III. ENHANCING CONSUMER PRIVACY ONLINE

[BACK][NEXT]

During the first day of the Workshop, participants discussed enhancing consumer privacy online through technological innovation, educa self-regulation, and law enforcement. They agreed that if consumers are not confident that their personal information will be protected or will not use the Internet for commercial purposes and the online marketplace will not thrive.(1)

A. Technologies to Enhance Notice and Consumer Choice Online

The Workshop highlighted three technologies that, in the view of many participants, could enhance online privacy and at the same time s legitimate needs of online businesses for information about current or potential customers. The approaches include technology that was the time of the Workshop, as well as technology that could be adapted or extended to enhance notice and consumer choice with respect information privacy online.

1. Universal Registration Systems

A representative of Internet Profiles Corporation (I/PRO), a market research firm, demonstrated the I/CODE system, a universal World W registration system.(2) Users and Web sites register with the system. When users register, they provide I/PRO with an array of personal information, including identifying information (name, street address, e-mail address), demographic information (age, gender, marital statu information about product and service preferences.(3) In return for this information, users receive an identifier called an I/CODE, which a to browse anonymously in the Web sites in the I/CODE system.(4) I/PRO aggregates the anonymous demographic information for mark analysis.(5)

When a user accesses a site in the I/CODE system, only the user's I/CODE and anonymous demographic information are transmitted to I/PRO uses the anonymous information collected in this manner by the site to perform aggregate data analysis for its clients. In respons request from the site, the user may opt to disclose his or her e-mail address, in order to receive future communications from the site, and then forwards the user's name and street address to the site. Personally identifying information is not sent to the site without the user's e consent.(6) All of the personal information transmitted between I/CODE and sites registered in the I/CODE system is encrypted. I/PRO a sites within the I/CODE system are contractually bound not to share or sell collected personal information to entities outside the I/CODE

Within the I/CODE system, consumers enjoy a measure of control over how their personally identifying information is used online by reg sites. The system shelters users from unsolicited e-mail from Web sites within it and allows them to browse anonymously on the Web. A time it allows Web sites to conduct analysis of site usage and aggregate user preferences. The I/CODE system has proven to be popula users registered in the first ten weeks of its operation, and about 25,000 new subscribers are joining per week.(8) The Internet Profiles C representative opined that a universal registration system is preferable to a system of online disclaimers and notices, because the latter the interactivity of the online medium.(9)

2. Cookies

Before the advent of "cookies" technology, a Web site's server was unable to know whether the downloading of separate pages within th example, when a user browses from page to page within an online catalogue) represented one individual's series of movements or the s movements of many individuals.(10) Cookies were invented to enable the Web site's server to keep track of a particular user's activity wi site. Cookies technology allows the Web site's server to place information about a user's visits to the site on the user's machine in a text only that Web site's server can read.(11)

Using cookies, a Web site assigns each user a unique identifier (not the actual identity of the user), so that the user may be recognized i subsequent visits to that site.(12) On each return visit, the site can call up user-specific information, which could include the user's prefe interests, as indicated by documents the user accessed in prior visits or items the user clicked on while in the site.(13) An expiration date allows cookies to be set to remain on a user's machine either permanently or for a specified length of time.(14) Cookies also vary in the security they provide for the information they contain.(15)

Cookies can store information that facilitates the interaction between user and Web site. As an example of how a permanent cookie func consider the online version of a newspaper. If a subscriber whose native language is Spanish informs the Web site that he prefers to dow Spanish edition of the newspaper, the newspaper can store that information in a cookie file on the user's hard drive. When the subscribe enters the newspaper's Web site, the site retrieves the language preference information from the cookie and automatically sends the Sp language edition to the user.(16) Temporary cookies can be created during online shopping expeditions. The cookies can tag the shoppe intended purchases to facilitate the ordering process and then expire after a purchase is made.(17)

According to the representative of Netscape Communications Corporation, cookies technology could be used by Web sites to facilitate communication of consumers' privacy preferences.(18) Once a user communicated his or her privacy preferences in response to a Web

notice of its information practices, the site could store that information in a cookie text file on the user's hard drive. The dialogue around p preference, notice, and consent that initially took place between user and site would, therefore, not have to be repeated in subsequent v site.(19)

