is an area in which formalities matter. Law enforcement agencies sometimes serve a subpoena and include nondisclosure language in the cover letter transmitting the subpoena. This procedure does not conform to § 2705(b), which requires a separate nondisclosure order from a court.

This provision raises other difficulties for ISPs. First, what happens when a nondisclosure order from one court is followed by a subpoena from a second court seeking all records in response to the first subpoena? This can occur in criminal cases when the defendant seeks to review the propriety of the prosecutor's searches. As a rule, it is prudent to assume that the nondisclosure order remains in effect and bars the second subpoena unless the order is lifted by the first court, or is at least considered and specifically superseded by the second court. ISPs often solve the problem by insisting that the prosecution give the defendant any materials received in response to the earlier subpoena, rather than requiring the ISP to go through the discovery process twice.

A second problem concerns state nondisclosure orders. State law and practice varies widely, and it is not always easy to know whether a nondisclosure order meets state law requirements. In addition, there is a reasonable, but untested, view that federal law preempts state law on this point, so that states must follow the procedures of § 2705 to impose a nondisclosure obligation on ISPs. Because of this uncertainty, ISPs are reluctant to rely solely on such orders to provide protection from liability for disclosure. ISPs therefore typically adopt privacy policies that notify subscribers that the ISP may respond to criminal investigative subpoenas or other law enforcement discovery orders without providing notice to the subscriber.

Finally, there is a question whether a nondisclosure obligation may be created by something short of a court order. Sections 2703(b)(1) and 2705(a)(1), when read together, seem to suggest that nondisclosure orders may not be available when the government uses a subpoena. Instead, the subpoenaing agency may simply delay its own notice to the subscriber. But the law enforcement agency is likely to argue that the delayed notice provision is binding on the ISP as well. While this view is questionable, no definitive interpretation of the provision is yet available. ISPs asked to follow this view are likely, at a minimum, to demand particularly strict adherence to the procedural requirements for such a delayed notice, including a copy of the "written certification of a supervisory official" required by § 2705(a)(1)(B).

8 NATIONAL SECURITY INVESTIGATIONS

Orders of the Foreign Intelligence Surveillance Court are classified. Government regulations provide that classified information may only be provided to individuals who have the appropriate security clearance and have a need to know the classified information. Although the FBI sometimes presses ISPs to obtain clearances in order to see FISA orders, such clearance is not required. As a rule, the government may not require a private citizen to obtain a clearance and thus become subject to many new legal liabilities and obligations. Nor may the government require a private citizen to obey court orders without letting the citizen see the order. Thus, if the government wants a FISA order carried out, it must show it to the ISP's personnel, whether or not the personnel agree to obtain clearances. In an emergency, the regulations have procedures permitting the government to provide classified information to an uncleared individual. An ISP without cleared personnel may insist on the use of this provision.

The regulations also require that classified information be stored in a government-approved secure facility. The government is on stronger ground when it refuses to allow the ISP to keep copies of classified documents in facilities that are not secure. If a company does not have such a secure facility, the FBI will show the FISA court order to the company and give the company a trust receipt; the FBI will retain the classified court order.

Company personnel who receive, or who are shown, a classified Foreign Intelligence Surveillance Court order may consult with company executives or with legal counsel where necessary. It is the government's position that such company personnel may not provide any classified information (for example, the name of the target of the search or surveillance, any identifying information about the target, or any classified information about the technique the government is using) to uncleared personnel. Certainly it is prudent for ISP personnel to avoid unnecessary disclosure of such information; however, in some cases disclosure of some classified information is necessary to provide a full view of the risks to the CEO or of legal issues to outside counsel. Classified information may not be used as a way to avoid an ISP's normal corporate oversight or legal clearances. The scope of any expected disclosure should be made clear to the government officials who serve the court order, however, because the government may wish to withdraw the order rather than accept the disclosure that the ISP deems necessary to brief management properly.

Whether to obtain security clearances and establish secure facilities for storage of orders is not a simple decision. The government will press

heavily for full security approval, but before agreeing to do so, ISPs should be sure that they know the full cost of security arrangements and whether the government will reimburse those costs.

