Federal Trade Commission
Protecting America's Consumers

II. ONLINE PRIVACY: General Practices and Concerns

[BACK][NEXT]

The first day of the Workshop focused on current online uses of personal information, the core elements of voluntary privacy protections interactive technologies for enhancing notice and choice, and the Government's role in protecting consumer privacy online. Individual W sessions also addressed consumer and business education strategies, the special issues posed by online uses of medical and financial information, and the potential impact of the European Union's Directive on the Protection of Personal Data on the online marketplace in t States.(1) This part of the report draws on both the Workshop transcript and comments submitted for inclusion in the Workshop record.

A. Current Collection and Uses of Information

The Internet is a highly decentralized, global network of electronic networks. It is unique among communications media in the variety an the personal information generated by its use.(2) When users browse on the World Wide Web ("the Web"), for example, they leave an el marker at each site (or on each page within a site) they visit. The series of electronic markers, or "clickstream," generated by each user's activities can be aggregated, stored, and re-used.(3) Each Web site, in turn, captures certain information about users as they enter the s site can "know" users' e-mail addresses, the names of their browsers, the type of computer they are using, and the universal resource lo (URL), or Internet address, of the site from which they linked to the current site.(4)

This information-gathering capability is built into the software that makes the Internet function.(5) Indeed, the software requires clickstrea be collected so the computer receiving the data can send the information file requested by a user (e.g., the Internet address of the next W that the user wants to browse) to that user's computer, rather than someone else's.(6) Clickstream data also permits Internet site owners understand activity levels at various areas within sites,(7) in a manner analogous to a retail store's practice of checking inventory.(8)

The fact that online information-gathering is automated means it is invisible to the user and often takes place without the user's knowled consent.(9) Internet users may also voluntarily disclose personal information, including their e-mail addresses, by filling out a questionna request of an online marketer,(10) or participating in a chat room, bulletin board, or other online forum. From such activities it is possible accumulate lists of individuals' e-mail addresses for marketing purposes.(11) Marketers, in turn, increasingly use electronic mail to reach current and potential customers.(12) Unsolicited commercial e-mail messages, though not always unwelcome,(13) are a growing proble Consumers incur the burden of processing such e-mail and the costs of downloading and reading it, including the time charges from thei services.(14) Electronic mass mailings of online commercial solicitations also impose burdens on computers operated by online services Internet access providers, with corresponding adverse effects for their subscribers.(15)

B. Consumers' Attitudes About Privacy And Interactive Media

While there is much to be learned about consumers' views on the collection and use of personal information in the online environment, it possible to discern some general trends. Survey research conducted over the last twenty years documents deep concern among Americ how personal information is being used in the age of computers.(16) In a 1994 Harris Survey of Americans' attitudes about privacy and e interactive technologies, eighty-two percent of respondents stated that they are concerned about threats to their personal privacy.(17) Ac the same survey, seventy-eight percent of respondents believe that consumers have lost all control over how businesses circulate and u personal information; seventy-six percent believe that businesses ask consumers for too much personal information;(18) and seventy pe refused to give information to a business because they felt it was either unnecessary or too personal.(19)

These findings must be understood in the context of a complex array of individual consumer attitudes about privacy in traditional context several Workshop participants noted, the decision to divulge or not divulge personal information varies not only with the individual, but al context.(21) According to one panelist, survey research consistently indicates that roughly one-quarter of the American public is "intense concerned about privacy and that another quarter has little or no concern; the remaining fifty percent view this issue pragmatically, appro on a case-by-case basis.(22) These individuals consider factors such as: the nature of the benefit being offered in exchange for persona information; whether the information being collected is relevant to the benefit or socially acceptable; and whether adequate safeguards a to protect their information.(23)

Survey results suggest that although many individuals are willing to strike a balance between maintaining personal privacy and obtaining information and services that new interactive technologies provide, they are concerned about potential misuse of their personal informati want meaningful and effective protection of that information.(24) In the 1994 Harris Survey, fifty-one percent of respondents stated they w concerned if an interactive service to which they subscribed engaged in "subscriber profiling," i.e., the creation of individual profiles base subscribers' usage and purchasing patterns, in order to advertise to subscribers.(25) Respondents were less concerned about subscribe where the interactive service provided privacy safeguards for subscribers, such as notice of when a profile would be created and how it w used, control over the types of information to be used for advertising and the types of advertising employed, and access to the informatio

profile.(26)

