UIC John Marshall Journal of Information Technology & Privacy Law

Volume 20
Issue 1 *Journal of Computer & Information Law - Fall 2001*

Article 1

Fall 2001

# The Electronic Communications Privacy Act: Does the Answer to the Internet Information Privacy Problem Lie in a Fifteen Year Old Federal Statute? A Detailed Analysis, 20 J. Marshall J. Computer & Info. L. 1 (2001)

Henry M. Cooper

# ARTICLES

# THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: DOES THE ANSWER TO THE INTERNET INFORMATION PRIVACY PROBLEM LIE IN A FIFTEEN-YEAR-OLD FEDERAL STATUTE? A DETAILED ANALYSIS

HENRY M. COOPER†

## I. INTRODUCTION

Does this situation sound familiar? You connect to the Internet to check your e-mail messages. You discover you have twenty new messages. However, you soon find out that eighteen of them are unsolicited commercial e-mail messages, commonly referred to as "spam."[1] You ask yourself, "How did they get my e-mail address?" Well, the simple answer is that individuals give out their personal information on a daily basis without the awareness and knowledge as to how that information is being used and disseminated.[2] For example, when you fill out a registration form on a Web site in order to shop for a product, the form also includes survey information asking you for very personal and private information.[3] "Fifty-four percent of Internet users have chosen to provide

† LL.M. in Information Technology Law, The John Marshall Law School; Microsoft Certified Professional. Mr. Cooper specializes in Technology and Intellectual Property law and can be contacted at hcooper@focolaw.com or at (561) 393-9111.

1. *See generally* Fight Spam on the Internet! *What Is Spam?* <http://spam.abuse.net/overview/whatisspam.shtml> (accessed Sept. 19, 2001).

2. *See House Member Preps Privacy Bill* ¶ 13 <http://www.wired.com/news/politics/0,1283,19004,00.html> (Apr. 7, 1999) (noting that in 1998, the Federal Trade Commission ("FTC") released the results of a survey of 1,400 Web sites; ninety-two percent of them collected data, but only fourteen percent disclosed how the information would be used).

3. *See e.g.* Barnes&Noble.com <www.bn.com> (accessed Sept. 19, 2001) (directing Internet consumers to a page requesting information "[f]or future reference"); Nine West <www.ninewest.com> (accessed Sept. 19, 2001) (directing Internet consumers to a page requesting personal information prior to "checkout").

personal information in order to use a [W]eb site."[4] However, by filling out this information and other similar forms, an individual's personal information is scattered around the world and stored in various public and private databases.[5]

In 1986, the *Electronic Communications Privacy Act* ("ECPA") was enacted to update and clarify federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.[6] These new technologies included electronic mail ("e-mail"), data transmission through computer networks, cellular and cordless telephones, and paging devices.[7] The purpose of ECPA was to protect against the unauthorized interception and storage of electronic communications.[8] Now, fifteen years later, the ECPA deals with one of man's greatest technological development – the Internet.

The Internet is a global network of interconnected computers.[9] The Internet provides a means through which an individual can quickly and inexpensively disseminate information to a global audience.[10] "People from all over the world can communicate and share information with little more than a few keystrokes."[11] Thus, due to the ability to transmit and share information with a global audience,[12] concerns have arisen over what privacy protections an individual has regarding personal information transmitted via the Internet.[13] Currently, industry self-regulation is the favored model to address the Internet information privacy problem.[14] However, lobbyists and privacy advocates have urged Congress to pass new federal legislation to effectively regulate this growing dilemma.[15]

This article examines whether new federal legislation is necessary in light of ECPA. In Part II, the author defines information privacy and explains how it is used and misused on the Internet. Part III of this article analyzes ECPA Title II in detail, including judicial interpretation of its major provisions. In Part IV, the author presents the argument

4. *See* The Pew Internet & American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* ¶ 2 <http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf> (accessed Feb. 4, 2000).

5. *See id.* at ¶ 5.

6. *See* Sen. Rpt. 99-541 at 20-23 (Oct. 1, 1986).

7. *Id.* at 10.

8. Sen. Rpt. 99-541 at 2.

9. Anne Meredith Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?*, 3 Comm. Law Conspectus 63, n. 5 (Winter 1995).

10. *Id.* at 63.

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.* at 69.

15. *See e.g. id.* at 70.

that ECPA Title II, in its current form, is inadequate to combat the misuse of an individual's personal information on the Internet. The author then proposes an amendment to ECPA to rectify the deficiencies in Title II so that ECPA may effectively prevent the misuse of an individual's personal information obtained via the Internet.