8.1 Customer Records

As noted before,[99] a provider is generally not permitted to disclose customer records to the government without appropriate legal authorization. The FBI has three different authorities for obtaining such records in national security investigations.

8.1.1 FISA Order for Business Records

First, the FBI may obtain a court order from the Foreign Intelligence Surveillance court to require "the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[100] It is not entirely clear whether this authority covers electronic records. For example, are stored customer e-mails "tangible things"? Do they become tangible things if they are burned to a CD? Given the emphasis on documentary evidence in this provision, it seems likely that the government will argue that electronic documents do fall within its scope, notwithstanding their intangibility.

If a provider is served with an order for such business records, it is prohibited from disclosing the fact that the FBI had sought or obtained those items.[101] However, this confidentiality requirement is not intended to prevent company personnel from seeking guidance from company executives or inside or outside legal counsel where necessary. A provider that complies in good faith with an order to provide such business records is immunized against any liability.[102]

8.1.2 FISA Order for Physical Search

Second, the government also may obtain a court order to conduct a physical search of premises or property within the United States that is "intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property."[103] Under a physical search order, an ISP may be directed to "furnish all information, facilities, or assistance

---

99. *See supra* Part 3.2.
100. 50 U.S.C. § 1861(a)(1).
101. 50 U.S.C. § 1861(d).
102. 50 U.S.C. § 1861(e).
103. 50 U.S.C. § 1821(5) (2000 & Supp. 2003).

necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such [ISP] . . . is providing the target of the physical search."[104] A FISA order for physical search is analogous to a search warrant in the criminal context and may be used to obtain communications and content stored in the target user's account. Unlike a search warrant, a FISA order for physical search typically has a duration of 90 days (it may be up to one year under certain circumstances), but this does not mean that a series of searches may be carried out over that period. Instead, it generally authorizes the government to complete a single search within that time.

Service providers are required to maintain records related to a secret search in accordance with security procedures set by the Attorney General and the Director of Central Intelligence.[105] The government must compensate providers "at the prevailing rate" for assistance provided under this section.[106]

8.1.3 Certification for Subscriber Information and Toll Records in Counter-Intelligence Investigations

The Director of the FBI is authorized to issue a certification, generally described as a "national security letter," requiring a provider to release certain subscriber information and toll records, as well as "electronic communication transactional records." Such a letter takes the place of the subpoena, search warrant, or court order that otherwise would be necessary.[107] This provision is an awkward one for ISPs, mainly because it uses terms that do not appear elsewhere in the electronic intercept statutes and are not defined. Viewed in relation to the more precise provisions of § 2703, § 2709 seems to give the government access both to subscriber identity information (subscriber information and toll billing records information) of the sort described in § 2703(c) as well as access to most of the transactional information covered by § 2703(d). But perhaps not all. Because this section is limited to "electronic communication transactional records," records of other transactions (for example, purchases from an online store) would not be made available in response to a national security letter, but would be available in response to a "section 2703(d)" order.

---

104. 50 U.S.C. § 1822(a)(4)(A)(i).

105. 50 U.S.C. § 1822(a)(4)(A)(ii).

106. 50 U.S.C. § 1822(a)(4)(B).

107. 18 U.S.C. § 2709. While the certification may require a telecommunications provider to disclose "local and long distance toll billing records" for the subscriber, ISPs do not maintain such records and, therefore, are not required to disclose them.

A provider is prohibited from disclosing that the FBI had served a certification for such basic subscriber information.[108] However, as mentioned above, company personnel may discuss the certification, as necessary, to get guidance from company executives or legal counsel. Providers that comply with a certification to provide such basic subscriber information are immunized against any liability.[109]

8.2 Pen Registers and Trap and Trace Devices

As in criminal investigations,[110] the government can also obtain a pen register or trap and trace order in national security investigations. Generally, these FISA pen register or trap and trace orders are treated almost identically to criminal pen register or trap and trace orders.

