

MAIN MENU:

[CALENDAR](#)[SYLLABUS](#)[DISCUSSION](#)[ADMINISTRATION](#)

NOTICES:

Online Privacy III: Individual Regulation: Technology and the Marketplace

READINGS

Here, we'll consider two more models that might offer solutions to the problems of online privacy. These models differ from the "collective" models in the sense that they are focused on giving the individual participant in eCommerce some additional tools (whether technological or legal) to use in determining the scope of privacy protections. In particular, these models are:

1. *Technological Regulation*: The use of new technological tools to define privacy rights.
2. *Market-based Regulation*: If personal information was understood to be commodified, might that allow users to better delineate privacy protections.

Overview

Margaret Jane Radin, John Rothchild and Gregory M. Silverman, *Internet Commerce: Doing Business in a Networked World* (2001). [excerpts from Chapter 10] [pdf, 32 kb]

The Technology of Privacy

EPIC, & JunkBusters, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy*, June 2000

ZeroKnowledge, *How Freedom Privacy Software Works* (2000)

Juliana Gruenwald, *Hardwiring Privacy*, Interactive Week, April 30, 2001 11:58 AM PT

Marketplace Responses to Privacy Concerns

Jared Sandberg, *The Privacy Officer*, Wall St. Jrnl., July 16, 2001. [pdf, 68 kb]

Microsoft Passport

Microsoft, Microsoft Passport: Streamlining Commerce and Communication on the Web, October 11, 1999

Microsoft, Passport Fact Sheet (2001).

Farhad Manjoo, *MS Passport: Straight to the FTC*, Wired News, Aug. 16, 2001

Wayne Rash, *Your stolen Passport*, Enterprise, September 26, 2001 9:37 AM PT

Liberty Alliance, *Industry Leaders to Form Network Identity Alliance*, Sept. 26, 2001.

COPYRIGHT © 2001 R. POLK WAGNER.

INTERNET COMMERCE: DOING BUSINESS IN A NETWORKED WORLD

MARGARET JANE RADIN, JOHN ROTHCHILD AND GREGORY M. SILVERMAN

© 2000, 2001 by Margaret Jane Radin, John Rothchild and Gregory M. Silverman

**Chapter Ten
Privacy Online**

[* * *]

D. Models for Protecting Online Privacy

Nearly everybody agrees that Internet users have legitimate privacy interests. There is much less agreement about the proper approach to protecting those interests, in view of the competing interests with which privacy protection can interfere. Several different models of online privacy protection have been implemented or proposed. Most observers agree that none of these approaches is by itself sufficient, and advocate some combination. To understand their strengths and weaknesses, it will be useful to consider the approaches individually.

[* * *]

3. Model III: Empowerment of individuals through technological tools

Another market-based approach to protecting online privacy is to make available to Internet users technological tools that they can use to protect themselves.

U.S. Senate Judiciary Committee, Know the Rules, Use the Tools—Privacy in the Digital Age: A Resource for Internet Users 10-21 (undated; Oct. 2000)

In the dynamic arena of Internet technology, a wide variety of exciting technological solutions exist to safeguard personally identifiable information and new ones are continually being developed. This Report's discussion of the available technologies is not intended to be a comprehensive one, but rather is intended to give consumers a sampling of the tools currently available to consumers that help empower them to safeguard their privacy to the extent they wish. The Committee's decision to describe particular technologies should not be interpreted as an endorsement of any technology.

The product and service descriptions listed below are short summaries based upon information received from the respective organizations, for the purpose of providing consumers with a starting point for learning about some of the technology options available to them. They

are not intended to replace independent consumer inquiry into full and complete product and service information, and they do not constitute an endorsement or recommendation of any kind.

The Committee invites the public and technology companies to forward additional privacy technology tools that might be helpful to Internet users to the Committee via e-mail or written correspondence. We will take the efforts to update this technology resource periodically with new technologies.

1. Ways of Handling Cookies.

Again, “cookies” are electronic tags that are placed on the hard drive of a user’s computer by websites he or she visits. . . . Currently available to users are a number of options to: (1) alert them as to when a cookie is placed on their hard drive, (2) block the placement of a cookie altogether, or (3) remove cookies from the user’s hard drive. A few of these options are described below:

a. Internet Browser Settings.

New technology permits Internet users to see when a cookie is about to be planted on their system and make an informed choice about whether to accept it or reject it. With current versions of leading browsers such as Netscape Navigator and Internet Explorer, a user can select to have an alert box flash on the screen to inform them whenever a server is trying to place a cookie on their system. Some sites, however, send cookies for every object the user clicks on the page, requiring the user to reject cookies dozens of times for a single web page.

b. Manual Deletion Of Cookies Using Browser Files.

Internet users can locate and delete cookies that already have been placed on their computer by websites. In Netscape Navigator, the cookies are stored in a single file called “cookies.txt.” This file generally is in the directory the user previously designated for Netscape to use for storing user profiles. To delete all cookies, find the “cookies.txt” file, highlight it, and delete it. To delete a specific cookie, open the file “cookies.txt” with an editor or word processor, and delete the line corresponding to the cookie you wish to delete.

For Internet Explorer, find the directory called “Cookies.” To delete all cookies, delete all the files in the directory. To delete a specific cookie, find the file in the directory corresponding to the cookie and delete that file.

c. Cookie-Cutters.

Various technology-based tools exist for coping with unwanted cookies. . . .

i. Netscape Cookie Manager.

Developed by America Online, Netscape Cookie Manager, a feature of the new Netscape browser, allows users to view, block, and delete cookies based on their individual privacy

preferences. For example, Cookie Manager permits a user to determine who may and who may not set cookies on his or her computer, edit and delete any of the cookies placed, and review a list and description of all of the cookies placed on the user's computer.

Other privacy technology developed by America Online includes AOL Parental Controls and AOL Instant Messenger. AOL Parental Controls permits parents to determine who their children may or may not communicate with when they use AOL by initiating specific privacy settings. AOL Instant Messenger allows a user to control his or her own privacy by limiting who is permitted to know when the user is online and who is permitted to make contact with the user.

ii. Privacy Companion.

Developed by Iddide, Inc., Privacy Companion is a browser software application that is intended to enable users to detect and block third party cookies, while allowing them to benefit from personalized services from the websites that they are visiting. Privacy Companion automatically detects and blocks cookies from third party advertisers and profiling companies which can be used to track a user's browsing behavior as he or she moves from website to website. It also provides statistics on sites which may have tracked a user's browsing behavior.

iii. NSClean Privacy Software.

NSClean Privacy Software provides products that permit the end-user to turn off the cookie warnings, accept cookies while online, and then remove them from their hard drive. "Owing to the need for legitimate cookies to be kept for the convenience of users for legitimate sites," the new NSClean products permit users control over cookies, enabling them to select which cookies they find useful and desire to keep and remove all other cookies automatically at their option.

iv. AdSubtract.

AdSubtract offers filtering to eliminate unwanted advertisements, animated images, cookies, pop-up windows, background music, and the like. By eliminating unwanted pages, AdSubtract speeds up web page download time. The downloadable software provides the user with statistics showing items filtered.

v. Cookie Jar 2.0.

Cookie Jar 2.0 software allows users control over which sites can send cookies to the user's computer. Using the Internet browsers, the user sets up a configured file allowing only specified sites to send cookies. Sites which have not been selected by the user are silently discarded. This technology also offers the ability to stop browsers from sending revealing information to web servers, and to block connections to certain sites.

vi. Cookie Cruncher.