## II. INFORMATION PRIVACY RIGHT

### A. BACKGROUND

An individual's right to information privacy has been defined as the right of an individual to control how his personal information is "acquired, disclosed, and used."[16] The key to the information privacy right is the definition of "personal information."[17] The Clinton Administration's Information Infrastructure Task Force ("IITF") released a document entitled "Principles for Providing and Using Personal Information," which provides a widely accepted definition for personal information.[18]

The IITF document defines personal information as "information identifiable to the individual."[19] This has not been interpreted to mean private, sensitive information.[20] Instead, it has been interpreted to "describe a relationship between the information and a person [such that it is identifiable to that individual because it] . . . bears (1) an authorship relation to the individual, (2) a descriptive relation to the individual, or (3) an instrumental mapping relation to the individual."[21] An example of an instrumental mapping would be a person's social security number.[22] This number has no relation to the individual except that it is a numeric identifier linked to him.[23]

Since the information privacy right only protects against the unlawful acquisition, disclosure and use of an individual's personal information, an individual's non-personal information is left unprotected.[24] Simply put, non-personal information is information that cannot be associated with a specific individual.[25] Non-personal information exists in three ways: non-human information, anonymous information and group information.[26] Non-human information is defined as information that is

16. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1205 (Apr. 1998).
17. *Id.*
18. *Id.*
19. *Id.* at 1206.
20. *Id.* at 1207.
21. *See id.*
22. *Id.* at 1208.
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.* at 1208-09.

not associated or identified with a human being.[27] An example of non-human information is the law of gravity. Certain types of anonymity can also be classified as non-personal information.[28] However, it is important to note that although cloaked in anonymity, if an individual's identity can still be discovered through research or publicity, it is considered personal information.[29] This type of anonymity is called traceable anonymity.[30] Traceable anonymity is considered personal information because "privacy involves the control of the flow of personal information in all stages of processing, acquisition, disclosure, and use."[31] If the identity of the individual was known at the acquisition stage but later became anonymous at the disclosure and use stage, it is still considered to be personal information.[32]

Group information is considered non-personal information when the information is identifiable to a group of people instead of a specific individual.[33] However, classifying group information as non-personal raises concerns when the group is small and an individual's identity can be inferred from the group information.[34] For example, group information such as "Microsoft released Windows 98 today" is sufficiently broad to make it impossible to discern an individual identity and should be considered non-personal.[35] However, group information concerning a cult could identify its leader and some individual members.[36] This raises a contextual issue regarding privacy protection for group information.[37] The proper analysis should fall on the context of the information, the size of the group, and whether an individual's identity can be discerned or inferred from the information.[38] If so, that particular group information should be considered personal information and afforded the appropriate privacy protection.[39]

Courts have used three factors in balancing an individual's information privacy interests versus the government's interest in disclosure.[40] First, a court must look at "[t]he extent to which the information sought

27. *See id.* at 1209.
28. *Id.*
29. *Id.*
30. *Id.*
31. *See id.*
32. *Id.* at 1210.
33. *Id.*
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.*
38. *Id.*
39. *Id.*
40. George P. Long, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U. Pitt. Rev. 1177, 1192 (Summer 1994).

to be disclosed will lead to embarrassment or reputational injury."[41] Second, a court must look at "whether disclosure will lead to harassment and intrusion."[42] Third, a court must look at the "reasonableness of the individual expectations of privacy."[43] Arguably, these factors can be easily met when weighing an improper disclosure and use of an individual's personal information in the context of e-commerce.[44] An online consumer has a reasonable expectation that his personal information will be used only for the primary purpose in which he consents to relinquish this information to the e-commerce entity. In most cases, there is no legitimate government interest in disclosure. Further, misuse and unauthorized disclosure of an individual's personal information can lead to embarrassment, intrusion, or reputational injury.

### B. The Internet's Gradual Erosion of the Right to Information Privacy

The Internet has unleashed a new era of privacy invasion.[45] It is the "most effective data-collector in existence."[46] In a recent poll, seventy-eight percent of the American public stated that they would use the Internet more if they were given assurances that their personal and information privacy was safeguarded against unauthorized intrusion.[47] E-commerce entities have taken full advantage of the plethora of personal information that exists online. An e-commerce entity, for purposes of this article, is defined as an Internet service provider, a commercial online service provider, a bulletin board service, and an individual or a company that publishes a Web site on the World Wide Web for the purpose of generating revenue.[48] "Information has taken on a new character . . . [i]t has passed from being an instrument through which we acquire and manage other assets to being a primary asset itself."[49]

#### 1. *Online Information Gathering Methods*

An e-commerce entity via the World Wide Web can collect information about an individual by using various Internet technologies such as "clickstream" data, server log information, and through the opt-in disclosure of