C. Privacy Protections: Areas of Agreement and Divergent Views

Workshop participants expressed a common understanding about the necessary elements of self-regulatory approaches to protecting co privacy online, but differed greatly on how to implement them. These elements closely track fair information practices identified by the U. Department of Health, Education & Welfare in 1973.(27) More recent government efforts to define privacy principles for interactive media incorporate these practices,(28) as do policies already in use in traditional marketing media. Privacy advocates did not dispute the value these measures, but argued that self-regulatory efforts are successful only against a background of legally enforceable rights to informat privacy.(29)

Many businesses operating in traditional media have yet to develop privacy policies,(30) and many businesses operating online have no confronted the privacy issues posed by interactive technologies.(31) Hence, few Web sites have privacy policies or display their informat practices to consumers.(32) With increasing competitive pressures to provide privacy protections, industry is recognizing the need to ad issue.(33) Indeed, the need to craft privacy policies is implicit in information practice guidelines promulgated by various industry groups.(

1. Notice

Workshop participants generally agreed that notice of information practices is an essential first principle in advancing online information privacy.(35) All of the guidelines and industry statements submitted by participants call for some form of notice of information practices to consumers.(36) Participants stated that, at a minimum, notice should include the identity of the collector of the information, the intended information, and the means by which consumers may limit the disclosure of personal information.(37)

2. Consumer Choice

Panelists also agreed that consumers should be able to exercise choice with respect to whether and how their personal information is us by businesses with whom they have direct contact online or by third parties. Panelists disagreed, however, as to how that choice should exercised. Industry representatives for the most part favor an "opt-out" approach, which allows personal information to be used unless c notify marketers that their information is not to be used in specified ways.(38) The privacy policies of America Online and CompuServe i "opt-out" mechanism that subscribers may use to have their names removed from membership lists made available to third parties.(39) and ISA's proposed Joint Statement on Online Notice and Opt-Out follows this approach,(40) as do DMA and ISA's proposed Principles Unsolicited Marketing E-mail.(41)

Some privacy advocates believe that requiring affirmative consent prior to any collection or commercial use of a consumer's personal inf the most effective privacy protection.(42) In their view, individuals have a property interest in their personal information. This interest can protected only through an "opt-in" regime that maintains the privacy of personal information unless an individual releases it.(43) Other pr advocates argued that interactive technology can provide an alternative to regimes requiring only an "opt-out" or an "opt-in." In their view could be used to allow consumers to communicate their privacy-related preferences automatically for all of their online interactions or on case-by-case basis.(44)

3. Data Security and Consumer Access

Panelists agreed that the security of personal information is essential if commerce in cyberspace is to flourish on the Internet.(45) Many agreed that consumers should have access to information about them that is held by marketers and other online businesses, and that co such information should maintain the information's accuracy and timeliness. IIA's Fair Information Practices Guidelines, DMA's Guideline Personal Information Protection, and CASIE's Goals for Privacy in Marketing on Interactive Media all call for mechanisms giving consum to stored information about them and a right to correct that information when necessary.(46) Privacy advocates likewise view access to p information as an essential privacy protection.(47) Panelists also agreed that the entities holding such information must take steps to pro loss or misuse.(48) Both IIA and DMA call for such protections in their guidelines.(49) IIA encourages its members to require any third pa whom they transfer personal information to extend a comparable level of protection.(50)

D. Sensitive Data: Medical and Financial Information Online

The first day of the Workshop focused on privacy practices and protections generally, rather than on particular categories of information collected. One panel, however, was devoted to online uses of medical and financial information, two categories generally thought to be p sensitive and worthy of special protection. As one panelist noted, of all the types of information collected about individuals, the public is r troubled by the prospect of unauthorized disclosure of medical and financial information.(51) Changes in the health care and financial ind affect how such personal information is used. As the health care industry changes, there is a move toward computerization of patient rec electronic exchange of medical information.(52) In the financial world, there are growing pressures to target-market products and service individual consumers that require the collection and use of detailed personal information.(53)

Several panelists noted the benefits of online technology in the areas of health care and financial services.(54) Electronic transmission o information, for example, can enhance the quality of health care by facilitating long-distance consultations between doctors(55) and by a doctors to use e-mail to monitor their patients' compliance with treatment regimens.(56) One panelist opined that online technology could consumers by making financial information that is currently available only through intermediaries, such as credit reports, instantly availab them.(57)