Like Cookie Jar, Cookie Cruncher works with the user's Internet browser to give the user control over the cookies that are accepted by and eventually stored on a system. Cookie Cruncher blocks cookies before they are placed on the user's hard drive by automatically and transparently accepting or rejecting cookies from specified servers without user interaction once the user has specified preferences. In addition, Cookie Cruncher informs the user of the cookie's specific purpose, such as advertisement tracking, online shopping or site tracking. It also can compile a list of all the cookies that have been accepted or rejected during the course of an online session, and gives the user the option to save the list for later use.

vii. Internet Junkbuster Proxy.

Internet Junkbuster Proxy is free software tool that gets rid of banner ads and cookies while individuals surf the Internet. The software only accepts cookies from sites which the user pre-selects. The software also prevents the disclosure of other personal details, such as information about the page clicked on and the user's computer software and hardware configuration. Users have the option to block whole sites or block ads. Junkbuster's features can be optionally disabled or altered.

viii. WebWasher for Windows and Macintosh.

WebWasher filters the HTML data stream to automatically block ads, animation, java script and cookies. The program comes configured to automatically block "bad" cookies that leak personal information while automatically accepting "good" cookies required for efficient online shopping and quick page views. From its "traffic cop" position in the data stream, WebWasher filters both incoming cookies from website servers and outgoing cookies from the user's browser. WebWasher can be installed on an individual computer or run as a proxy-server for an entire office network.

2. Identity Scrubbers.

Various user information is instantly available to websites when users visit them. Identity scrubbers are tools developed to allow users of the Internet to remain anonymous while surfing the Internet. While a number of companies offer different options for consumer, the following is a sampling of identity scrubbing tools that are available.

a. PrivadaControl.

Privada is a digital privacy service created for Network Service Providers. PrivadaControl, operated on a user's personal computer, permits the user to browse the Internet anonymously and to send and receive emails anonymously. While using PrivadaControl during Internet use, a user's webpage requests are encrypted and sent to the Privada Network. The Privada Network then retrieves the webpage and returns it to the user. Additionally, PrivadaControl allows users to manage the placement of cookies, which are assigned to the user's individual profile on the Privada Network rather than on the user's computer. As a result, the user may take advantage of the benefits of customized browsing without privacy concerns. Users may disable PrivadaControl's privacy protections in order to share personal information

with those websites they choose. PrivadaControl also allows a user to send and receive email anonymously by permitting the user to create a separate identity and to establish an anonymous email account with that identity on the Privada Network. A user may then send and receive email from this account without disclosing his or her personal identity. E-mail messages sent by the user to the Privada Network are encrypted, and the user may choose to have the Privada Network assign his or her sent messages a random delay of 30 minutes to four hours.

b. Incogno SafeZone.

Developed by Incogno Corporation, Incogno SafeZone is a patent-pending technology that enables Internet merchants to offer anonymous checkout services to privacy-sensitive buyers. Using Incogno SafeZone, customers buy directly from the merchant's site and receive product shipments without revealing their names, addresses, email addresses, or credit card information to the merchant. Additionally, because the merchant does not receive, store, or transmit the customer's credit card information in unencrypted form, the risk of credit card fraud is reduced. In using Incogno SafeZone, a merchant can request that customers disclose their personal information, but any such disclosure is fully voluntary. Incogno SafeZone currently is in the market trial stage.

c. Freedom.

Developed by Zero-Knowledge Systems, Inc., Freedom works in conjunction with the Freedom Network, which is a series of globally distributed, independently hosted servers. Freedom is intended to ensure a user's online privacy and security by encrypting all email and browsing communications. Users of Freedom manage their online activities with the help of pseudonyms or "nyms." Each nym has its own email address and "cookie jar," thus each nym can build its own pseudonymous reputation capital—allowing users to take advantage of targeted on-line marketing material when desired. According to Zero-Knowledge, Freedom is created in such a way that no one, not even Zero-Knowledge, can trace a nym to its actual owner.

d. Anonymizer.com.

Recognizing that each time an Internet user enters a website, he or she could provide certain personal information, including viewing habits, geographical location, addresses, e-mail and credit card numbers, Anonymizer.com enables users to visit sites while concealing their identity. Anonymizer protects consumer privacy by acting as an intermediary between the user and a particular website. The following are a few of the services offered by Anonymizer.com:

- "Anonymizer Surfing" offers a free and nominal-fee based system that allows users to browse the web through using an intermediary to prevent unauthorized parties from gathering personal information. The system is web-based and does not require software or upgrades.
- Anonymizer Window Washing is a fee-based program that automatically cleans up the user's browser, cache, cookies and other online history.
- Anonymizer Pipeline protects the user's Internet activity with encryption between consumers and the Anonymizer network. It enables customers to use e-mail, news, and the web anonymously from their personal computer. The Internet service provider, and anyone between

the individual and the Anonymizer network, sees only scrambled data, with all activity appearing to come from the Anonymizer subnetwork located in California.

e. Crowds.

Developed by AT&T Research, Crowds allows users to blend into a virtual crowd on the Internet by hiding an individual's actions within the actions of many users. Users are placed into a large and geographically diverse group, or "crowd," which collectively issues requests on behalf of its members. The end server is unable to identify the initiator of the request because the initiator is indistinguishable from any of the other "crowd" members.

3. Privacy Preference Technology.

Privacy preference technology allows the user to select his or her own privacy preferences, to modify those preferences, and to compare how particular websites' privacy policies match his or her own preferences.

a. AT&T Research.

AT&T Research, in conjunction with Microsoft Corporation, is developing browser software technology to be used with Microsoft's Internet Explorer. When installed by the user, this technology will add a privacy button to the top of his or her browser window. By clicking on this button, a user will be able to set his or her privacy preferences, check how well a website's privacy policy matches the user's preferences, and view a site's actual privacy policy. AT&T's technology currently is in the development stages.

b. PrivacyRight.

PrivacyRight's Unified Customer Permissions platform (UCP) is a server-side privacy solution which may be accessed by consumers at any point during their visit to a website, and with which they may set privacy preferences governing the use of their personal information. The UCP platform allows the interpretation and enforcement of persistent rules assigned to personal information and facilitates consumer-approved data exchanges between applications within an organization and from business-to-business.

Platform for Privacy Preferences (P3P)

The Platform for Privacy Preferences ("P3P") is another technological approach to empowering Internet users to retain control of their personal information. P3P, which was developed by the World Wide Web Consortium, is a protocol that allows a website to describe its privacy policy in a standardized format. When an Internet user accesses a P3P-compliant website, the server automatically communicates the website's privacy policy to the user's browser. The browser is configured with the user's privacy preferences. For example, if you are unwilling to have your personal information shared with any third party, you can indicate that preference in your browser settings. When you access a website, your browser compares the

site's policies with your own preferences. If the site meets your privacy requirements, the browser accesses the website. If not, the browser may alert you of the mismatch, and allow you to decide whether to bypass the site.¹

There are several important tasks relating to online privacy that P3P does not undertake. As the W3C explains: "P3P does not set minimum standards for privacy, nor can it monitor whether sites adhere to their own stated procedures. Addressing all of the complicated, fundamental issues surrounding privacy on the Web will require the appropriate combination of technology, a legal framework and self-regulatory practices." World Wide Web Consortium, "P3P 1.0: A New Standard in Online Privacy," www.w3.org/P3P/brochure.html.