8.2.1 The Government's Ability to Use FISA Pen Register and Trap and Trace Surveillances

Except in the very limited emergency situations set forth below, the government must obtain a FISA order before it can lawfully conduct a pen register or trap and trace surveillance in a national security investigation.[111] An order may only authorize the installation and use of a pen register or trap and trace device for up to 90 days, although the government may obtain an unlimited number of 90-day extensions.[112]

Like the modifications to ECPA's pen register and trap and trace provisions,[113] the USA PATRIOT Act also amended FISA to clarify the government's ability to use pen register and trap and trace devices to capture routing information for electronic communications. FISA's original statutory language had referred to "telephone lines," which had raised questions about whether the pen register and trap and trace authority could be extended to Internet communications (such as e-mail or web browsing). The USA PATRIOT Act resolved this ambiguity by expanding the statute's language to include any "other facility to which the pen register or trap and trace device is to be attached or applied."[114]

---

108. 18 U.S.C. § 2709(c).
109. 18 U.S.C. §§ 2703(e) & 2707(e) (2000 & Supp. 2003).
110. See *supra* Part 4.
111. 50 U.S.C. § 1842.
112. 50 U.S.C. § 1842(e). In contrast, criminal pen register/trap and trace orders and extensions only last 60 days. 18 U.S.C. § 3123(c).
113. See *supra* Part 4.
114. 50 U.S.C. § 1842(d)(2)(A).

8.2.2 Emergency Law Enforcement Use of Pen Register and Trap and Trace Surveillances

The Attorney General may authorize the installation and use of a FISA pen register or trap and trace surveillance before obtaining a court order, but only if the Attorney General: 1) determines that an emergency exists requiring the immediate installation of the surveillance before an order "can with due diligence be obtained;" and 2) subsequently applies to the Foreign Intelligence Surveillance court for an order within 48 hours.[115] Even in this type of emergency situation, the government must stop using the pen register or trap and trace surveillance after 48 hours (at the latest) if it subsequently fails to obtain a court order.[116]

8.2.3 A Provider's Obligations to Provide Assistance

An order authorizing the installation of a pen register or trap and trace surveillance may direct a provider to furnish "any information, facilities, or technical assistance necessary to accomplish the installation and operation."[117] The government must reimburse a provider for its "reasonable expenses" in providing such assistance.[118] No cause of action can be brought against a provider for furnishing any assistance or information in accordance with a FISA pen register or trap and trace order.[119]

As mentioned above, FISA pen register and trap and trace orders are governed by special confidentiality requirements. A FISA order will direct a provider to maintain the order and "any records concerning the pen register and trap and trace device or the aid furnished" in compliance with the security procedures approved by the Attorney General and the Director of Central Intelligence.[120] Again, however, this confidentiality requirement is not intended to prevent personnel from getting guidance from company executives or inside or outside counsel where necessary.

8.3 Interception or Disclosure of Communications

Finally, like criminal investigations,[121] the government can also obtain a wiretap order to intercept a target's communications in national security

115. 50 U.S.C. § 1843(a)-(b) (2000 & Supp. 2003).
116. 50 U.S.C. § 1843(c).
117. 50 U.S.C. § 1842(d)(2)(B)(i).
118. 50 U.S.C. § 1842(d)(2)(B)(iii).
119. 50 U.S.C. § 1842(f).
120. 50 U.S.C. § 1842(d)(2)(B)(ii)(II).
121. *See supra* Part 6.

investigations.[122] Generally, these FISA interceptions are treated almost identically to criminal wiretap orders.

8.3.1 Government's Ability to Intercept Communications

Except in certain limited situations set forth below, the government must obtain a court order before it can lawfully intercept a target's communications.[123] FISA wiretap orders usually last up to 90 days, although an order may last up to one year. The government may obtain an unlimited number of extensions.[124]

8.3.1.1 "Roving" FISA Orders

FISA allows the government to serve a "roving" wiretap order on multiple providers "in circumstances where the Court finds that the actions of the target . . . may have the effect of thwarting the identification" of a single provider.[125] For example, if a target frequently uses different Internet accounts with various ISPs, the government might serve an order on all of the providers, instructing them to implement surveillance on any account the government believes the target may be using at a particular moment.