Concerns about online uses of medical or financial information fall into two categories. First, there is a concern about unauthorized acce sensitive medical and financial information. The confidentiality of medical records, for example, could be compromised,(58) and informat misused by third parties who gain unauthorized access to it through chat rooms, bulletin boards, or by other means.(59) Second, there is about the commercial use of medical and financial information. DMA believes that medical information derived from a patient-provider re should never be disclosed or used for marketing purposes, unless the patient has voluntarily provided such information through questior the information has been otherwise compiled with the patient's knowledge.(60) DMA's Guidelines for Ethical Business Practice state that information such as credit card numbers and checking account numbers should not be sold, rented, exchanged, or transferred to third pa where the consumer has a "reasonable expectation" that the information will be kept confidential.(61)

Representatives of the direct marketing and banking industries rejected any approach that would categorically limit online commercial us financial information.(62) In DMA's view, the online marketplace will not become economically viable if marketers cannot use financial int to evaluate the credit-worthiness of a potential customer.(63) In the banking industry transfers of certain personal financial information ar institutions are essential to prevent fraud.(64) The American Bankers Association representative argued that privacy protections must be against the industry's need for customer accountability.(65)

Many panelists agreed that a secure online medium is a prerequisite for routine online transmission of medical and financial information, special protections are necessary for such information.(66) Privacy advocates viewed ready access to an individual's own medical and fi information as an essential privacy protection.(67) For some panelists, encryption and other technologies that facilitate anonymity, such Cards,(68) are valuable means of protecting the privacy of medical and financial information.(69)

---

1. A summary of the discussion on the European Directive is included in Appendix B.

2. Center for Democracy and Technology (CDT) Comment at 8 (Doc. No. 5). Footnote citations are either to the printed record of the Wo to comments submitted after the Workshop was held. All of these materials are on file at the Federal Trade Commission. The transcript c Workshop is available online at http://www.ftc.gov. Complete lists of Workshop participants and documents referenced in the footnotes c found in Appendices G and H, respectively. Copies of privacy guidelines and online privacy proposals submitted for the Workshop recor found in Appendix C.

Workshop participants differed in how they defined "personal information," for purposes of their guidelines or privacy-related proposals. Coalition for Advertising Supported Information and Entertainment (CASIE), for example, defines "personal information" as "data not oth available via public sources." Goals for Privacy in Marketing on Interactive Media (1996) at ¶ 3 (Doc. No. 18). The Direct Marketing Asso (DMA) Guidelines for Personal Information Protection use a similar definition. Doc. No. 24, Attachment B at 2 ("information that is linked individual on a file and that is not publicly available or observable"). Other organizations employ broader definitions. The Information Indu Association (IIA)'s Fair Information Practices Guidelines refer to "personally identifiable information," defined as "information relating to a or identifiable individual." Doc. No. 23, Attachment, at ¶ 1 Commentary. The Center for Media Education (CME) and the Consumer Fede America (CFA) define "personal information" very broadly, to include both "any information that is linked to or allows for the identity of inc children, their families, household members or other individuals the child knows to be determined" and such information as a child's phys psychological description, health, school, date of birth, interests and opinions, "when used in conjunction with identifying information." CM Proposal at 2 (Doc. No. 19).

3. Goldman 13-14; CDT Comment at 8-9 (Doc. No. 5).

4. Goldman 15-16. This scenario is drawn from the CDT online privacy demonstration, which is accessible through its Web site at www.c

5. Goldman 14, 16.

6. Ingenius Comment at 3 (not paginated) (Doc. No. 29).

7. Lieberman 316-17. Although the technology makes it possible for Web site owners to maintain logs of this "transactional" information visitor to the site, Goldman 14, it is currently difficult to accomplish this when more than one person uses the same computer. Ingenius C 3 (not paginated) (Doc. No. 29). Participants differed on the question of whether it is currently possible to tie clickstream data to particula individuals. Some panelists argued that it is indeed possible to use the clickstream data to create a profile of individuals' preferences and patterns. Howard 383. See also Goldman 14; CDT Comment at 8 (Doc. No. 5). Others asserted that tracking site activity for individuals g large, complex data files that cannot be used for profiling with current technology. Lieberman 317; O'Connell 321.