P3P has drawn sharply mixed reviews. Detractors note that website operators will have little incentive to take the trouble implement P3P. Given the complexity of configuring a browser with one's privacy preferences, most users will leave their browsers in their default configurations, which will likely not be highly protective of privacy, since that would result in denying access to a large number of popular websites. Even users who want strong privacy protection will probably leave their browsers configured to a low level of protection, since otherwise there will be few sites they can visit. As a result, P3P will not create any meaningful incentives for websites to implement fair information practices. Internet users will get only the illusion, but not the reality, of sovereignty in the marketplace for privacy. Furthermore, no mechanism currently exists for enforcement of privacy promises embedded in P3P code. For a critique of P3P, see Electronic Privacy Information Center, "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy" (2000), www.epic.org/reports/pretypoorprivacy.html.

Notes

1. *Costs of self-empowerment.* The use of privacy control technologies entails significant costs for Internet users. A user must invest a substantial amount of time and effort to research the various tools, select the one she thinks will best suit her purposes, install it, and learn how to use it. There are likely to be significant segments of the online population that lack the skills necessary to make use of these tools: an August 2000 study found that 56 percent of web users did not know what a cookie is.² Adding a new piece of software to one's computer always carries the risk that it will be buggy or incompatible with other software on the system, costing more time and effort. Some of these tools significantly degrade a user's experience in accessing the Web, by slowing down communications or by adding additional procedures that must be followed when accessing a new website. Some of them are free, but others carry a purchase price or subscription fee. How much burden is it appropriate for Internet users to shoulder to protect themselves from invasions of their privacy?

¹ P3P does not define how a browser responds in case of a mismatch: it is only a language that allows the website to communicate with a browser. It is up to the browser developer to determine how the browser will communicate to the user the result of its comparison of the website privacy policy with the user's preferences.

² Pew Internet & American Life Project, [*].

2. *Does individual empowerment obviate regulation?* Should the availability of tools like these lead legislators and regulators to the conclusion that government intervention to protect privacy online is unnecessary? How would you distinguish this argument from: “Door locks, window bars, burglar alarms, and private guard services are widely available. Heavy-handed government intervention in the form of criminalization of burglary is therefore unnecessary. We should instead devote more resources to educating householders to make use of these tools and protect themselves.”

3. *Will tools emerge without law?* Lawrence Lessig argues that technology enabling automated negotiations over privacy between a website and a prospective site visitor, like P3P, will not emerge unless the law mandates it, since “[t]he power of commerce is not behind any such change.” LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 163 (1999). Do you agree? Are the imperatives of commerce necessarily opposed to implementation of fair information practices?

5. Model V: Commodification of privacy?

Kenneth C. Laudon, Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information, in U.S. DEP’T OF COMMERCE, PRIVACY AND SELF REGULATION IN THE INFORMATION AGE 41, 41-42 (1997)

The theory of markets and privacy begins with the understanding that the current crisis in the privacy of personal information is a result of market failure and not “technological progress” alone. The market failure has occurred because of a poor social choice in the allocation of property rights. Under current law, the ownership right to personal information is given to the collector of that information, and not to the individual to whom the information refers. Individuals have no property rights in their own personal information. As a result, they cannot participate in the flourishing market for personal information, i.e., they receive no compensation for the uses of their personal information. As a further consequence, the price of personal information is so low that information-intensive industries become inefficient in its use. The price is low because the price of personal information does not reflect the true social costs of coping with personal information. The market is dominated by privacy-invading institutions. And as a further result, there is a disturbing growth in privacy invasion, an excessive and abusive disregard for the interests of many in keeping elements of their life private, or at least under their control.

* * *

An earlier paper attempted to lay the legal and economic foundation for a true marketplace for personal information [Laudon, 1996]. In this marketplace, individuals would retain the ownership in their personal information and have the right, but not the obligation, to sell this information either to institutional users directly, or more likely, to information intermediaries who would aggregate the information into useful tranches (e.g. blocks of one thousand individuals with known demographic characteristics) and sell these information baskets on a National Information Exchange.

Individual ownership of personal information can be anchored within British and American common law. The common law tort of appropriation protects the right of celebrities to own their images, likenesses, voices, and other elements of their persona. To appropriate personal images of celebrities for commercial purposes without consent or payment is recognized by the courts as an appropriation. Likewise, it is conceivable that courts and juries could be convinced to protect the personal “data images” of ordinary citizens. These data images have somewhat less resolution than a photographic image, but they are increasingly and profoundly descriptive and predictive of human behavior. As computers extend their powers, these data images will approach photographic resolutions.

The economic foundation for individual ownership of personal information can be found in the theory of markets (and related theories of governance) and the theory of externalities. Markets are likely the most efficient mechanisms for allocating scarce resources. Governments should intervene in markets only if markets fail. Markets do fail under conditions of monopoly, asymmetries in power and information, and in the case of public goods, e.g., clean air. Governments should either seek to restore markets or regulate the activity. In the case of personal information, the market has failed because of asymmetries in power and information brought about by poor social choice in the allocation of property rights to information. The price of personal information is far too low, and therefore its abuse in the form of privacy invasion is far too cost beneficial to those institutions that dominate the market. The function of government here should be to restore the power of one class of participants in the market, namely individuals, by vesting ownership of personal information in the individual. A second function of government is to ensure the orderly functioning of a personal information marketplace.

The failure of the marketplace results in significant negative externalities for individuals. These externalities are experienced as excessive indirect and direct costs involved in “coping” with information. Coping costs include tangible costs like excessively large mail handling facilities (public and private), and loss of attention, as well as intangible costs like loss of serenity, privacy, and solitude. These negative externalities must be balanced against the positive externalities of nearly unlimited exploitation of personal information which results in enormous amounts of marketing information being delivered to consumers (whether they want it or not). However, it can no longer be argued that these positive externalities fully compensate individuals or society for the negative costs of unlimited exploitation of personal information.

* * *

Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1300-01 (2000)

Imagine the commercial world wide web in a world that treats personal data as alienable personal property. If personal data are alienable, then by ordering that free computer, downloading that free MP3 recording of a hit song, downloading and installing that software, you will surely have consummated the transfer. We could make a rule that the terms of such a transfer must be disclosed as part of the inevitable click-through license, and just as surely, they would be, and everyone would click “I accept” without even reading them. Indeed, arguably, for

any website for which access requires clicking an “I accept” box, the fact that you, for instance, read the *New York Times* on the Web at a considerable savings over the newsstand rate will support the claim of transfer.

It’s no better out here in meatspace. Imagine that a person, and let’s for the sake of convenience and brevity call her “I,” has initial ownership of information about herself, that is, me. I sign up for a check cashing card at the supermarket, or a shopper’s club discount card, and, in return for the convenience of paying by check or a steady stream of small discounts on products I may or may not buy, I waive, forfeit, or assign any ownership rights I might have in whatever information resides in an ongoing record of my purchases.

The store, meanwhile, has its own proprietary interest in the compiled purchasing records of each and all of its customers, and will rely on that interest to sell facts about me to whomever. Whomever, of course, has a property interest in those facts because it paid for them, and will be able to combine them with facts about other people and more facts about me from other sources. Whomever may use that collection of data to make up a list of people who are ripe for Discover Card[®] solicitations, or who might be interested in a mail order catalog for folks suffering from depression, or who, based on recent medical and pharmaceutical purchases, might be eager to purchase some no-questions-asked life insurance.

What makes the whole situation worse is that privacy is one of those things that many people don’t believe they really need until they find themselves with something to keep secret. If easy assignment is the rule, they may no longer have the power to preserve their secrecy; even if they could, the exceptional nature of their asserting a privacy claim will tip off those from whom this is a secret that there is an interesting secret there. So, if someone who is deemed to have waived any property rights in the information supplied to businesses in return for product discounts should suddenly find himself diagnosed with hemorrhoids, or herpes, or HIV, he may have no practical way to recapture his secrecy.

