Staff Workshop Report:
Technologies for Protecting Personal Information[1]

In May and June 2003, the Federal Trade Commission convened a two-part workshop to examine the current and potential role of technology in protecting consumer information.[2] Titled "Technologies for Protecting Personal Information: The Consumer and Business Experiences," the workshop examined how technology is used to manage and secure personal information, and explored such topics as:

- consumer and business behavior regarding privacy-enhancing technologies;
- P3P and other automated privacy protections;
- the development and use of identity management systems; and
- benchmarks and standards for improving privacy processes across organizations.

Many panelists agreed that the current challenges with respect to protecting personal information could best be addressed by considering four critical elements: (1) people; (2) policy; (3) process; and (4) technology. The panel presentations and discussions illustrated how each of these elements plays a role in privacy problems and solutions, and how neglecting any one element could limit the effectiveness of a privacy program.

The Challenges Faced

Workshop participants included industry leaders, technologists, researchers on human behavior, and representatives from consumer and privacy groups. The panelists identified a range of challenges facing consumers, industry, and policy makers. For example, many consumers do not buy the privacy tools now on the market because they are often available only as expensive, hard-to-use system add-ons. Further, many consumers are largely u

[1] This report was prepared by James Silver, Toby Levin, and Loretta Garrison of the Division of Financial Practices, Bureau of Consumer Protection, Federal Trade Commission.

[2] The workshop agenda and transcripts are available at www.ftc.gov/bcp/workshops/technology. A previous Commission workshop addressed the topic of spam and related technologies (www.ftc.gov/bcp/workshops/spam/index.html), and future workshops will address spyware (www.ftc.gov/bcp/workshops/spyware/index.htm) and radio frequency identification, or RFID (planned for June 2004).

software and operating systems without properly updating them. Panelists stated that these problems are best addressed through educational campaigns, similar to the campaigns launched to increase seatbelt use or discourage smoking. Such campaigns can take years to produce changes in consumer behavior, but can help consumers play a more effective role in protecting themselves and society as a whole. Many panelists agreed, however, that further study is needed to identify the best vehicles for educating consumers and creating a culture of security.

In addition, some panelists criticized the rapid introduction of technology, hardware, and software without adequate testing and quality assurance. They also noted the general trend toward poor accountability and limited IT training budgets for the protection of consumer information. Some urged technology vendors to make security support and updates easier and more automatic, e

could be forgotten after purchasing certain technology.

Panelists cited examples of recent initiatives designed to apply these principles. For example, Microsoft has a new policy of making its products secure "by design," "by default," and "in deployment." The policy includes measures to reduce security flaws in code, ship products in a more secure configuration, add new security features to products, and provide better security support, such as patching and warnings, to already-deployed products. Similarly, Dell Computer has incorporated security standards into its desktop systems installed with Windows 2000, thus integrating protections into the system and enabling consumers to protect themselves more easily.

Automated Privacy Protections

One of the panels addressed privacy-enhancing technologies that notify consumers of privacy policies in an automated and seamless manner. Panelists discussed P3P, a computer language designed to enable a consumer's PC to read privacy policies automatically and match them against the consumer's privacy preferences. Although P3P implementation received a boost when Microsoft enabled its Internet Explorer Version 6 to interface with P3P, participants agreed that adoption of P3P by consumers and industry has still been very slow.

One major obstacle has been the scarcity of consumer products incorporating P3P. In contrast, software companies are beginning to incorporate P3P and similar standards into business technologies. One such technology is IBM's new EPAL language, which is related to P3P, but adds the possibility of automated privacy policy enforcement. Businesses that write privacy policies in EPAL can convert their privacy policies into rule-based data handling practices that can be enforced automatically across their systems, and communicated to Web site customers via P3P. EPAL has been submitted to the World Wide Web Consortium for consideration as a new standard language that would be available for public use.

negligence actions include claims that hasty software development has led to flawed software design.

In addition, recently-enacted laws – the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) – apply security requirements to entities that maintain financial and health information, respectively. Federal agencies are implementing these laws through rules and guidelines that allow flexibility, depending on the needs of particular businesses. Although flexible, these rules and guidelines contain requirements that depend on the effective deployment of technology – for example, requiring appropriate security for a network and proper encryption – and are likely to influence the market for technological products and services.

Conclusion

Workshop panelists agreed that technology alone cannot solve all of our privacy challenges, but that it can be an important part of a privacy program that also involves the effective use of people, policies, and processes. Since the workshop, there have been a number of new developments that apply this principle. For example, the Department of Homeland Security successfully deployed its new National Cyber Alert System, designed for consumers and businesses, to warn of a new variation of the MyDoom virus only hours after the system came online. The system uses email and the Web to notify business and consumers quickly of urgent information security threats, and also provides information on effective security policy and processes. Also, the Department of Energy recently negotiated a five-year, five-million dollar contract with Oracle and Opsware that requires its database software to be configured in compliance with the CIS standards. Outside observers hailed the contract as a breakthrough in government computer security, and the Energy Department expects to significantly reduce system administration costs, and increase security, through centralized update, configuration, and deployment processes.

In addition, many companies have recognized that consumer privacy tools must be useful and accessible to typical users. Some have recently announced the integration of various security features in their software. Microsoft is reportedly developing a two-factor authentication system to replace passwords, which have been criticized as difficult for consumers to remember or easy for unauthorized users to guess.

Each of these developments involves new technology, but also people, policies, and processes working together to ensure that the technology is used effectively to further information protection. The Federal Trade Commission will continue to monitor developments such as these, and to consider the role that technology plays in protecting consumer information.