3. Platform for Internet Content Selection (PICS)

The World Wide Web Consortium at the Massachusetts Institute of Technology developed its Platform for Internet Content Selection (PI enable parents to block their children's access to Internet sites whose content the parents deem objectionable.(20) PICS establishes a s "labeling" Internet sites on the basis of their content and for creating label-reading software to block access to some sites and permit acc others based upon the labels. PICS is a set of technical specifications, a standard format for labels; it is neither software nor label, but te language that allows software and label to work together.(21)

PICS itself is "viewpoint-neutral."(22) Anyone can develop a set of content-rating criteria (identifying "hate speech," for example, or "exce nudity"), create a labeling vocabulary, evaluate Internet sites, and use the PICS specifications to label sites accordingly. Labels are affixe electronic documents such as home pages on the World Wide Web by site owners or third parties -- parent groups, religious groups, cor groups -- who can locate their labels on agreed-upon sites. Software capable of reading labels in the PICS format may be developed ind of these labels. This software automatically checks for the labels and blocks access to sites based upon the labels.(23) Thus, if a user's has been configured to block electronic documents labeled as "excessively violent" by a site-rating service that screens Web sites for su it will deny access to any site to which the rating service's "excessive violence" label is affixed. The user can override the software's acti through use of a password.(24)

The use of PICS technology for content-blocking purposes is proliferating.(25) Several panelists noted that PICS technology could be ac enhance online privacy.(26) Industry groups, privacy advocates, and consumer groups could use existing PICS technology to create rati based upon the privacy-protectiveness of Web sites' information practices, and these systems could then be used to block access to site strong protections.(27) If, for example, a consumer group created an index of privacy-protective Web sites based upon a review of their i practices, a user could set her PICS-compatible browser to allow access only to sites labeled as being in the index. The label-reading so would block access to sites that were not on the list.(28)

PICS technology might be extended further to allow more sophisticated notice and choice options. The prerequisite to extending PICS te would be a standard format for describing information practices and user preferences as to how their information should be used.(29) A set his preferences (e.g., "no restrictions on use" or "no transfers to third parties") on his computer with software that employs this forma sites would similarly give notice of their information practices (e.g., "we do not sell or rent our customer list to other companies"). The us browser would be capable of automatically comparing his preferences with sites' practices, as the user moves around the World Wide W particular Web site's practices matched the user's preferences, notice and choice would occur "seamlessly" in the background, and the u proceed to enter the site. If there were a mismatch, the user's software would alert him to that fact.(31) The Web site could respond by p explanation for the mismatch, or offering the user an opportunity to view its information policy.(32) The Web site could offer the user ince such as discounts in exchange for the user's agreement to accept the site's information practices.(33) Finally, extended PICS technology theoretically enable this sort of negotiation about notice and choice to be automated.(34)

4. Participants' Views on the Demonstrated Technological Approaches

Workshop panelists agreed generally that the technologies demonstrated are promising means of advancing consumer privacy.(35) The disagreement, however, as to whether these technologies are sufficient to address the full range of online privacy concerns. For some pa technologies including encryption, that allow individuals to use the Internet anonymously, offer more effective privacy protection.(36)

Participants devoted considerable time to the PICS technology, and raised several concerns. Representatives of the direct marketing an information industries viewed filtering technologies such as PICS as "blocking technologies" that give consumers a "no" vote on entire ca information content available online. IIA opined that use of PICS to block information by category, rather than on a case-by-case basis, w unacceptably restrict commercial speech.(37) A DMA representative shared this concern and asserted that filtering technologies such as should be paired with technology that allows consumers to release information alerting marketers to the kinds of products and services a they would be willing to accept solicitations. In DMA's view, this would balance consumers' privacy with the needs of businesses whose investments are crucial to the success of the online marketplace.(38)