Now, imagine the world we have made. We each owned our own personal data initially, but we’ve assigned them for value to some business, which has sold them to some other business, which combines them with other data to generate a profile of each of us, and sells or rents that profile out. Nor is it unrealistic to imagine those businesses asserting their property interest in their collections of data: There is a lot of that going around. In October, the *New York Times* reported that the NIH Recombinant DNA Advisory Committee had been stymied in its efforts to require more complete disclosure of the safety problems encountered in gene therapy by pharmaceutical companies’ insistence that that information is proprietary.

The market in personal data is the problem. Market solutions based on a property rights model won’t cure it; they’ll only legitimize it.

* * *

1. *Privacy as property in the courts.* The courts have held, in several contexts, that individuals generally have no enforceable property right in their personal information. See *U.S. News & World Report, Inc. v. Avrahami*, 1996 WL 1065557 (Va. Cir. Ct. Jun. 13, 1996), reh’g denied, *Avrahami v. U.S. News & World Report, Inc.*, No. 961837 (Va. 1996) (holding that an

individual has no property right in his name, so commercial exchange of names on a mailing list does not violate state statute or common law); *Polin v. Dun & Bradstreet, Inc.*, 768 F.2d 1204 (10th Cir. 1985).

Pretty Poor Privacy:
An Assessment of P3P and Internet Privacy

June 2000

Electronic Privacy Information Center
www.epic.org

Junkbusters
www.junkbusters.com

Summary

This report examines whether P3P is an effective solution to growing public concerns about online privacy. The report surveys earlier experience with "cookie" technology and notes similarities. The report finds that P3P fails to comply with baseline standards for privacy protection. It is a complex and confusing protocol that will make it more difficult for Internet users to protect their privacy. P3P also fails to address many of the privacy problems specifically associated with the Internet. The report further finds that earlier versions of P3P were withdrawn because the developers recognized that the proposed negotiation process was too burdensome for users and that the automatic transfer of personal information would be widely opposed. It is anticipated that this version of P3P will also be significantly overhauled once it is reviewed. The report concludes that there is little evidence to support the industry claim that P3P will improve user privacy citing the widely accepted Fair Information Practices.

The report recommends the adoption of privacy standards built on Fair Information Practices and genuine Privacy Enhancing Techniques that minimize or eliminate the collection of personally identifiable information. Simple, predictable rules for the collection and use of personal information will also support consumer trust and confidence. P3P, on the other hand, is likely to undermine public confidence in Internet privacy.

Table of Contents

- **Understanding Privacy**
- **Current Internet Privacy Risks**
- **Cookies -- The Precursor to P3P**
- **What is P3P and How Does it Work?**
- **Relating Cookies to P3P**
- **Failure to Establish Privacy Standards**
- **Exclusion of Non-Compliant Sites**

- **Absence of Enforcement**
- **Prognosis for Adoption**
- **Impact on Privacy if P3P is Deployed**
- **P3P Fails to Satisfy Jurisdictions with Strong Privacy Standards**
- **Better Alternatives Exist**
- **Conclusions and Recommendations**
- **References**

Understanding Privacy

To assess a proposed technical standard for privacy protection for the Internet, it is necessary to understand the nature of privacy protection and the legal and ethical norms associated with privacy protection.

Privacy protection is widely understood as the right of individuals to control the collection, use and dissemination of their personal information that is held by others. This central principle has been adopted in U.S. law, privacy laws outside of the United States and many international agreements, including the U.S. government, the 1980 OECD (Organization for Economic Cooperation and Development) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The OECD Privacy Guidelines and privacy laws are based on a set of Fair Information Practices that describe the obligations of organizations that collect personally identifiable information and the rights of individuals who give up their personal information.

Central to the concept of privacy and the aim of Fair Information Practices are the goals of transparency and fairness. Transparency means that when organizations collect information about individuals they should make known to the individual the information that is collected and how it is used. Fairness means that information is used only for the purpose for which it is collected. If the organization wishes to use personal information for additional purposes, it is obligated to obtain the explicit permission of the individual involved. Together the principles of transparency and fairness help establish trust and confidence in commercial relations where personal information is acquired. It is widely understood that for these principles to be effective they need to apply on a widespread basis, with few if any exceptions.

Privacy protection is also understood as the ethical obligations associated with the collection and use of personal information. Doctors, lawyers, accountants, and professionals all understand the obligation to hold in trust personal information that is obtained in the provision of a service.

Central to the legal and ethical norms for privacy protection is the recognition that individuals should not be required to negotiate or choose among Fair Information Practices. Such negotiations would invariably disadvantage those who could not purchase sufficient privacy and would lead to a gradual decline in the level of protection available to the general public. Privacy protection exists where Fair Information Practices are enforced.

Current Internet Privacy Risks

To assess a proposed technical standard for privacy protection for the Internet, it is necessary also to understand the privacy problems that are unique to the Internet.

Today the Internet faces a wide range of privacy problems. The Internet Protocol (IP) used to transmit web pages creates a privacy risk that is not imposed by web browsers but in the transmission of web pages through the IP. When a browser requests a page from a server, the browser's IP address is transmitted as the return address to which the requested page is to be sent:

a kind of digital caller ID. Various services are available today to disguise one's IP address. These are true privacy-enhancing technologies, because they remove identifying information.

An example of a privacy-impacting feature is the "referrer" header that identifies the URL of the page that caused the current page to be requested. This can happen in two ways. The first is where the user clicks on a link; this allows sites to see where their visitors are coming from. The second is if a graphic is included in a page; the most important case for privacy is where a banner ad is served on a page returned by a search engine. The companies that serve banner ads use this feature to target advertising: search for "station wagon" for example, and you may get an ad for Volvo. This feature might be acceptable as providing transient information only, were it not for another feature that allows long and potentially revealing records of search queries to be assembled. That feature goes under the innocent-sounding name of "cookies."

Cookies -- The Precursor to P3P

Before cookies, HTTP was a "stateless protocol": nothing linked your request for one page on a site to subsequent requests. Netscape decided to extend the protocol to allow sites to tag your browser with information that would be available to the site when you returned. As a result, the ability of Internet users to freely navigate the Internet was diminished.

Subsequent public outcry and growing awareness of cookies has led browser manufacturers over a period of several years to slowly give users some measure of control over cookies, assuming the user is aware of them and knowledgeable enough to exercise the choices that have been provided. Still, these measures are confusing and impractical and falls far short of what privacy advocates have asked for.

In Netscape's original patent application, engineers did not intend cookies to be privacy-invasive; they anticipated that the contents of shopping carts would be kept on the shopper's PC for the duration of the visit. But since 1996 they have been almost universally used in one way: to assign a unique visitor number to the PC, and to keep all relevant information on the server side indefinitely.

A third party can also set cookies when accessing a web site. Third party banner advertisers such as DoubleClick typically do this. This permits a history of browsing behavior to be assembled, and linked to other information. These so-called third-party cookies practice are clearly privacy-invasive, and since 1997 privacy advocates have asked browser manufacturers to remove them.

In the same year a document before the Internet Engineering Task Force, RFC 2109 proposed the same change. These requests have met with resistance and inaction because by making that simple change of disallowing third-party cookies, the privacy damage being done by Internet advertisers could have been avoided. The browser makers decided the privacy of surfers was not as important as that the data-gather opportunities of their companies and their commercial partners. Rather than fix the problems with cookies, which Microsoft and Netscape could have done long ago, the companies that develop browser software are now promoting P3P which will raises even more privacy problems than cookies.

What is P3P and How Does it Work?

P3P is a protocol that requires Internet users to reveal their privacy preferences before they are allowed to access information on the Internet.