41. *See id.*
42. *See id.*
43. *See id.*
44. *See* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 San Diego L. Rev. 1153, 1172 (Summer 1997).
45. *See generally id.*
46. *Id.* at 1164.
47. Nancy Lazar, *Consumers Online: Your Right to Privacy in Cyberspace*, 10 Loy. Consumer L. Rev. 117 (1998).
48. *Id.*
49. *See* Gindin, *supra* n. 44, at 1162.

personal information in registration forms, online surveys, sweepstakes, and e-mail.[50]

"Clickstream" data is anonymous data that tracks a user's computer as it navigates through a particular Web site.[51] Clickstream data monitors the time, order and duration the computer spent on each Web page as well as which files were accessed and/or downloaded.[52] For example, if a user's computer accesses Widget.com's Web site, Widget.com will monitor Web pages the user's computer viewed; how much time the user's computer spent on each Webpage; the products viewed and ordered, if any; and other interests the user's computer expressed while navigating the Widget.com Web site.[53] This navigational information is supposedly used to make improvements to the e-commerce Web site.[54] Clickstream data is either directly retrieved from the e-commerce entity's server logs or indirectly collected by the use of a "cookie."[55]

The e-commerce entity's Web site administrator may directly access clickstream data through its server logs.[56] These logs contain information including "length of time logged on, particular pages visited or downloaded, type of browser used and the user's computer IP address."[57]

A cookie is a file stored on a user's computer[58] that stores data sent by an e-commerce entity.[59] This data may contain a serial number that correlates with database information held by the e-commerce entity.[60] The cookie may contain data that allows tracking of the user's activities on the particular e-commerce entity's Web site.[61] It might also contain data that indicates what pages or advertisements a user has seen on the e-commerce entity's Web site during previous visits.[62] In addition, the cookie may also contain information such as a user's account number, password, credit card information or other stored information that can then be called up by the e-commerce entity when the information is needed again. A cookie that is correlated with logs from an e-commerce entity's Web server can relate a specific user with the pages the user has

50. Leslie A. Kurtz, *The Invisible Becomes Manifest: Information Privacy in a Digital Age*, 38 Washburn L.J. 151, 159 (Fall 1998).

51. Kang, *supra* n. 16, at 1129.

52. *Id.* at 1227.

53. *Id.* at 1228.

54. *Id.*

55. Joshua B. Sessler, *Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet*, 5 J.L. & Policy 627, 631-36 (1997).

56. *See id.* at 635.

57. *See id.*

58. *Id.* at 632.

59. *Id.*

60. *See id.* at 632-33.

61. *Id.* at 633.

62. *See id.* at 632-33.

viewed, the operating system and Web browser the user has installed on the user's computer, and other similar information.[63] The cookie may store clickstream data which can be read by the e-commerce entity.[64] The entity may use this information to provide the user with a more personalized experience when revisiting the entity's Web site.[65] The cookie may also store other anonymous information including the user's "Internet service provider and the kind of computer and software used."[66]

An e-commerce entity may gather an individual's personal information through the Internet user's opt-in disclosure of such information in registration forms, online surveys, sweepstakes, and e-mail.[67] Many e-commerce entities require an individual to fill out a registration form to place an order with them or to use their Web site.[68] An individual, by consenting or opting-in to disclose personal information in exchange for benefits, assistance, or the unrestricted use of the Web site, enables the e-commerce entity to gather the individual's credit card information, directory information, social security number, family information, economic status, and other personal information.[69]

The anonymous clickstream data when combined with the personal information obtained through registration forms, online surveys, sweepstakes, or e-mail can be used to create a complete electronic record of the user.[70] An electronic record, for purposes of this article, is defined as an electronically stored, organized collection of related items of data compiled from separate pieces of information retrieved from server logs, cookies, registration forms, online surveys, sweepstakes, e-mail and other means that provides a complete profile of an individual. These electronic records enable the e-commerce entity to have a single source containing an individual's name, address, telephone number, e-mail address, social security number, credit card information, employment, salary, browsing and shopping preferences, and many other interests.[71]

### 2. *How This Information Violates the Right to Information Privacy*

Although these information-gathering methods may seem to have law-

63. *See* Netlingo.com § Cookies <www.netlingo.com/lookup.cfm?term=cookies> (accessed Jan. 4, 2002).

64. Gindin, *supra* n. 44, at 1170.

65. Kang, *supra* n. 16, at 1129.

66. *See* Gindin, *supra* n. 44, at 1170.

67. *See e.g.* Barnes&Noble.com <www.bn.com> (accessed Sept. 19, 2001).