As a result, an ISP could receive a Foreign Intelligence Surveillance Court order in which the ISP is not specifically named and the service that is under surveillance is not specifically identified. In order to minimize the risk of miscommunication, the provider should check the description of the target provided in the order to ascertain that the target really is one of its subscribers. ISPs with questions about such an order should discuss the matter with the government official who served them with the court order.

8.3.1.2 Attorney General's Certification to Intercept Communications without a Court Order

In certain circumstances, FISA permits the Attorney General to authorize the interception of communications for up to one year *without* a court order. However, in order to do so, the Attorney General must certify under oath that "there is no substantial likelihood that the surveillance will acquire the contents of any communications to which a United States person is a party" and must file a copy of the certification with the Foreign Intel-

122. 50 U.S.C. § 1805 (2000 & Supp. 2003).

123. 50 U.S.C. § 1805.

124. 50 U.S.C. § 1805(e). In contrast, the duration of criminal wiretap orders and extensions is limited to only 30 days. 18 U.S.C. § 2518(5).

125. 50 U.S.C. § 1805(c)(2)(B).

ligence Surveillance court.[126] Because of these requirements, such certifications are extremely uncommon.

8.3.2 Government Interception of Communications in Emergency Situations

The Attorney General may authorize the interception of communications before obtaining a FISA court order if the Attorney General: 1) determines that an emergency exists requiring the immediate installation of the surveillance before an order "can with due diligence be obtained;" and 2) subsequently applies to the Foreign Intelligence Surveillance Court for an order within 72 hours.[127] Even in this type of emergency situation, the government must stop intercepting the communications after 72 hours (at the latest) if it subsequently fails to obtain a court order.[128]

8.3.3 A Provider's Obligations to Provide Assistance

An order authorizing a FISA interception may direct a provider to furnish "all information, facilities, or technical assistance necessary to accomplish the electronic surveillance."[129] Law enforcement must compensate a provider for its expenses in providing such assistance.[130] No cause of action can be brought against a provider that furnishes any assistance or information in accordance with a FISA wiretap order.[131] As mentioned above, FISA court orders are governed by special confidentiality requirements. A FISA order will direct a provider to maintain the order and "any records concerning the surveillance or the aid furnished" in compliance with the security procedures approved by the Attorney General and the Director of Central Intelligence.[132] However, company personnel may discuss these orders, as necessary, to get guidance from company executives or inside or outside legal counsel.

9 REIMBURSEMENT FOR COSTS

Federal law makes it clear that ISPs are not expected to conduct government investigations at their own expense:

126. 50 U.S.C. § 1802.
127. 50 U.S.C. § 1805(f).
128. 50 U.S.C. § 1805(f) (2000 & Supp. 2003).
129. 50 U.S.C. § 1805(c)(2)(B).
130. 50 U.S.C. § 1805(c)(2)(D).
131. 50 U.S.C. § 1805(i).
132. 50 U.S.C. § 1805(c)(2)(C).

> (a) Payment–Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.
>
> (b) Amount–The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).[133]

The exception to this provision is so narrow that it mainly serves to establish that ISPs should always be reimbursed. Paragraph (c) simply excludes searches of "telephone toll records and telephone listings" supplied by a "communications common carrier" from reimbursement and neither of those terms applies to ISPs.

Notwithstanding this clear language, law enforcement agencies are often reluctant to provide reimbursement. This can make it hard to "mutually agree" on an appropriate fee as the statute provides.