The Platform for Privacy Preferences (P3P) is a protocol developed by the World Wide Web Consortium (W3C), with funding from many private sector organizations that have opposed privacy

legislation. P3P presumes no single privacy standard, such as the OECD Privacy Guidelines, which would provide a simple, predictable, uniform environment for online transactions. Instead, P3P proposes the development of an elaborate range of privacy "choices" that require individual Internet users to make selections about the collection and use of personal data, even for online activities that would not normally require the disclosure of personal information, such as simply visiting a web site.

P3P attempts to accomplish these goals by creating a complicated and confusing language for web sites to describe their privacy policies in a machine readable format. Major elements of the protocol allow policies to describe the contact information of the legal entity making a privacy statement, whether users will have access to information collected about them, numerous categories of data being collected (physical contact information, online contact information, unique identifiers, purchase information, etc.), the purpose(s) for collection (web site administration, research and development, profiling, etc.), and what organizations will have access to collected data (primary service provider only, delivery services, unrelated third parties, etc.).

According to W3C, P3P also allows for the creation of user agents that can be configured to reflect the privacy preferences of individual end users. Once configured, a user agent would compare its preferences with the machine readable privacy statements made by various web sites. If a web site's policy matches a user's privacy preferences, access to the site will be granted. If there is a conflict, a pop-up window describing the discrepancy might notify the user, or access to the site may be blocked.

A sample P3P transaction might look something like the following. Joe Surfer configures his P3P enabled web browser to say that he does not want to disclose his home address unless he is purchasing a product that will be delivered to his home. When Joe then connects to a popular news site that requires the disclosure of his home address before he can view content on the web site, Joe's P3P-enabled browser will block access to the site. If other popular news services also require home addresses, Joe's P3P-enabled browser will prevent Joe from receiving news over the Internet. Or he will have to give up his choice to keep his home address private.

It is reported that in earlier versions of the protocol, P3P also had "negotiation" and "data transfer" modules. The negotiation module would require an end user and a web site to haggle over the terms of access by negotiating an acceptable privacy agreement. Negotiation was dropped due to concerns about the complexity of the process. The data transfer module would have allowed for the automatic exchange of personal information after an acceptable privacy agreement was reached between a user agent and a web site. This idea was dropped due to polling data that revealed widespread public opposition to the automatic transfer of personal information.

Relating Cookies to P3P

The history of cookies illustrates several problems with industry-developed Internet standards, without privacy laws, that are likely to reappear with P3P.

Cookies by default are set as a silent tracking device rather than asking the user by default whether they wish to be tracked by a particular company. Similarly, we anticipate that P3P browsers will set a low standard of privacy before the user is "alerted."

Studies have found that web users find changing the default cookie settings to be burdensome and confusing. This is partly due to the many different versions of browsers that have been released over the years. (See for example <http://www.junkbusters.com/cookies.html> for a sampling of the various instructions for changing cookie settings.) On most browsers multiple clicks are need to get to relevant setting, and even if people who are aware of the need to change the default find it difficult to determine the appropriate action and understand the extent of its effects. P3P promises to be vastly more complex.

Many browsers also require the user to say "no" to each cookie when a users asks to be informed when cookies are placed, which can be very burdensome when several attempts are made per page. Useful features provided by third-party cookie management software is still not standard equipment: the ability to nominate certain sites that are permitted to set cookies, and have all others silently rejected.

Failure to Establish Privacy Standards

Technical methods to implement Fair Information Practices seek to give individuals greater control over the collection and use of personal information and to enable access to information. But P3P does not take this approach. It fails to establish privacy standards.

P3P builds on the notice and choice privacy approach. This is a weak model for privacy protection because it fails to ensure the observance of Fair Information Practices. This is also not the approach that the United States has typically taken to ensure privacy protection in other sectors with rapidly changing technology. The privacy of cable subscriber records is protected because of a provision in the Cable Act. The privacy of video rental records is protected by the Video Privacy Protection. The privacy of telephone calling records is protected by a series of laws and regulations.

Many in industry believe that the P3P standard will help solve the privacy problem because it will facilitate choice about privacy practices. But the real choice offered is not how to protect privacy, but how much privacy to give up. The FTC Chairman, in a report released in May 2000, made the point very well that the reason we need privacy laws today is that consumers are too often asked to give up their privacy for some benefit.

Strong technical measures are needed that give people greater control over the collection and use of personal information, and that limit where possible the collection and use of personal data.

Exclusion of Non-Compliant Sites

P3P will effectively exclude good web sites that lack P3P code even though the privacy practices of these sites may far exceed sites those that are "P3P compliant."

P3P is developed from a self-regulatory aspect giving web sites the option of whether to incorporate the P3P protocol on their web site. When a web site collects too much data they probably will not incorporate the P3P protocol. If few sites support P3P, consumers will have little incentive to use the technology, thus creating a sort of chicken and egg problem. "If not enough sites support the standard, consumers are not likely to deal with the daunting configuration, yet if not enough consumers demand it, marketers are unlikely to bother implementing it (Bruner, 1998)." Citigroup, who helped author the original P3P specification, presented this situation for data marketers in their white paper on P3P.

According to W3C, P3P also does not address how it will handle third party data collection on web sites. P3P currently cannot handle multiple privacy policies for one web page. For example, lets assume that the member only part of the site uses cookies for user tracking purposes, while the guest-only section uses cookies for session tracking. Since there can only be one policy per resource there is no way to accurately represent the distinctions between these two policies. It is suggested that the more restrictive of the two policies be in force for the target. However, that solution is not 100% accurate.

Absence of Enforcement

P3P lacks any means to enforce privacy policies.

Even where there is agreement about the privacy terms for a particular transaction, P3P provides no means to ensure enforcement of the stated privacy policies and the P3P developers do not seem particularly concerned about this problem. According to the most recent P3P specification:

Although P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personal information, it does not provide a mechanism for making sure sites act according to their policies. Products implementing this specification MAY provide assistance in that regard, but that is up to specific implementers and outside the scope of this specification. (Cranor et al, 2000)

Thus in jurisdictions where there are no privacy rights established in law, Internet users will have to rely on the non-enforceable policies represented in the P3P protocol.

Prognosis for Adoption

After more than three years in development, P3P still faces a number of serious challenges that will likely preclude its widespread adoption.

There is no user base and no user demand. Companies have been reluctant to adopt the complicated protocol structure, and governments has shown little indication that it will address public concerns about privacy protection.

Experience with cookies sheds light on another possible P3P user agent-side problem. Those consumers, who have taken the time to configure their browsers to notify when receiving, or reject cookies, have found that web surfing becomes nearly impossible.

The same situation will likely apply to P3P user agents. Concerned users will configure their P3P user agents to reflect high privacy protections. However, when these users attempt to access the majority of commercial web sites, endless pop-up windows warning them that a site wishes to go beyond their specified privacy preferences will result. Users who have configured their agents to block sites that do not meet their preferences may well find that there are few web sites left to surf. Consumers will likely respond to this frustrating situation by begrudgingly reverting to low P3P privacy protective configurations, thus maintaining industry's present privacy invasive status quo.

The incredible complexity of P3P, combined with the way that popular browsers are likely to implement the protocol could also undermine well-established privacy standards particularly where legislation is in place. P3P may actually strengthen the monopoly position over personal information that U.S. data marketers now enjoy.

Impact on Privacy if P3P is Deployed

Given the bleak prospects for adoption, P3P will likely serve to delay other efforts to establish privacy standards.