68. *See e.g. id.*

69. *Id.*

70. *Id.*

71. *Id.*

ful purposes, they are also very profitable.[72] "Illinois raises $10 million annually from the sale of public records, . . . [and] companies, including credit reporting agencies and direct selling marketers, pay the United State Postal Service $80,000 each year in return for the information from change of address cards."[73] It is these secondary uses of personal information that have many privacy advocates concerned over the gradual erosion of the individual's right to information privacy.[74]

Secondary uses of personal information most often occur without the knowledge or consent of the individual.[75] In 1998, "the FTC released a survey of 1,400 Web sites showing that [ninety-two] percent collected data but only [fourteen] percent disclosed how the information could be used."[76] Due to the enormous growth in demand for personal information, the commercial marketplace has created a new type of business-data-mining.[77]

Data-mining is the process of collecting numerous types of personal information from a variety of sources and then compiling the separate pieces of information into one, organized, indexed, and complete electronic record for subsequent sale to online services, companies, individuals, government entities, or any interested party.[78] "As cyberspace becomes the preferred medium to complete the day's innumerable tasks, it will generate for each individual a mother lode of personal information, recorded dutifully—and often invisibly—by computers that know no sleep."[79] This data-mined collection of information may include directory-type information, social communications, organization and political memberships, medical history, education records and other highly detailed personal information that provide the data miner with a complete electronic record of an individual's personality, interests, intelligence, shortcomings, fears, allegiances and health.[80]

Data-mining has been praised by advertisers and marketing firms.[81] It allows a marketing firm to target its product advertisements and promotional offers to a specific individual whose profile is a direct match for

72. *See e.g.* Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate,* 49 S.C. L. Rev. 847, 855-56 (Summer 1998).

73. *See id.* at 855-56.

74. *See id.*

75. *See generally House Member Preps Privacy Bill, supra* n. 2.

76. *See id.* at ¶ 13.

77. Kang, *supra* n. 16, at 1238.

78. *Id.*

79. *See id.*

80. *Id.*

81. *See e.g.* The Data Mining Group <http://www.dmg.org/aboutdmg/aboutdmg.htm> (accessed Oct. 7, 2001).

their ideal consumer.[82] Although this sounds innocent and non-invasive to some people, imagine being in one of the following situations. First, you feel a little overweight so you decide to purchase weight-loss products via the World Wide Web and are shocked to suddenly receive e-mail and regular mail soliciting you with discount offers on candy and junk food. Second, you are trying to quit smoking so you purchase a nicotine patch online. Soon thereafter, you are inundated with free samples from cigarette companies.

## III. ECPA TITLE II: 18 U.S.C. §§ 2701-2712

ECPA Title II is concerned with the storage stage of a communication.[83] Title II prohibits the unlawful access and disclosure of "electronically stored" communications.[84] For purposes of Title II analysis, "electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[85] An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[86] However, courts have interpreted this definition to include only those entities that provide such service to the public and not for their internal use only.[87] A "remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[88]

### A. SECTION 2701

Section 2701 of ECPA Title II prohibits the unlawful access to electronically stored communications.[89] The term "access" is not defined by ECPA. However, under Title II, courts have interpreted access to involve the situation in which an individual or entity places itself in a "po-

82. *See e.g. id.*

83. *See* 18 U.S.C. §§ 2701-2712 (2001) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)). ECPA Title I is concerned with the unlawful interception of an electronic communication during its transmission stage. *Id.* §§ 2510-2522 (2001).

84. *See generally id.* §§ 2710-2712 (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

85. *See id.* § 2510(17).

86. *See id.* § 2510(15).

87. *See Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998) (holding that where a private corporation provided e-mail service for its employees, the e-mail service was not an electronic communication service because the corporation did not provide the e-mail service to the public).

88. *See* 18 U.S.C. § 2711(2).

89. *Id.* § 2701.

sition to acquire [the] contents of a[n electronic] communication."[90] Subsection (a) divides the elements of an unlawful access into two main categories: unauthorized access and an affirmative act pertaining to the electronically stored communication.[91] First, the person[92] must either, without authorization or exceeding his or its level of authorization, intentionally access the electronically stored communication files of an electronic- communication service provider.[93] Second, once the person gains access to the electronic-communication service provider's electronically stored communication files, the person must obtain, modify or block authorized access to a "wire or electronic communication while it is in electronic storage in such system."[94] Thus, a hacker who gains unauthorized access to a company's file system may be liable under this section if he alters an e-mail file, downloads an e-mail file or crashes the company's server thus preventing authorized users to access their files.[95]

Subsection (b) provides the penalty for violating Section 2701.[96] A person who unlawfully accesses an electronically stored communication for the purpose of "commercial advantage, malicious destruction or damage, or private commercial gain" may be fined and/or imprisoned for up to one year for a first offense and up to two years for any subsequent offenses.[97] For any other unlawful access, the person may be fined and/or imprisoned for up to six months.[98] Thus, a hacker who unlawfully accesses the company's server could be fined and/or imprisoned for up to two years for his violation of Section 2701.[99]

Subsection (c) provides exceptions that make subsection (a) inapplicable in certain situations.[100] A person is exempt from liability for an unauthorized access to an electronically stored communication under four circumstances.[101] First, no liability attaches to a person who was given permission by the electronic-communication service provider to access the communication files.[102] Second, a person is not liable for unlaw-

90. *See U.S. v. Smith*, 155 F.3d 1051, 1058 (9th Cir. 1998).