Others expressed concern that a PICS-based model for notice and consent would be too complicated and frustrating for consumers, esp they were continually required to reset their privacy preferences.(39) One panelist argued that this model would unjustifiably shift the bur industry to consumers to take affirmative steps to protect their privacy.(40) A representative of the advertising industry opined that online interactions could disrupt the substantive dialogue between marketer and customer (or potential customer). According to this panelist, th such interactions would be critical.(41)

PICS proponents countered that any use of the Internet requires many affirmative steps and that the additional steps consumers would t PICS to express privacy-related choices would not be burdensome.(42) PICS, they argued, empowers individuals to express a broad ra preferences and enables Web sites to respond to the variations.(43) Technology like PICS, which builds an information profile, works in t background and need not interrupt the communication between the user and a Web site.(44) According to one panelist, it would therefor possible to create a system in which users would set their privacy preferences once, and the question of compatibility of their privacy pre and Web sites' privacy policies would be resolved automatically through communication between computers.(45)

Privacy advocates expressed the concern that PICS technology is valuable only where a consumer is interacting directly online with an e seeking to use his or her personal information.(46) For this type of interaction, these participants agreed that PICS provides useful tools

enhancing notice and choice.(47) These panelists argued, however, that PICS does not address the online use of a consumer's persona information by entities with whom that consumer has had no direct relationship.(48) Yet the unauthorized collection and use of personal i by third parties is, in one participant's view, so common that it is "where the action is today on the Internet."(49) In such situations, it was the government has a role to play in protecting individual privacy online.(50)

The extension of PICS technology to interactions between users and Web sites around notice and choice issues is currently a theoretica An extended PICS regime will require a standard vocabulary for describing Web sites' information practices and for labeling Web sites.(5 labeling vocabulary could be based upon existing rating systems or could be developed from new criteria.(52) Panelists speculated upor feasibility of a regime in which Web sites labeled themselves. Several panelists argued that independent entities should label and rate W sites,(53) but others doubted whether this was realistic, given the sheer number of Web sites and the difficulty in ascertaining Web sites' information practices.(54) Web site self-labeling, coupled with third party certification of label accuracy, was said to be a more efficient approach.(55)

Ultimately, there was considerable optimism that an online notice and choice regime based upon PICS technology is attainable. The onli is continually evolving, and several participants suggested that it can be shaped to create electronic privacy protections in relatively shor industry, technologists, and privacy advocates work together to that end.(56) The result could be an online environment in which users c safe interacting with Web sites and could choose to reveal personal data where they felt it was in their interests to do so.(57)

B. Consumer and Business Education

Workshop panelists agreed that consumer and business education is an indispensable component of any strategy to protect consumer p online and ensure the growth of the online marketplace. As several panelists pointed out, consumers generally know little about the way personal information can be used online.(58) They do not understand the potential risks of divulging personal information online, and the guidance on how to protect that information from unauthorized use.(59) This is true for both new and seasoned users of the Internet.(60) Consumers also need to understand the trade-offs in order to make an informed decision to divulge personal information online.(61) Par noted that business must be educated about the importance of privacy protection to the growth of the online marketplace,(62) and that s businesses, in particular, must be shown the benefits to their enterprise of protecting the privacy of personal information.(63)

Several panelists stated that industry, consumer groups, and government all have a role to play in educating consumers and businesses online privacy issues.(64) Such efforts should proceed on many fronts and in many media. Panelists urged that educational efforts be cr they should take advantage of the interactive nature of the online marketplace and include fresh approaches. Computer companies, for could include point-of-sale materials with each new computer.(65) Panelists also urged that consumers be involved in education efforts a such efforts be directed toward the elderly, who are increasingly active on the Internet,(66) and toward young people.(67)

Several panelists noted that the power of new electronic technologies can be harnessed to further education efforts. Individual online en educate their visitors simply by disclosing their information practices electronically.(68) The Privacy Rights Clearinghouse, a non-profit c education and research program, provides guidance for protecting information privacy online, and interacts with consumers across the c through its site on the Internet.(69) In March 1995, ISA and the National Consumers League (NCL) launched Project OPEN (the Online Education Network) to educate consumers on important online issues, including privacy.(70) There was a suggestion that the Commissi with ISA, NCL, DMA and other interested parties to develop a model business curriculum on online privacy issues.(71) Efforts of this sor necessary complement to technological approaches to protecting information privacy online.(72)