Microsoft and Netscape/AOL are likely to implement P3P in a way that sets very low privacy preference defaults. This is true because these companies are paid through advertisements and data collecting, so it in their best interest to have the lowest privacy preference as defaults. If this is the case, user agents may actually facilitate the collection of even more information than is now typical.

The perverse effect of possible P3P implementations which seeks to extract privacy rather than protect it, is that those people who most value their privacy will be shut out of the web.

Critiques of P3P also call into question its much-hyped role as a self-regulatory "solution" to the online privacy problem. Rather than a Privacy Enhancing Technique (PET), P3P may well prove to be a Privacy Intrusive Technique (PIT) (Rotenberg, 2000).

P3P Fails to Satisfy Jurisdictions with Strong Privacy Standards

P3P has not impressed those jurisdictions that have considered its use to implement legal rules for privacy.

The European Union, which does have baseline, legally enforceable privacy rights in the form of the EU Data Directive, has explicitly rejected P3P as part of its privacy protection framework. In a strongly worded January 1998 opinion statement, the European Commission identified numerous problems with the protocol. First it argued that P3P "has not been developed with reference to the highest known standards of data protection and privacy, but has instead sought to formalize lower common standards." Next it pointed out the information asymmetry problem, noting that:

A technical platform for privacy protection will not in itself be sufficient to protect privacy on the web. It must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals. Use of P3P in the absence of such a framework risks shifting the onus primarily onto the individual user to protect himself, a development which would undermine the internationally established principle that it is the "data controller" who is responsible for complying with data protection principles.

Finally, there was concern that P3P might create confusion about the obligations of EU-based companies, and the privacy rights of EU consumers:

There is a risk that P3P, once implemented in the next generation of browsing software, could mislead EU-based operators into believing that they can be discharged of certain of their legal obligations (e.g. granting individual users a right of access to their data) if the individual user consents to this as part of the online negotiation. In fact those businesses, organizations and individuals established within the EU and providing services over the Internet will in any case be required to follow the rules established in the data protection directive 95/46/EC (as implemented in national law) as regards any personal data that they collect and process. P3P might thus cause confusion not only among operators as to their obligations, but also among Internet users as to the nature of their data protection rights. (European Commission, 1998)

For these reasons, the EU has not adopted P3P as a technical mechanism for enforcing its privacy laws.

Better Alternatives Exist

There are much better technical methods for Internet privacy protection than P3P currently available to Internet users.

The P3P developers claim that the P3P protocol is the only widespread standard for privacy protection, but this is nonsense. At present, there is hardly any P3P enabled web sites in the world. Meanwhile, there are many genuine technologies for privacy protection widely available on the

Internet. A quick survey of the EPIC Online Guide to Practical Privacy Tools [<http://www.epic.org/privacy/tools.html>] shows a wide range of services currently available for anonymous surfing, defeating cookies, HTML filters and more.

Those techniques that protect privacy minimize or eliminate the collection of personally identifiable information. There are many tools currently available that provide these privacy solutions and many more are being developed.

Conclusions and Recommendations

P3P fails to comply with baseline standards for privacy protection. It is a complex and confusing protocol that will make it more difficult for Internet users to protect their privacy. P3P also fails to address many of the privacy problems specifically associated with the Internet.

Earlier versions of P3P were withdrawn because the developers recognized that the proposed negotiation process was too burdensome for users and that the automatic transfer of personal information would be widely opposed. It is anticipated that this version of P3P will also be significantly overhauled once it is reviewed.

Companies that seek to promote online privacy will not burden web visitors with P3P. Good privacy standards will be built on Fair Information Practices and genuine Privacy Enhancing Techniques that minimize or eliminate the collection of personally identifiable information. Simple, predictable rules for the collection and use of personal information will also support consumer trust and confidence. P3P, on the other hand, is likely to undermine public confidence in Internet privacy.

References

Ackerman, M.S. and Cranor, L.F. (1999, September). Privacy critics: Safeguarding users' personal data. WebTechniques.com. Available: <http://www.webtechniques.com/archives/1999/09/ackerman/> .

Bruner, R.E. (1998, 30 June). P3P: Programming privacy. Executive Summary, 1 (7). Available: <http://www.exec-summary.com/trends/980630.phtml> .

Cerasale, G. and Faley, P. (1998, 6 July). Comments of the Direct Marketing Association on elements of effective self regulation for the protection of privacy and questions related to online privacy. Testimony before the Department of Commerce. Available: <http://www.ntia.doc.gov/ntiahome/privacy/mail/disk/DMA.htm> .

Clarke, R. (1998). Platform for privacy preferences: A critique. Available: <http://www.anu.edu.au/people/Roger.Clarke/DV/P3PCrit.html> .

Coyle, K. (1999, June). P3P: Pretty poor privacy? A social analysis of the Platform for Privacy Preferences. Available: <http://www.kcoyle.net/p3p.html> .

Cranor, L., et al. (2000, 10 May). The Platform for Privacy Preferences 1.0. W3C Working Draft. Available: <http://www.w3.org/TR/P3P/> .

Einstein, D. (1997, 27 May). New standard offers privacy protection. San Francisco Chronicle, C1.

European Commission. (1998, January). Platform for Privacy Preferences and the Open Profiling Standard. Draft opinion of the Working Party on the Protection of Individuals with regard to the

processing of Personal Data. Available: <http://www.epic.org/privacy/internet/ec-p3p.html> .

Federal Trade Commission. (2000, May). Privacy online: Fair information practices in the electronic marketplace. Report to Congress. Available: <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> .

Federal Trade Commission. (1996, 4 June). Testimony: Public Workshop on Consumer Privacy on the Global Information Infrastructure. Available: <http://www.ftc.gov/bcp/privacy/wkshp96/pw960604.pdf> .

Guglielmo, C. (1999, 26 January). Privacy proposal faces patent challenge. Inter@ctive Week. Available: <http://www.zdnet.com/intweek/stories/news/0,4164,2194490,00.html> .

Hunter, C.D. (1999). Filtering the future? Unpublished thesis in Communication. Annenberg School for Communication, University of Pennsylvania.

Lee, K. and Speyer, G. (1998). Platform for Privacy Preferences project and Citibank. Citibank White Paper. Available: http://www13.w3.org/P3P/Lee_Speyer.html .

Mulligan, D. et al, (2000, 28 March). P3P and privacy: An update for the privacy community. Available: <http://www.cdt.org/privacy/pet/p3pprivacy.shtml> .

Netscape Communications Corporation. (1997, 27 May). Netscape, Firefly and Verisign propose Open Profiling Standard (OPS) to enable broad personalization of Internet services. Netscape press release. Available: <http://www.netscape.com/flash4/newsref/pr/newsrelease411.html> .

Reagle, J. and Cranor, L. (1998). The Platform for Privacy Preferences. World Wide Web Consortium NOTE. Available: <http://www.w3.org/TR/1998/NOTE-P3P-CACM/> .

Reagle, J. and Wenning, R. (2000, 18 April). P3P and privacy on the web faq. Available: <http://www.w3.org/P3P/P3FAQ.html> .

Rotenberg, M. (2000, 7 February). What Larry doesn't get: Fair information practices and the architecture of privacy. Paper presented at the Stanford Law School Symposium on Cyberspace and Privacy. Available: http://stlr.stanford.edu/STLR/Articles/01_STLR_1/index.htm

Rotenberg, M. (1998, 26 March). Testimony before the House Judiciary Committee. Available: <http://www.epic.org/privacy/internet/rotenberg-testimony-398.html> .

Weitzner, D. J. (2000, 25 May). Testimony before the United States Committee on Commerce, Science, and Transportation. Available: <http://www.w3.org/2000/05/25-Senate-Privacy-Testimony.html> .