91. 18 U.S.C. § 2701(a).

92. *Id.* § 2510(6) (defining a person as an individual, a corporation or other business entity, employees, and/or a government agent or entity).

93. *Id.* § 2701(a)(1).

94. *See id.* § 2701(a)(2).

95. *See generally Cyber-attacks Batter Web Heavyweights* <http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/> (Feb. 9, 2000). Recently, this unlawful conduct has become more prevalent as evidenced by several denial-of-service attacks upon e-commerce entities such as Yahoo.com. *Id.* at ¶¶ 2-3.

96. 18 U.S.C. § 2701(b).

97. *Id.*

98. *Id.*

99. *Id.* § 2701(b)(1)(B).

100. *Id.* § 2701(c).

101. *Id.*

102. *Id.* § 2701(c)(1).

ful access if "a user of that service with respect to a communication of or intended for that user" permitted such access.[103] Third, no liability attaches if access was authorized by a valid subpoena or court order.[104] Fourth, access to an electronically stored communication for the sole, intended purpose of backup preservation of that communication is a lawful access.[105] Thus, if a company hires a hacker to access its system to ascertain unsecured areas of its network, the hacker would be exempt from liability in the event the hacker gains unauthorized access to an electronically stored communication.[106]

### B. SECTION 2702

Section 2702 of ECPA Title II prohibits the unauthorized disclosure of the contents of an electronically stored communication.[107] "Contents" is defined as "any information concerning the substance, purport, or meaning of that communication."[108] Subsection (a) prohibits an electronic-communication service provider or a remote computing service from knowingly disclosing the contents of an electronically transmitted communication that is maintained in electronic storage on that service provider's computer system to any person or entity.[109] For example, under this subsection, an electronic-communication service provider or remote computing service would generally be prevented from disclosing the contents of a subscriber's e-mail messages to the public.

Subsection (b), however, provides for exceptions to the general prohibition on disclosing the contents of electronically stored communications.[110] First, it is lawful for an electronic-communication service provider or remote computing service to disclose the contents of an electronically stored communication to the intended recipient/addressee of that communication.[111] Without this exception, an Internet Service Provider or commercial online service provider would not be able to route a sender's e-mail to its intended destination.[112] Second, this subsection

103. *See id.* § 2701(c)(2); *see also In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001). The court dismissed plaintiffs' 18 U.S.C. § 2701 claim against DoubleClick holding that DoubleClick fell under the § 2701(c)(2) exception. *Id.* The court found DoubleClick-affilated Web sites were "users" of Internet access under ECPA and had given DoubleClick adequate authorization to access plaintiffs' information by placing cookies on plaintiffs' hard drives. *Id.*

104. 18 U.S.C. § 2701(c)(3).

105. *Id.*

106. *Id.* § 2701(b).

107. *Id.* § 2702 (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

108. *See id.* § 2510(8).

109. *Id.* § 2702(a) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

110. *Id.*

111. *Id.* § 2702(b) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

112. *See id.* §§ 2702, 2703.

allows disclosures to law enforcement officers under Section 2517 to an electronic-communication service provider or remote computing service employees for use in the normal course of employment, and to the government under very specific circumstances.[113] Third, disclosure is permitted if a party to the communication consents to disclosure.[114] Fourth, disclosure is permitted to an authorized re-mailer or other authorized electronic communication forwarding service.[115] Fifth, disclosure is lawful if the communication service provider or remote computing service must do so to properly render its services or to protect its property or rights.[116] Sixth, disclosure may be made to a law enforcement agency if the contents of an electronically stored communication "were inadvertently obtained by the service provider and appear to pertain to the commission of a crime, if required by Section 227 of the *Crime Control Act of 1990*, or if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."[117]

Further, Section 2702(a)(3) of ECPA Title II prohibits the unauthorized disclosure of a record or other information pertaining to a subscriber or customer.[118] Subsection (a)(3) prohibits an electronic-communication service provider or a remote computing service from knowingly disclosing a record or other information pertaining to a subscriber or customer of such service to any governmental entity.[119]

Subsection (c), however, provides for exceptions to the general prohibition on disclosing a record or other information pertaining to a subscriber or customer to any governmental entity.[120] First, it is lawful for an electronic-communication service provider or remote computing service to disclose a record or other information pertaining to a subscriber or customer to a governmental entity in accordance with the terms of a valid warrant, administrative subpoena or court order.[121] Second, it is lawful to disclose a record or other information pertaining to a subscriber or customer to any governmental entity if they have the consent of the customer or subscriber.[122] Third, disclosure is lawful if the communication service provider or remote computing service must do so to properly