8. Waters 407.

9. Goldman 13; CDT Comment at 9 (Doc. No. 5). In certain instances, the transmittal of personally identifying information is blocked. If, f example, a user accesses the Internet through an online service provider such as America Online, Prodigy or CompuServe (as do forty-s of current users who access the Internet), the user's identity and e-mail address are protected by the service's proxy server, which is a c acting as an intermediary between the sender and recipient of information. Interactive Services Association (ISA) Comment at 2 (Doc. N Web sites that the user enters will obtain the address of the proxy server (e.g., aol.com), and not the user's e-mail address. Ek 98. In this only the online service provider could tie clickstream data captured from the user's browsing activities directly to the user. Similarly, if a u accesses the Internet from a computer system protected by a "firewall," as is true for many corporate systems, the user's e-mail address ascertained. ISA Comment at 2 (Doc. No. 15); Goldman 16.

10. DMA Comment at 4 (Doc. No. 24).

11. The DMA and ISA's proposed Principles for Unsolicited Marketing E-mail provide that marketers who compile lists in this manner sho users whose names have been gathered an opportunity to have their information suppressed. Doc. No. 3 at ¶ 3; ISA Comment at 4 (Doc

12. ISA Comment at 3 (Doc. No.15).

13. Competitive Enterprise Institute (CEI) Comment at 2 (not paginated) (Doc. No. 31).

14. See Sherman 29.

15. ISA Comment at 3 (Doc. No. 15).

16. Louis Harris and Associates, Inc., Interactive Services, Consumers, and Privacy (conducted for Privacy & American Business) (1994 (Doc. No. 11) [hereinafter "1994 Harris Survey"] (summarizing results of surveys conducted from 1978-94). A national study of online an users' opinions on various privacy issues is currently being planned by Professor Alan Westin and Privacy & American Business. Westin

17. 1994 Harris Survey at 70 (Doc. No. 11).

18. Id. at 73-75, 76-78.

19. Id at 85-87.

20. Consumers' privacy concerns should also be viewed against the backdrop of federal privacy protections. There is no overarching fed statute governing information privacy in the United States. Congress has addressed information privacy on a sectoral basis, crafting stat govern distinct concerns and establish targeted individual rights. The Privacy Act of 1974, for example, places limitations on the collectio dissemination of information about individuals by federal agencies. 5 U.S.C. § 552a. The Tax Reform Act of 1976 restricts the ability of th Revenue Service to disclose personal information obtained in connection with its review of individual tax returns. 26 U.S.C. § 6103. Cong enacted protections for individual bank records (Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401) and for personal information in credit reports (Fair Credit Reporting Act, 15 U.S.C. § 1681). Federal statutes have also created privacy rights with respect to student rec (Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g), electronic mail and voicemail communications (Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510), video rental records (Video Privacy Protection Act of 1988, 18 U.S.C. § 2710), television subscriber information (Cable Communications Policy Act of 1984, 47 U.S.C. § 521), and customer information held by telecommunications carriers (Telecommunications Act of 1996, Pub.L. No. 104-104, 110 Stat. 56). Federal legal protections are complen state law and by self-regulatory efforts such as those described elsewhere in this report.

21. Westin 39-40; Consumer Alert Comment at 1-2 (Doc. No. 13); CEI Comment at 1-2 (Doc. No. 31).

22. Westin 39.

23. Westin 39-40.

24. Westin, A. F., "Interpretive Essay," in 1994 Harris Survey at xxv-xxvii (Doc. No. 11).

25. 1994 Harris Survey at 93-94 (Doc. No. 11).

26. Id. at 96, 108-19; Westin, "Interpretive Essay," supra n. 27, at xxvi-xxvii.

27. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health, Education and Welfare, I Computers and the Rights of Citizens (July 1973) (recommending legislation establishing a federal Code of Fair Information Practice for "automated personal data systems").

28. U.S. Govt. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Inf Infrastructure: Principles for Providing and Using Personal Information (1995); National Telecommunications and Information Administrat Dept. of Commerce, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (1995).

29. Rotenberg 137-38; Smith 43-44. See Givens Comment at 3 (Doc. No. 9).

30. See, e.g., Westin 144 (discussing the banking industry).

31. Strenio 255-56.

32. Id; Weitzner 115.

33. Jaffe at 102-03.

34. See, e.g. IIA Fair Information Practices Guidelines (1994) (Doc. No. 23, Attachment); CASIE Goals for Privacy in Marketing on Intera Media (1996) (Doc. No. 18); ISA Guidelines for Online Services: The Renting of Subscriber Mailing Lists (1995) (Doc. No. 15, Attachmer

35. See e.g., Golodner 60; CDT Comment at 2 (not paginated) (Doc. No. 22); DMA and ISA proposed Joint Statement on Online Notice Opt-Out (1996) (Doc. No. 4); ISA Guidelines for Online Services: The Renting of Subscriber Mailing Lists (1995) (Doc. No. 15, Attachme Goals for Privacy in Marketing on Interactive Media (1996) (Doc. No. 18); IIA Fair Information Practices Guidelines (1994) (Doc. No. 23,

Attachment); DMA Guidelines for Personal Information Protection (1995) (Doc. No. 24, Attachment B).