World Wide Web Consortium. (1999a, 21 September). Removing data transfer from P3P. P3P Working Group. Available: <http://www.w3.org/P3P/data-transfer.html> .

World Wide Web Consortium. (1999b, 28 October). World Wide Web Consortium clears patent hurdle for web privacy. W3C press release. Available: <http://www.w3.org/1999/10/28-P3P-IntermindPatentAnalysis-PressRelease.html> .

World Wide Web Consortium. (1998a, 19 May). The W3C publishes first working draft of P3P 1.0. W3C press release. Available: <http://www.w3.org/Press/1998/P3P> .

World Wide Web Consortium. (1998b, 19 May). P3P 1.0 testimonials. W3C press release. Available: <http://www.w3.org/Press/1998/P3P-test.html> .

World Wide Web Consortium. (1997a, 23 May). W3C Platform for Privacy Preferences (P3) project approved. W3C press release. Available: <http://www.w3.org/Privacy/announce/P3Approval.html>

World Wide Web Consortium. (1997b, 11 June). W3C announces the Platform for Privacy Preferences project at FTC workshop. W3C press release. Available: <http://www.w3.org/Press/P3>

World Wide Web Consortium. (1997c, 30 October). World Wide Web Consortium announces completion of P3P project phase one. W3C press release. Available: http://www.w3.org/P3P/press_release.html

□

□

>> Freedom FAQ

- 1 [Product Information](#)
- 2 [Purchasing Information](#)
- 3 [Using Freedom Privacy & Security Tools 3.0](#)
- 4 [Online Privacy](#)

1. Product Information

- [What is Freedom Privacy & Security Tools 3.0?](#)
- [What is new in Freedom Privacy & Security Tools 3.0?](#)
- [How does Freedom Privacy & Security Tools Features compare to other privacy products?](#)
- [Do I need to use a special browser with Freedom Privacy & Security Tools?](#)
- [How does the Personal Firewall protect me? What if I have a high-speed connection?](#)
- [How does the Form Filler help me when I am browsing?](#)
- [Is the information I enter into the Form Filler safe? Where is it kept?](#)
- [How does the Keyword Alert protect me on the Internet?](#)
- [How does the Ad Manager speed up browsing?](#)
- [What are cookies and how does Freedom Privacy & Security Tools handles them?](#)

What is Freedom Privacy & Security Tools 3.0?

Freedom Privacy and Security Tools 3.0 comprises the following features:

- Personal Firewall
- Form Filler / Password Manager
- Ad Manager
- Cookie Manager
- Keyword Alert

Freedom Privacy & Security Tools is a flexible suite of tools to secure your PC and protect your privacy on the Internet. It includes a Personal Firewall to prevent malicious attacks to your computer; a Form Filler to secure passwords and online registrations; an Ad Manager to block banner ads, web bugs and to speed up browsing; a Cookie Manager to block cookies you don't want; and a Keyword Alert to prevent unauthorized information from leaving your computer. For detailed information, please visit the [Freedom Privacy & Security Tools product information center](#).

What is new in Freedom Privacy & Security Tools 3.0?

We've incorporated a lot of what you, our customers, have told us you want: a simplified interface; an easier installation and setup process; more control for each individual feature; and a handy privacy and security guide to help you and your family navigate the Internet safely.

[Features & Benefits](#)[Product Information](#)[Awards & Reviews](#)[Why You Need Protection](#)[How We Compare](#)**FAQ****Distribution Partners**

Bundle Freedom to increase revenue, differentiate and add value to your offering and strengthen customer relationships.

[Find out more!](#)

Privacy policy

Zero-Knowledge does not require and, as a matter of policy, does not want to obtain any more information from subscribers than absolutely necessary. Learn how we're striving to protect your privacy, [here!](#)

How does Freedom Privacy & Security Tools compare to other privacy products?

For a full comparison of how Freedom Privacy & Security Tools stacks up to other products, click [here](#).

Do I need to use a special browser with Freedom Privacy & Security Tools?

No special browser is necessary. Freedom Privacy & Security Tools works with almost any program for supported Internet protocols. The Internet protocols that Freedom Tools supports are email (SMTP), Web surfing (HTTP and SSL), news (NNTP), Internet Relay Chat (IRC), and Telnet.

How does the Personal Firewall protect me? What if I have a high-speed connection?

A Personal Firewall is necessary to keep unauthorized data from entering or exiting your computer. Any machine connected to the Internet is potentially vulnerable, but the best targets are those with high-speed, "always on" connections, such as cable modems or digital subscriber lines. It's fairly simple for someone to find out if they can connect to your machine and then look for files to compromise. High-speed connections are typically targeted as they are the simplest to track down and find again; your Internet service provider generally assigns your system a fixed Internet Protocol address, which identifies your computer to the network.

How does the Form Filler help me when I am browsing?

The Form Filler automatically fills out online forms with your real information or can generate random information for you. It also remembers and manages your online account names and password. All personal and sensitive information is encrypted and stored on your own computer, where only you have access to it.

Is the information I enter into the Form Filler safe? Where is it kept?

The information you enter in the Form Filler is kept in your Freedom Privacy & Security Tools settings file (called freedom.dat). This file is encrypted with military-grade encryption and stored safely on your computer. No one, not even Zero-Knowledge employees, has access to this information.

How does the Keyword Alert protect me on the Internet?

The Keyword Alert feature can help to ensure that your personal information will not be transmitted without your permission. By adding what information you would like scanned to the Keyword Alert, you can prevent the accidental release of your data and have the Keyword Alert prompt you for permission each time you send out information by email, web and IRC.

How does the Ad Manager speed up browsing?

The Ad Manager speeds up your Web browsing by blocking unwanted banner ads. The Web

pages you access will load faster because they don't download the ads.

What are cookies and how does Freedom Privacy & Security Tools handle them?

Cookies are text files that Web servers place on your computer. The server uses the file to identify you when you return to the site. Cookies not only aid websites in identifying repeat visitors, they also allow you to customize your browsing experience. For example, when you log into a password-protected website, a cookie from that website helps the site "remember" you and your site preferences so you don't have to re-enter the password every time you go to a new page on the site.

Cookies also allow servers to monitor your browsing habits, including how many times a site is visited, as well as which pages you view. The Cookie Manager in Freedom Privacy & Security Tools gives you control over how much information Web sites record about your browsing habits. Before a cookie is placed on your machine, the Cookie Manager checks the Cookie Filter to see if the cookie is from a Web site that you previously asked to be blocked. If the cookie is from a blocked site, it is deleted immediately. Otherwise, Freedom Privacy & Security Tools catches the cookies and deposits them in your Cookie Jar®.

[◀ back](#)

[next ▶](#)

[feedback](#)

[privacy statement](#)

[legal](#)



To print: [Click here](#) or Select **File** and then **Print** from your browser's menu

This story was printed from [ZDNN](#),
located at <http://www.zdnet.com/zdnn>.

Hardwiring Privacy

By *Juliana Gruenwald*, *Interactive Week*

April 30, 2001 11:58 AM PT

URL: <http://chkpt.zdnet.com/chkpt/printthisclick/www.zdnet.com/filters/printerfriendly/0,6061,2713739-2,00.html>

A European Parliament committee is expected to take up legislation in coming weeks that would require companies to include privacy-protection technology in their products.

The controversial provision is included in proposed revisions to a 1997 European Union law outlining privacy protections in telecommunications. The parliament's citizens' freedoms and rights committee is expected to vote on it next month.

Computer companies and mobile phone makers argue that the provision would not stop those intent on misusing personal data. Instead, it would stifle innovation and hurt competition, according to the European Information and Communications Technology Industry Association.