ISPs must in any event take the lead in identifying such "costs as are reasonably necessary and . . . directly incurred in searching for, assembling, reproducing, or otherwise providing" the requested records.[134] At a minimum, those costs should include the hourly cost of any paralegals, engineers, or lawyers involved in the search. In addition to salary, it is reasonable to include benefits and social security, as well as overhead items such as office space and utilities. It is less common for ISPs to include other overhead items, from general administrative allocations to outside counsel costs associated with searches, though the statute would seem to permit their recovery if the costs are properly attributed to searches. When tools have been developed by company engineers to make searches more

133. 18 U.S.C. § 2706.
134. 18 U.S.C. § 2706(a) (2000 & Supp. 2003).

efficient, the cost of the total can be amortized and applied to all searches conducted with the tool until the cost has been recovered.

Some ISPs use an estimate of costs to create a per-search charge; others charge based on the number of hours required. The latter method seems to produce fewer objections from law enforcement.

A particular difficulty arises in the context of preservation requests under § 2703(f). There is no provision for receiving payment from the government when a preservation request is made, even though the preservation itself requires substantial searching and assembling. Of course, these costs can be assessed when the subpoena or other order arrives and the information is released. But close to half of all preservation requests are simply abandoned. No subpoena is ever issued. The costs incurred as a result of these requests cannot be recovered in the subpoena process, except as part of a general office overhead charge.

10 LIABILITY FOR ECPA VIOLATIONS

10.1 Criminal Liability

Violations of ECPA's prohibition of the interception and disclosure of electronic communications[135] can give rise to criminal liability, including fines and/or imprisonment for up to five years.[136] Knowing violations of ECPA's provisions concerning pen registers and trap and trace devices[137] also can give rise to criminal liability, including fines and/or imprisonment for up to one year.[138]

In addition, ECPA imposes criminal liability for intentionally accessing, without authorization, a stored electronic communication.[139] This provision does not apply, however, to conduct authorized by providers of electronic communication service, and therefore would not apply to ISPs, except in cases of malicious acts by their employees.[140]

10.2 Civil Liability

Under ECPA, a person whose electronic communications are intercepted or disclosed may sue a provider for illegally intercepting or disclosing the communications.[141] The person must allege, however, that the pro-

135. *See supra* Part 6.
136. 18 U.S.C. § 2511(4)(a).
137. *See supra* Part 4.
138. 18 U.S.C. § 3121(d).
139. 18 U.S.C. § 2701(a); *see supra* Part 5.
140. 18 U.S.C. § 2701(c) (2000 & Supp. 2003).
141. *See supra* Part 6.

vider or one of its employees: a) acted without a facially valid court order or other lawful authorization; b) acted beyond the scope of a court order or lawful authorization; or c) acted in bad faith.[142] A provider, subscriber, or customer may also sue a party for illegally obtaining or divulging his stored communications or records.[143] Possible relief for violations of either provision includes damages (including, potentially, punitive damages) and reasonable attorneys' fees and litigation costs.[144] ECPA's provisions concerning pen registers and trap and trace devices[145] do not state a cause of action for violations.

10.3 Service Provider Immunity

A lawsuit cannot be brought, under ECPA or otherwise, against a provider for assisting law enforcement in carrying out a court order, warrant, subpoena, or other lawful authorization.[146] In addition, a provider's good faith reliance on court orders or other legal authorizations is a complete defense against any civil or criminal actions brought under ECPA.[147]

11 INTERNATIONAL JURISDICTIONAL ISSUES

The global nature of the Internet and many ISPs' networks frequently raises international jurisdictional issues with respect to ECPA. For example, a multinational ISP might be presented with a non-U.S. judicial order for the interception and/or disclosure of electronic communications stored or transmitted within the United States. The ISP would be at risk of violating ECPA, however, if it complied with the non-U.S. order by intercepting or disclosing electronic communications stored or transmitted within the United States, absent an applicable exception to ECPA.[148] Therefore, in order to access such communications, in most cases, the foreign government would have to obtain the appropriate (ECPA-compliant) U.S. legal

142. 18 U.S.C. § 2520(a).