C. Participants' Views on Self-Regulation and Government's Role

Throughout the first day of the Workshop, participants expressed differing views of the role government should play in the area of online information privacy. Industry representatives and trade associations took the position that it would be both inappropriate and counterpro mandate particular privacy protections. According to these participants, regulation would stifle the creativity and innovation that have ma development of interactive media to date,(73) could infringe important First Amendment rights,(74) and might force marketers off the Inte entirely.(75) Government should step back, it was argued, and permit industry to develop privacy protection models.(76)

According to these panelists, market pressures will define the best privacy protections,(77) as consumers increasingly make known their preferences regarding information privacy online.(78) In their view, it is critical that government permit the development of a healthy marl online privacy protections.(79) Moreover, according to several panelists, regulation is an insufficiently precise method of shaping informa online. Given the rapid pace of technological development in interactive media, government regulations tied to particular technologies w quickly become obsolete.(80)

Panelists strongly disagreed about whether emerging technologies would obviate the need for governmental regulation to protect online ISA's representative saw PICS as an especially important alternative to government regulation in the global online marketplace. Regulat limited by the geographic boundaries of the regulating jurisdiction; but PICS can operate globally to benefit both industry and consumers Privacy advocates argued that the technologies demonstrated during the Workshop are not a substitute for an enforceable code of fair ir practices, and that they are not likely to flourish without government enforcement of privacy rights.(82) One panelist urged the Commissi assume that these technologies can solve all abuses related to information privacy online.(83)

Panelists offered various opinions on the role the Commission should play in protecting individual privacy online. Some privacy advocate that the Commission should intervene promptly to protect online privacy. In their view, purely self-regulatory approaches to protecting pri failed.(84) Self-regulation will not be effective, according to these participants, unless regulation operates in the background to deter bad Otherwise, companies that abide by self-regulatory guidelines will be at a competitive disadvantage.(85)

Some participants suggested that the Commission should undertake research on issues related to information privacy online. Several pa urged, for example, that the Commission conduct focus groups with users of online services and with consumers generally, to obtain an understanding of their expectations and experiences regarding online privacy and to assess issues such as consumers' willingness (or la thereof) to divulge personal information in return for customized products and services.(86)

Finally, several panelists stated that the Commission has the authority to step in where online information collection and use are shown t fraudulent or deceptive, in violation of the Federal Trade Commission Act.(87) Law enforcement was said to be appropriate where, for ex company misrepresents the nature of its online information practices or fails to adhere to the practices it has announced.(88)

---

1. See e.g., Rotenberg 24; Krumholtz 38; Jaffe 105; Wellbery 205.

2. Poler 64-68.

3. I/PRO Comment, FAQ List and Answers, at ¶ 1.3 (Doc. No. 12).

4. Id.

5. Id. at ¶ 5.4.

6. Poler 67; I/PRO Comment, FAQ List and Answers at ¶ 5.2 (Doc. No. 12).

7. I/PRO Comment, FAQ List and Answers at ¶¶ 5.5-6.2.

8. Poler 66; I/PRO Comment at 5 (Doc. No. 12).

9. Poler 65.

10. Harter 71.

11. Id. Although not discussed at the Workshop, there has been controversy surrounding cookies, because users initially were unaware t cookies were being created on their hard drives. The latest version of Netscape's Web browser, Navigator 3.0, includes an alarm that ca activated at the user's discretion. Once activated, the alarm sounds before a cookie is created on the hard drive. Harter 74.

12. W. Andrews, "Sites Dip Into Cookies to Track User Info," Webweek 17 (June 3, 1996).

13. Id.

14. Harter 72.

15. Harter 74. Ordinary cookies employ hypertext transfer protocol (HTTP); "secure" cookies employ secure hypertext transfer protocol (Id.