113. *Id.*

114. *Id.* § 2702(b) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

115. *Id.*

116. *Id.*

117. *See id.*

118. *Id.* § 2702(a)(3) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

119. *Id.*

120. *Id.* § 2702(c) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

121. *Id.* § 2702(c)(1) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

122. *Id.* § 2702(c)(2) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

render its services or to protect its property or rights.[123] Fourth, disclosure may be made to a governmental entity if the service provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."[124] Fifth, it is lawful for an electronic- communication service provider or remote computing service to disclose a record or other information pertaining to a subscriber or customer to any private individual or entity.[125]

It is important to note that although an e-commerce entity is a party to the electronic communications in which personal information is collected from a user (and, according to some analyses, a communication in which a cookie is set),[126] and thus may disclose the contents under Section 2702(b)(3), the privacy concern is not over one particular piece of personal information communicated from a user to an e-commerce entity. The real concern is the aggregated user records that are compiled from these communications by the e-commerce entity into customer records that amount to dossiers on a particular consumer. These aggregated records are the customer's records properly covered by Section 2702(a)(3) of ECPA.

### C. SECTION 2703

Subsections 2703(a) and 2703(b) of ECPA Title II set forth the requirements for a governmental entity to gain lawful access to the contents of electronically stored wire or electronic communications.[127] The requirements set forth in these subsections are time-dependent.[128] If an electronic-communication service provider has electronically stored the contents of a wire or electronic communication for not more than 180 days, a governmental entity must have a warrant to require the service provider to disclose the contents of that communication.[129] If the electronic-communication service provider has stored the contents for 180 days or more, a governmental entity may require disclosure of the contents of a wire or electronic communication without prior notice to the customer if the governmental entity has a warrant.[130] Prior notice to the customer must be given by the governmental entity if the entity re-

123. *Id.* § 2702(c)(3) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

124. *See id.* § 2702(c)(4) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

125. *Id.* § 2702(c)(5) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

126. *But see In re DoubleClick Inc. Privacy Litigation,* 154 F. Supp. 2d at 526.

127. 18 U.S.C. § 2703(a)-(b) (amended by *U.S.A. . PATRIOT Act,* H.R. 3162, 107th Cong. (2001)).

128. *Id.*

129. *Id.* § 2703(a) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

130. *Id.*

quires disclosure based upon an administrative subpoena or a court order.[131] But, under Section 2705, the government may petition a court to grant a delay of notice for up to ninety days, with the possibility of additional extensions on that delay in ninety-day increments.[132] A court may grant such a petition if there is evidence to support the belief that notification might have an adverse result.[133] Possible adverse results include "endangering the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or otherwise seriously jeopardizing an investigation or unduly delaying a trial."[134] The requirements for lawful government access have been discussed in some detail by our court system.[135]

Subsection 2703(c) of ECPA Title II sets forth the requirements for a governmental entity to gain lawful access to a record or other information pertaining to a subscriber to or customer of an electronic-communication service provider or remote computing service.[136] First, it is lawful for a governmental entity to receive a record or other information pertaining to a subscriber or customer in accordance with the terms of a valid warrant, administrative subpoena or court order.[137] Second, a governmental entity may receive a record or other information pertaining to a subscriber or customer if they have the consent of the customer or subscriber.[138] Third, a subscriber's record or other information may be disclosed to a governmental entity who submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud.[139] The service provider must disclose the subscriber's name; address, local and long distance telephone records; records of session times and durations, length of service, the types of service utilized; and telephone or instrument number or other subscriber number or identity information, including any temporarily assigned network address and the

131. *Id.* § 2703(b) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

132. *Id.* §§ 2705(1), (4) (2001).

133. *Id.*

134. *See id.* § 2705(2) (2001).

135. *See generally Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 816 F. Supp. 432 (W.D. Tex. 1993) (holding that the Secret Service violated the Section 2703 "mere disclosure" requirement by unlawfully seizing the entire computer which also contained other, private electronically stored communications that were not the subject of the warrant); *see Lopez v. First Union Natl. Bank of Fla.*, 129 F.3d 1186 (11th Cir. 1997) (holding that First Union violated § 2703(a) for disclosing information to a governmental entity based on verbal instructions, instead of a warrant or other written instructions).