143. 18 U.S.C. § 2707(a); *see supra* Part 5. In one notable ECPA lawsuit, a Virginia ISP paid an undisclosed amount in 1998 to settle a claim by a homosexual Navy sailor that it had improperly disclosed information about him to a Navy investigator. *See* Bradley Graham, *Gay Sailor Takes Navy Retirement Settlement; AOL Also Will Pay For Privacy Violation*, WASH. POST, June 13, 1998, at A3; *see also* McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998).

144. 18 U.S.C. §§ 2520(b)-(c), 2707(b)-(c).

145. *See supra* Part 4.

146. 18 U.S.C. §§ 2511(2)(a)(ii), 2703(e), 3124(d) (2000 & Supp. 2003).

147. 18 U.S.C. §§ 2520(d), 2707(e), 3124(e).

148. *See supra* Part 5.3.

order through the United States government.[149] Foreign governments have been known to object to such time-consuming processes, and claim that an ISP subject to its jurisdiction must comply with its order without obtaining process through the United States government. ISP staff should coordinate closely with legal counsel in such situations.

The USA PATRIOT Act made two changes to ECPA that are particularly notable in the international context. First, it altered the statutory provisions for search warrants, "section 2703(d)" orders, and pen register and trap and trace orders such that jurisdiction for issuing these orders vests in a court having jurisdiction over the underlying offense. When dealing with international requests for assistance, this change raises a question as to whether or not federal courts have jurisdiction to grant relief. Because the offenses being investigated were committed abroad in circumstances under which a federal district court would not have jurisdiction over the offense, there is an argument that federal courts do not have jurisdiction. A counterargument likely to be advanced by the government is that the court acquires jurisdiction over the offense by virtue of the international request for assistance. As a practical matter, an ISP will only be required to act when presented with an order. Having issued the order, the court will have resolved the issue.

Second, the Act amends the definition of "protected computer" to make clear that this term includes computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States."[150] The United States can now use purely domestic procedures, as opposed to international legal assistance, to join in international hacker investigations when hacking a foreign computer constitutes an offense under U.S. law.

Finally, enactment of the USA PATRIOT Act and the Homeland Security Act of 2002,[151] has made international waters a bit more dangerous for ISPs. Section 225 of the Homeland Security Act amends the emergency disclosure provision. Before the amendment, ISPs could make emergency disclosures of the contents of a communication to "a law en-

149. There is a formal process for "domesticating" such foreign orders. The process is often referred to as the MLAT-process—named for the Mutual Legal Assistance Treaties that provide for this form of assistance by the U.S. government—and is operated by the Department of Justice Office of International Affairs. *See* Mutual Legal Assistance and Other Agreements ("MLAT"), *at* http://travel.state.gov/mlat.html (last visited Oct. 17, 2003).

150. 18 U.S.C. § 1030(e)(2)(B).

151. Pub. L. No. 107-296, § 1, 116 Stat. 2135 (2002) (codified as 6 U.S.C. § 101 (Supp. 2003)).

forcement agency." After the amendment, such disclosures may be made "to a Federal, State, or local governmental entity." While this may not sound like much of a change, it may exclude emergency disclosures to a foreign law enforcement agency unless that agency can be characterized as a "local government entity." Of course, whether U.S. law governs such disclosures and whether the subscribers may have consented to such disclosures in an ISP's acceptable use policies, are separate questions.

12 INTERRELATION WITH STATE LAW

Federal law has "preempted" the states in the field of electronic surveillance and interception of wire and electronic communications. 18 U.S.C. § 2516(2), which authorizes state electronic surveillance laws, lists the offenses for which state statutes may authorize interceptions, and requires that the procedures set out in 18 U.S.C. § 2518 be followed in issuing interception orders. At the same time, since the original wiretap law in 1968, it has been clear that a state may have stricter (but not more lenient) requirements. ECPA has similar provisions regarding state authority[152] and the same logic applies to these other forms of obtaining evidence—that is, state requirements may be stricter than the federal statute, but not more permissive. Pursuant to these authorities, most states have adopted their own wiretap and pen register and trap and trace statutes, as well as "mini-ECPAs."[153]

After the passage of the USA PATRIOT Act, several states have sought to amend their laws to track the federal amendments. However, proposed state amendments in some states have differed in critical ways from federal law. ISPs should carefully track amendments to state laws, both before and after passage.