16. Harter 71-73.

17. Andrews, supra n. 84.

18. Harter 73.

19. Id.

20. Resnick Comment at 2 (Doc. No. 14).

21. Id. at 3; Resnick 80-81.

22. Vezza 77, 131.

23. Resnick Comment at 3 (Doc. No. 14).

24. See Resnick Comment at 3-5 (Doc. No. 14).

25. Software capable of reading PICS labels is currently being included in new versions of Internet browsers and in programming offered services. Content labeling and rating services will soon be publicly available. Vezza 77; CDT Comment at 15 (Doc. No. 5); Resnick Com (Doc. No. 14). For a discussion of currently available PICS-compliant filtering software for children, see Appendix F.

26. Resnick Comment at 2 (Doc. No. 14); CDT Comment at 16-23 (Doc. No. 5); Vezza 78.

27. CDT Comment at 20 (Doc. No. 5).

28. Id. at 21.

29. CDT Comment at 4 (not paginated) (Doc. No. 22); Resnick 87. At this time there is no agreed-upon vocabulary for describing particu information practices as "privacy protective." However, a hypothetical application of PICS technology, using the Canadian Standards Ass (CSA) 1996 Model Code for the Protection of Personal Information as the basis for such a rating vocabulary, was demonstrated at the W In this hypothetical scenario, the user's browser is configured to locate Web sites that carry a CSA label. PICS technology gives the user flexibility to set his preferences to reflect the degree to which he is concerned about various requirements of the CSA Code. If, for examp willing to access sites that comply with some but not all Code provisions, he can so indicate. If he does not want to do business with site they are in full compliance with the Code, he can set his preferences accordingly and the software will block access to non-complying sit Resnick 83-85.

30. According to CDT, the ability to pre-set the user's preferences is more protective of privacy than a model that forces the user to decic to opt-out of a site's information practices on a transaction-by-transaction basis. Comment at 4 (not paginated) (Doc. No. 22).

31. CDT Comment at 18-20 (Doc. No. 5).

32. Id. at 20; Resnick 85; Resnick Comment at 9-10 (Doc. No. 14).

33. Resnick Comment at 10 (Doc. No. 14).

34. Id; Resnick 86.

35. See, e.g., Jaffe 103; Ek 96-97; Rotenberg 99, 101-02; Weitzner 95-96; Hendricks 107; Vezza 78; Reid 121; IIA Comment at 11 (Doc. Givens Comment at 1 (Doc. No. 9).

36. Harter 74; Hendricks 107; Rotenberg 137.

37. IIA Comment at 12 (Doc. No. 23).

38. Reid 91-93, 121.

39. IIA Comment at 11-12 (Doc. No. 23).

40. Rotenberg 99.

41. Jaffe 104-05.

42. Weitzner 114; Goldman 126.

43. Weitzner 114-15.

44. Vezza 109.

45. Goldman 126-27.

46. Smith 42-43; Rotenberg 99-100.

47. Rotenberg 101-02.

48. Smith 42-43; Rotenberg 99-100.

49. Rotenberg 100. Indeed, one panelist asserted that credit reports, social security numbers, arrest records and unlisted telephone num currently being sold online without the data subjects' knowledge. Smith 42.

50. Rotenberg 102.

51. Reidenberg 111; Westin 117-18; Resnick Comment at 10 (Doc. No. 14). This would be especially true, if labeling is to be done by We themselves. Resnick Comment at 10 (Doc. No. 14).

52. Resnick Comment at 10 (Doc. No. 14).

53. Golodner 120; Ek 125. See also Reidenberg 112. It is likely that many rating entities will be created. One recent effort is eTRUST, a p the Electronic Frontier Foundation and CommerceNet, a non-profit association of banks, telecommunications companies, Internet servic providers, online services and software developers. eTRUST is developing online privacy standards and a system for rating Web sites' p protections that will be communicated through licensed visual symbols. Developments in this effort are posted to eTRUST's Web site at http://www.eTRUST.org.

54. Knight 124-25; Resnick Comment at 10 (Doc. No. 14).

55. Reidenberg 133; Resnick Comment at 11 (Doc. No. 14). The role such certification authorities would play was analogized to that of a who certify that business' records conform to generally accepted accounting principles. Reidenberg 133.