136. 18 U.S.C. § 2703(c) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

137. *Id.* § 2703(c)(1) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

138. *Id.*

139. *Id.*

means and source of payment for such service, including any credit card or bank account number.[140] Under subsection 2703(c)(3), the governmental entity is not required to give notice to a customer or subscriber that it has received the subscriber's record or other information.[141] Further, subsection (e) provides the electronic-communication service provider with immunity against any lawsuit filed against it based upon the provider's assistance or disclosure of the contents of a communication or a subscriber's record in accordance with the terms of a valid warrant, administrative subpoena or court order.[142]

### D. SECTION 2707

Section 2707 of ECPA Title II provides that an aggrieved "service provider, subscriber or other person" may bring a civil action against the "person or entity other than the United States which engaged in that violation" of ECPA Title II.[143] If the person or entity who violated Title II committed such violation with scienter, meaning with knowledge or intent, the aggrieved party may recover, under subsection (b), preliminary, equitable and/or declaratory relief, as well as, reasonable attorney fees and court costs.[144] Further, under subsection (c), the aggrieved party may recover actual damages, the violator's profits, punitive damages, and statutory damages no less than $1,000.[145]

However, a person or entity that is alleged to have violated Title II can assert several defenses under subsections (e) and (f).[146] First, no civil action may be brought under Title II if it was filed more than two years after the alleged violation.[147] Second, if a person or entity violated Title II based on a good-faith reliance on the authority granted to it by a statute, warrant, subpoena, court order, or at the request of the police or other investigative personnel, it would not be held liable.[148] Further, it is "a complete defense to any civil or criminal action brought under any law" if it is determined that an electronic-communication service provider disclosed the contents of an electronic communication to a person or entity based upon a good-faith reliance.[149] The disclosure must be predicated upon the good-faith belief that the provider had the consent of a party to the communication, the information was disclosed to an in-

140. *Id.* § 2703(c)(2) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).
141. *Id.* § 2703(c)(3) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).
142. *Id.* § 2703(e).
143. *Id.* § 2707(a).
144. *Id.* § 2707(b).
145. *Id.* § 2707(c).
146. *Id.* § 2707.
147. *Id.* § 2707(f).
148. *Id.* § 2707(e).
149. *Id.*

tended party of the communication, and/or the information pertained to the commission of a crime.[150]

### E. Section 2712

Section 2712 of ECPA Title II provides that an aggrieved person may bring a civil action against the United States to recover money damages for a willful violation of ECPA Title II.[151] The aggrieved party may recover, under subsection (a), actual damages no less than the sum of $10,000 and reasonable litigation costs.[152]

However, the United States can assert several defenses under subsections (b) and (e).[153] First, a civil action may be brought under Title II against the United States only after the claim is presented to the appropriate department or agency under the procedures of the *Federal Tort Claims Act*.[154] Second, the civil action is barred unless it is presented to the appropriate department or agency in writing within two years after the claim accrues or the action has commenced within six months after the date the appropriate department or agency mailed notice of final denial of the claim.[155] Further, the United States may move the court for a stay of the civil action if discovery will "adversely effect the ability of the [g]overnment to conduct a related investigation or the prosecution of a related criminal case."[156]

In sum, Title II is a detailed statute that is effective in preventing many persons and entities, especially the government, from unlawfully accessing and disclosing electronically stored wire or electronic communications. The following section of this article is devoted to a detailed discussion of the effectiveness of Title II in remedying the Internet information-privacy problem.

## V. THE ECPA AND THE RIGHT TO INFORMATION PRIVACY ON THE INTERNET

### A. Applicability and Effectiveness of Title II

An individual's personal information is more often than not accessed and/or disclosed while it is in electronic storage.[157] All information that is transmitted via the Internet is considered to be an electronic commu-

150. *Id.*
151. *Id.* § 2712 (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).
152. *Id.* § 2712(a) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).
153. *Id.* § 2712 (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).
154. *Id.* § 2712(b) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).
155. *Id.*
156. *Id.* § 2712(e) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).
157. *See* Sessler, *supra* n. 55, at 635.

nication that affects interstate commerce.[158] ECPA would apply to e-commerce entities because, arguably, these entities fall within the definition of an electronic-communication service provider or a remote computing service since they provide their subscribers or users "the ability to send or receive [an] electronic communication."[159] By way of illustration, an Internet user of an individual or company's Web site receives an electronic communication just by visiting the Web site. Since the Internet user requests the Web site to be sent to him, arguably, the Web site owner is sending the user an electronic communication. Further, the Internet user has the ability to download information contained on the Web site and may send the Web site owner registration information by filling out an electronic registration form. Thus, most likely, these e-commerce entities will be found to be providers of an electronic communication service.