36. The substance of the notice varies, however. The IIA Fair Information Practices Guidelines state that members should establish a fai information practices policy and make it publicly available. Doc. No. 23, Attachment at ¶ 1. Nynex Corporation provides its customers a " Statement" detailing its information practices. Nynex Comment at 2 ¶ 2.(Doc. No. 8). The IIA Guidelines also provide for disclosure of int uses of personal information, when the information is obtained directly from an individual. Doc. No. 23, Attachment at ¶ 3. The DMA Gui Personal Information Protection state that individuals who provide personal information to marketers should be given notice of the poten sale, or exchange of their personal information to third parties. Doc. No. 24, Attachment B at Art. 5. The ISA Guidelines for Online Servic Renting of Subscriber Mailing Lists provide that subscribers are to be "clearly and actively notified" of a member service's subscriber list practices "proximate to sign-up." Doc. No. 15, Attachment at ¶ A.

CASIE's Goals for Privacy in Marketing on Interactive Media state that marketers seeking information through interactive media should r consumers of potential transfers of the information to third parties. Doc. No. 18 at ¶ 4. The DMA and ISA proposed Joint Statement on C Notice and Opt-Out provides that online marketers should make their information practices available online in a manner that is "easy to f to read, and easy to understand." Doc. No. 4. ISA noted that this can easily be accomplished online. The ISA has posted such a notice c page, as has the DMA. ISA Comment (Doc. No. 15 at 4); DMA Comment, Appendix C (Doc. No. 6). Users can click on an icon to read h Web site handles the browsing information transmitted to it. ISA Comment at 4 (Doc. No. 15).

37. CDT Comment at 2 (Doc. No. 22); DMA and ISA proposed Joint Statement on Online Notice and Opt-Out (Doc. No. 4); IIA Fair Infor Practices Guidelines (Doc. No. 23, Attachment).

38. Sherman 28 (referring to unsolicited e-mail); DMA Guidelines for Personal Information Protection Art. 5 (Doc. No. 24, Attachment B); ISA proposed Joint Statement on Online Notice and Opt-Out (Doc. No. 4); CASIE Goals for Privacy in Marketing on Interactive Media at No. 18); ISA Guidelines for Online Services: The Renting of Subscriber Mailing Lists ¶ B (Doc. No. 15, Attachment). The IIA's Fair Inforr Practices Guidelines do not specify the timing of notice and consumer choice. Doc. No. 23, Attachment at ¶ 3. See also Nynex Privacy F at 3 (providing for customer "opt out") (Doc. No. 8); Consumer Alert Comment at 3 (not paginated) (Doc. No. 13).

39. America Online Comment, Attachment at 12 (Doc. No. 17); CompuServe Comment, Attachment A at 8 (not paginated) (Doc. No. 25)

40. Doc. No. 4. The ISA's Guidelines for Online Services: The Renting of Subscriber Mailing Lists do not specify the mechanism membe provide to subscribers for removing their names from mailing lists. Members may devise any scheme so long as the process is "easy an publicized." ISA Comment, Attachment at ¶ B (Doc. No. 15).

41. Doc. No. 3. The proposed Principles provide several strategies for addressing the problem of unsolicited commercial e-mail. They pr commercial solicitations be identified as such and disclose the marketer's identity. Id. at ¶ 2. They provide that recipients of these solicita have no prior relationship with the marketer should be told of a mechanism through which they can instruct the marketer to send no othe solicitations. Id. They also propose that marketers having an established relationship with online customers should provide them a notice opt-out mechanism to prevent the use of their e-mail addresses in marketing lists sold, rented or exchanged for online solicitation purpos

42. Hendricks 31; Goodman Comment at 1 (Doc. No. 26).

43. Goodman Comment at 1 (Doc. No. 26). Consumers' views on the "opt-in" vs. "opt-out" debate are not well understood. Professor Ala is planning a study that would investigate consumers' preferences in this regard. Westin 41. In a recent survey of consumer views on dir marketing generally, eighty-three percent of respondents stated that they favored legislation requiring an "opt-in" regime for including nar mailing lists used for marketing. Negus, B., "You're Not Welcome," Direct 1 (June 15, 1996).