Another emerging problem area is the extent to which ECPA, particularly 18 U.S.C. § 2702, may prohibit access to the content of e-mail based on state discovery subpoenas. In addition, several states are considering various privacy laws and criminal statutes relating to illegal Internet content, all of which could have serious consequences for ISPs.

The law in this area is in a state of flux, with many federalism and other constitutional issues yet to be resolved by the courts. ISPs and their

---

152. *See, e.g.*, 18 U.S.C. § 2703; 18 U.S.C. § 3122 (2000 & Supp. 2003).

153. *See, e.g.*, 720 ILL. COMP. STAT. 5/14-1 (2003) (defining "eavesdropping" to include interception of electronic communications); N.Y. PENAL LAW § 250.05 (McKinney 2000) (defining the offense of eavesdropping as including the "intercepting or accessing of an electronic communication"); VA. CODE ANN. §§ 19.2-61 to 2-70.3 (Michie Cum. Supp. 2003) (Chapter 6—Interception of Wire, Electronic or Oral Communications).

legal counsel should bear in mind that both state and federal law can be the basis for electronic surveillance requests and the legal requirements, provisions for reimbursement, and immunity from liability under state law must be checked carefully with their federal counterparts.

13 CONTACT INFORMATION

If you would like to get in touch with some of the contributors to this Guide, see the contact information below:

Drew C. Arena
Assistant General Counsel for Legal Compliance
Verizon Communications
1515 North Courthouse Road, Suite 500
Arlington, Virginia 22201-2909
Telephone: 703.351.3007
Fax: 703.351.3667
E-mail: drew.c.arena@verizon.com

Stewart A. Baker
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Telephone: 202.429.6413
Fax: 202.261.9825
E-mail: sbaker@steptoe.com

Elizabeth Banker
Associate General Counsel
Yahoo! Inc.
701 First Avenue
Sunnyvale, California 94089
Compliance Fax: 408.349.7941

Christopher G. Bubb
Assistant General Counsel
American Online, Inc.
22000 AOL Way
Dulles, Virginia 20166
Fax: 703.265.2305

Kate Dean
Manager
US Internet Service Provider Association
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Telephone: 202.862.3816
Fax: 202.261.0604
E-mail: kdean@steptoe.com

Susan Kelley Koeppen
Senior Attorney
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
Telephone: 425.705.4788
Fax: 425.936.7329
E-mail: susankoe@microsoft.com

14 GLOSSARY

Electronic Communication: For purposes of ECPA, "electronic communication" is defined broadly to encompass a wide range of technologies. Specifically, ECPA defines an "electronic communication" 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 that affects interstate or foreign commerce[.]"[154]

Electronic Communication Service: As defined by ECPA, "any service which provides to users thereof the ability to send or receive wire or electronic communications," including electronic mail services.[155]

Electronic Storage: As defined by ECPA, "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."[156]

Interception: An "intercept" of an electronic communication (such as an e-mail message) occurs when someone other than the intended recipient gains access to the communication during the transmission phase (as opposed to when it is stored). Technically, ECPA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[157]

Pen Register: A device or process that attaches to a telephone line or facility and records outgoing dialing, routing, addressing, or signaling information. It does not record the content of communications.[158]

Remote Computing Service: As defined by ECPA, the provision to the public of computer storage and processing services.[159]

Trap and Trace Device: A device or process which attaches to a telephone line or facility and records "the incoming electronic or other impulses [for example, telephone numbers] which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source

154. 18 U.S.C. § 2510(12).
155. 18 U.S.C. § 2510(15).
156. 18 U.S.C. § 2510(17).
157. 18 U.S.C. § 2510(4).
158. 18 U.S.C. § 3127(3) (2000 & Supp. 2003).
159. 18 U.S.C. § 2711(2).

of a wire or electronic communication . . . ." It does not record the content of communications.[160]

160. 18 U.S.C. § 3127(4).