56. Resnick 88; Weitzner 95-96; Vezza 109; Berman 254.

57. Resnick Comment at 11 (Doc. No. 14).

58. Jaffe 36; Givens 231; Golodner 246; Smith 259; CDT Comment at 8 (Doc. No. 5).

59. Golodner 246.

60. Smith 259.

61. Cole 265.

62. Burrington 242-43; Strenio 255-56; Smith 259-60.

63. Burrington 242-43; Strenio 256.

64. Burrington 239, 242; Golodner 246-47; Strenio 255; Givens Comment at 3 (Doc. No. 9); IIA Comment at 14 (Doc. No. 23).

65. Golodner 246; Strenio 255.

66. Golodner 247.

67. Id; Givens 234-35.

68. See Givens 231-32; Burrington 242. World Wide Web sites operated by DMA, ISA and CDT currently disclose their information-gath practices in this manner. Heatley 263; ISA Comment (Doc. No. 15, Attachment); Goldman 15-16. These sites are located at http://www.t dma.org; http://www.isa.net; and http://www.cdt.org, respectively. Panelists asserted that interactive regimes for notice and consumer ch useful in educating consumers about online privacy issues. Givens 231-32; Burrington 242.

69. Givens Comment, Attachment at 1 (Doc No. 9). The Internet address is http://pwa.acusd.edu:80/~prc/. Privacy Rights Clearinghouse Sheet devoted to protecting individual privacy in cyberspace may be found at http://pwa.acusd.edu:80/~prc/fs/fs18-cyb.html.

70. Burrington 241; ISA Comment at 2 (Doc. No. 15). Project OPEN's site on the World Wide Web is http://www.isa.net/project-open.

71. Burrington 242.

72. Burrington 239.

73. CASIE Comment at 2 (Doc. No. 18); ISA Comment at 2 (Doc. No. 15). This view was echoed by the representative of the National Telecommunications and Information Administration, U.S. Department of Commerce. Wellbery 205.

74. IIA Comment at 10 (Doc. No. 23).

75. Krumholtz 38.

76. Krause 46.

77. IIA Comment at 5-6 (Doc. No. 23); Jaffe 36.

78. Jaffe 36; Consumer Alert Comment at 4-5 (not paginated) (Doc. No. 13).

79. Westin 40-41. See also Sherman 26-27.

80. Poler 54; Ek 98; Cochetti 209; Vezza 227. Industry participants and some public interest groups generally viewed self-regulatory effo necessary complement to technological innovations designed to enhance online information privacy. Reid 90; IIA Comment at 11 (Doc N See also Consumer Alert Comment at 5 (not paginated) (Doc. No. 13) (arguing that self regulation and market-driven technological inno efficient alternatives to regulation in this area). Participants noted that self-regulatory efforts developed for traditional marketing media ar applicable to the online environment. Efforts are currently underway, for example, to adapt the DMA's Fair Information Practices Manual account the unique qualities of interactive media, including the Internet. Reid 91. Consumer choice mechanisms such as the DMA's Mail Preference Service, for example, could be expanded to the online environment, giving consumers the choice to "opt-out" of particular on of their personal information by participating member Web sites. Reid 91-92. One participant argued that the Mail Preference Service is because it is voluntary. Givens Comment at 2 (Doc. No. 9).

81. Ek 97-99.

82. Rotenberg 137; Givens Comment at 1 (Doc. No. 9).

83. Givens Comment at 1-2 (Doc. No. 9).

84. See, e.g., Rotenberg 21; Hendricks 32. One panelist urged the Commission to establish standards against which self-regulatory effo be measured, and to impose time limits for compliance with those standards. In the absence of timely compliance, the Commission shou a regulatory scheme. Givens Comment at 3 (Doc. No. 9).

85. Rotenberg 23.

86. Burrington 238; Golodner 245; Strenio 254-55. See Givens Comment at 3 (Doc. No. 9).

87. Plesser 50; Sherman 51; Jaffe 104; Reidenberg 112; IIA Comment at 5, 8, 10 (Doc. No. 23).

88. Jaffe 104; Reidenberg 112.

[BACK][NEXT]

Last Modified: Monday, June 25, 2007