44. Goldman 14-15; CDT Comment at 15-23 (Doc. No. 5); CDT Comment at 4 (Doc. No. 22). See also Resnick Comment at 9-10 (Doc.

45. See Rotenberg 24; Krumholtz 38; Jaffe 105; Wellbery 205.

46. IIA Comment, Attachment at ¶¶ 4-5 (Doc No. 23); DMA Comment, Attachment B at Arts. 3-4 (Doc. No. 24); CASIE Goals at ¶ 5 (Doc

47. CDT Comment at 2-3 (Doc. No. 22); Rotenberg 159-60. See also Smith 164 (calling for screening mechanisms to ensure the accura personal information prior to its transmittal via the Internet).

48. See e.g., CDT Comment at 3 (not paginated) (Doc. No. 22). For example, the IIA's Guidelines call for "reasonable and appropriate st protect personal information from loss, destruction, or unauthorized use. IIA Comment, Attachment at ¶ 2 (Doc. No. 23). DMA's Guidelin Personal Information Protection include a similar provision. Doc. No. 24, Attachment B at Arts.7-8. ISA's Guidelines for Online Services: Renting of Subscriber Mailing Lists provide that members should take appropriate action where they identify misuses of personal informa third parties to whom they have transferred personal information. ISA Comment, Attachment at ¶ C (2)-(3) (Doc. No. 15).

49. IIA Comment, Attachment at ¶ 2 (Doc. No. 23); DMA Comment, Attachment B (Guidelines for Personal Information Protection) at Art (Doc. No. 24)

50. IIA Comment, Attachment at ¶ 2 (Doc. No. 23).

51. Westin 143 (discussing the consistent findings of survey research on this question).

52. Id.

53. Westin 144; Bushey 151.

54. Frawley 165; Hendricks 171; Strenio 177-78; Westin 146-47.

55. Frawley 165.

56. Id; Strenio 177-78.

57. Westin 146-47.

58. Frawley 166.

59. Frawley at 166-67; Westin 147. For example, a user might participate in a chat room for AIDS or breast cancer patients. As chat roo essentially public places, the user's e-mail address could be obtained and archived, as could the content of the user's posted comments Westin 147.

One panelist argued that medical information should not be transmitted at all on the Internet, because it is an insecure medium. Goldma some panelists' view, legislation is needed in this area to fully protect individuals. Frawley 167; Goldman 174-75. One panelist argued th personal information should be offered for sale to third parties on the Internet. Smith 164.

60. Sherman 160-161; DMA Comment (Doc. No. 24), Attachment B (DMA Guidelines for Ethical Business Practice (1995) at 24). DMA's Guidelines for Ethical Business Practice provide that consumers who voluntarily give medical information to marketers should be notifiec potential uses of the information (such as transfer to third parties) at the time they provide the information and that they should be given opportunity to opt out of such uses. Id.

61. Sherman 170; DMA Comment (Doc. No. 24), Attachment B (DMA Guidelines for Ethical Business Practice at 23). According to DMA representative, financial information such as a credit account number should be used only to complete a given transaction, absent the cc knowledge and consent to transfer it to third parties. Sherman 170.

62. Sherman 169-70; Daguio 171-73.

63. Sherman 169-70.

64. Daguio 173.

65. Daguio 172. According to this Workshop panelist, privacy of financial information is an especially complex issue in an environment w neither the consumer, the merchant, nor the financial institution has absolute rights to individual financial information. Daguio 173.

66. Westin 145-47; Bushey 151; Sherman 161; Merold 169; Hendricks 170; Daguio 172; Strenio 177.

67. See Rotenberg 159-60.

68. A Smart Card is a stored value card bearing an implanted microprocessor. It permits its owner to enter into transactions anonymousl transmit encrypted information via the Internet. Koehler 154-55.

69. Westin 145; Koehler 155; Rotenberg 180. One Workshop panelist suggested that his company's practice of stripping identifying infor from individuals' medical prescription information compiled for marketing and research purposes is a solution transferrable to the online Merold 168.

[BACK][NEXT]

Last Modified: Monday, June 25, 2007