However, ECPA Title II, in its current form, would not adequately protect an individual's personal information that was transmitted via the Internet and subsequently electronically stored in an electronic record on an e-commerce entity's server from being disclosed to the private sector.[160] As discussed in Part II, an e-commerce entity gathers an individual's information via the Internet by several means and creates an electronic record that is electronically stored on its server. Title II, in its current form, would prevent the e-commerce entity from disclosing the contents of any electronic communication, except information transmitted by a cookie, stored on their computer system to any person or entity.[161] For example, Widgets.com would be prohibited from disclosing the contents of a customer's order to any person or entity, including the private sector, without the member's consent. Title II would also generally prevent a governmental entity from receiving a record or other information pertaining to a subscriber or customer of the service provider.[162] Thus, a governmental entity would arguably be prohibited under Title II from receiving an electronic record stored by Widgets.com. But, Title II permits an electronic-communications service provider, or a remote com-

158. 18 U.S.C. § 2510(12).

159. *See id.* § 2510(15).

160. *See generally* 18 U.S.C. §§ 2701-2712 (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

161. *Id.* §§ 2702(a)(1)-(2) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)); *see In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d at 511 (holding that a cookie is not an electronic communication protected from disclosure by Title II). Arguably, the *DoubleClick* decision is inapplicable to an electronic record as the electronic record, is not comprised solely from the contents of a cookie but rather is an organized collection of related items of data compiled from various sources pertaining to a subscriber or customer and, thus, arguably falls under 18 U.S.C. § 2702(a)(3) and not § 2702(a)(1) and (2).

162. 18 U.S.C. §§ 2702(a)(3) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

puting service to disclose a "record or other information pertaining to a subscriber to or customer of such service . . . to any person other than a governmental entity."[163] Therefore, it is lawful for an e-commerce entity to disclose the information contained in an electronic record to any private entity that is willing to purchase it. This is because Title II contains a fine-line distinction between disclosure of a subscriber's record or other information to a governmental entity and disclosure to the private-sector.[164] But for this private sector exception, Title II would effectively address Internet information-privacy concerns regarding the electronic storage and disclosure of an individual's personal information contained in an electronic record.

### B. A Proposed Amendment to Title II to Remedy the Above Loophole

It is this author's contention that ECPA Title II should be amended to repeal this exception. The amended Title II would repeal Section 2702(c)(5), revise section 2702(a)(3) to include disclosure to any person or entity, and add the above definition of personal information to Section 2510. Further, Section 2707 would be amended to include a new damages provision for the unlawful disclosure of an individual's personal information and/or electronic profile to the private sector. This personal-information damages provision would entitle an aggrieved party whose personal-information was unlawfully accessed and/or disclosed to actual damages (not including personal injury, mental or emotional distress), injunctive relief, and reasonable attorney's fees and costs for the prevailing party.

Thus, the new Title II would prohibit an e-commerce entity, electronic- communications service provider, or remote computing service from unlawfully disclosing an electronic record to the private sector. The proposed revisions would make Title II apply equally to the private sector and a governmental entity for the unlawful access and disclosure of the contents of an electronic communication as well as a user, subscriber, or customer's personal information contained in an electronic record. Further, similar exceptions may apply to the private sector. Thus, it would be lawful for an e-commerce entity to disclose a user's electronic record to the private sector, if such private entity obtained the user's consent and/or upon a subpoena or court order. Moreover, Section 2703(c) would remain in effect as it adequately controls the circumstances in which an electronic-communication service provider or remote comput-

163. *See id.* § 2702(c)(5) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

164. *Compare id.* § 2702(a)(3) *with* § 2702(c)(5) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

ing service is permitted to disclose a user, subscriber or customer's personal information to a governmental entity.

## VI. CONCLUSION

"Technology propels us forward, and we react to the social consequences only after the fact . . . It may dawn on us too late that privacy should have been saved along the way."[165] The erosion of an individual's information-privacy rights via the Internet is a real and growing problem. ECPA is a judicially interpreted, time-tested, and well-established federal wire and electronic-communications privacy statute. It has been deterring and penalizing persons and entities for unlawfully intercepting, accessing, disclosing, and using wire or electronic communications for fifteen years. Title II prevents the unlawful access to electronically stored wire or electronic communications.[166] In addition, it prevents the unlawful disclosure of the contents of these stored communications to any person or entity.[167] However, Title II does not prevent the disclosure of an Internet user's personal information contained in an electronic record to the private sector.[168] This author has concluded that the most feasible solution to this Internet information privacy problem is by amending ECPA Title II. The proposed amendment would prohibit an e-commerce entity, electronic-communication service provider, or remote computing service from unlawfully disclosing an electronic record to the private sector. "The law [of information privacy] must advance with the technology . . . Congress must act to protect the [information] privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right."[169]

---

165. *See* Kang, *supra* n. 16, at 1286.

166. *See generally* 18 U.S.C. §§ 2701-2712 (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

167. *See generally id.* §§ 2702(a)(1) & (2) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

168. *Id.* § 2702(c)(5) (amended by *U.S.A. PATRIOT Act*, H.R. 3162, 107th Cong. (2001)).

169. *See* Sen. Rpt. 99-541 at 3.