"We do not want to get into a situation where [information technology] and technology development is being directed by a government body," said Melika D. Carroll, Intel's government affairs policy manager for Europe.

The measure's controversial provisions include a demand that all EU member states adopt an opt-in scheme requiring prior consent to send unsolicited e-mail. Supporters say this would help address the growing spam problem. An EU report released in February estimated that spam costs Net users and Internet service providers a total of \$9 billion per year.

Direct marketers say the proposal does not distinguish between spam and marketing from legitimate companies. They say the opt-in requirement will not stop spam and will instead harm legitimate businesses.

A spokesman for Marco Cappato, the parliament member drafting a report on the proposal for the citizens' freedoms committee, said his boss is "not enthusiastic about the proposal." Cappato has come under fire for using unsolicited e-mail for his political party.



July 16, 2001

Special Report: E-Commerce

The Privacy Officer

What's standing between your personal information and the world? People like Benjamin E. Robinson III

By JARED SANDBERG

Benjamin E. Robinson III probably knows more about you than you know about him.

As chief privacy officer of MasterCard International Ltd., he is the keeper of all manner of sensitive financial information about MasterCard carriers. Mr. Robinson is among the growing numbers of chief privacy officers, a newly created executive post popping up throughout corporate America. Companies like **American Express Co.**, **Sony Corp.**, **Citigroup Inc.** and **International Business Machines Corp.** have appointed their own privacy chiefs. Today, there are an estimated 300 of them, and their numbers are expected to swell over the next few years.

Detractors call the appointing of CPOs a public-relations ploy or a case of the fox guarding the henhouse. They agree somebody has to look after consumer privacy. They just aren't convinced it's the companies that should be doing it.

Whoever is the guard, electronic commerce clearly has made the job an important one. E-commerce depends on collecting and sharing an unprecedented amount of sensitive information. For companies to succeed in the e-commerce business, they must flesh out details of their customers' otherwise anonymous digital personas. Collecting information about consumer preferences -- which products people buy and those they're likely to buy -- can allow e-merchants to offer convenience unrivaled in the offline world. By tracking prior purchases and recognizing repeat users, Amazon.com, for example, is able to promote a strikingly tailored range of products to customers revisiting its site.

Need to Know?

But with the increase in companies gathering data on their customers has come a growing concern about where that personal information is going.

Lawsuits against companies charging privacy violations, including some filed by state attorneys general, are on the rise. Most commonly, plaintiffs are taking companies to task for violating their own privacy policies by sharing customer data. Up until last year, such suits were unsuccessful, but the courts have begun to rule in favor of plaintiffs more frequently, reflecting judges' sensitivity toward the public's growing privacy concerns. The newsletter Privacy and American Business estimates that companies have paid \$61.5 million in settlements of such suits since 1999.

Meanwhile, the Gramm-Leach-Bliley Act, signed by President Clinton in 1999, requires the financial industry, including credit-card companies, brokerage services and travel agencies, to notify consumers of their privacy policies. They also must allow consumers to "opt out" of practices in which companies disclose certain financial details to other companies. That is, consumers must be able to tell companies to keep private any personal information.

It's the chief privacy officer's job to keep a company out of hot water -- whether in a court of law or in the court of public opinion. Some CPOs may come from the government-affairs department of a company, the legal department, consumer affairs or the information-systems group. But all of them must help their companies avoid consumer litigation, assess any risks to customer privacy and develop Internet privacy policies. They also must create a system that will handle and resolve consumer complaints and make sure new products don't threaten customer privacy.

Simply put, CPOs have to protect consumers from their companies while protecting companies from consumers.

Politics of Privacy

It's trickier than it sounds. CPOs must balance their customers' right to privacy with their corporation's need for profits. And the two don't necessarily go hand in hand.

"How do you mobilize support when you're stepping on the bottom line and you know powerful people are going to be your foes?" says Alan Westin, president of the Center for Social & Legal Research, a Hackensack, N.J., organization that publishes the Privacy and American Business newsletter and has conducted training sessions for CPOs. "If you are not good at people skills, at coalition building, at using the political environment to show top management what it must do, then you're in the wrong job."



John Patrick Naughton

The Quiet Man: Benjamin E. Robinson III, MasterCard's CPO

Not Mr. Robinson. As the 37-year-old executive strolls the white-marble headquarters of MasterCard, set amid the stately oaks and maples of Purchase, N.Y., he greets everyone, chatting with each person he meets about personal affairs. Mr. Robinson's congeniality, his light touch and big smile, come in handy for a typically politicized post. He balks at the notion that his job puts him between a rock and a hard place, in large part because conflict isn't his style. He says he never has arguments over the cost of privacy compliance. "Usually, I get, 'Fine, make it happen,'" he says.

As an association of member banks, MasterCard hasn't traditionally dealt directly with consumers. It has known only credit-card numbers -- data that are protected in a hush-hush facility in St. Louis -- and nothing about the people behind them. Only the member banks knew the customers' names. But with a growing number of online products and services, the company is dealing directly with its customers, attaching addresses, phone numbers and even purchases to the card numbers.

There are moments when Mr. Robinson has had to play the bad guy. Take MasterCard's Online Exclusives offering. If users sign up for the service -- supplying their names and addresses, among other details -- they can receive discounts from dozens of e-commerce merchants. You can get a 10% discount, for example, at MoroccanLanterns.com if you use your MasterCard. But for MoroccanLanterns.com to qualify for the service, the Dallas company had to comply with MasterCard's privacy policy, which says the only reason a partner can share data with another company is to fulfill a customer order. So in the case of MoroccanLanterns, the company can give its suppliers the customers' addresses and product specifications only to produce and ship a lantern. It can't share the information with, say, a company selling light bulbs.

In the year that Mr. Robinson has held the post, he has scotched about a half-dozen proposed partnerships because he lacked confidence that the partners could keep a lid on sensitive customer data. Though he concedes he may have locked horns with colleagues who were pushing such partnerships, he doesn't see any evidence of rancor. That may be because he's convinced them of his motto: "Good privacy is good business."

"The CPO position doesn't have to be adversarial," he adds. "It's not my personality or style to take disagreements personally." For Mr. Robinson, the job is largely about finesse. When he missed an important marketing meeting, he sent its organizer flowers.

Perhaps his greatest challenge is making sure that as MasterCard offers more and more consumer services in which a great deal of information about the cardholder is known, the personal details of the holder doesn't spin out of control in the ether of the Internet. An online merchant could pass the data along to a direct marketer, who, in turn, could pass it along to yet another company. This "data flow" concerns Mr. Robinson most. E-commerce has "nuances that we never necessarily thought of," he says. "Cyberspace is so broad that we don't know where the information is going."

Mobile Concerns

On one recent morning, after his requisite cup of coffee, Mr. Robinson sat down with separate MasterCard businesses that make up the so-called E-Business Group. Included among the meeting's participants were people from various emerging technology divisions such as those involving smart cards, which have built-in microprocessors and memory and are considered more secure than credit cards, and mobile commerce, which involves purchasing products through cell phones and other wireless products.

The meeting's big issue: how the Federal Communications Commission might regulate the nascent arena of mobile commerce. Like many of his CPO counterparts, Mr. Robinson spends much of his time schooling colleagues on existing privacy regulations or anticipating potential new rules.

It was Mr. Robinson's task to sift through current regulations and look for a hint. But no such luck. "No one has really talked about" privacy and mobile commerce, he says.

So he points out -- as he had done many times -- that if consumers use new technology that involves MasterCard, the company will have to draft a privacy policy, notify users of the policy and give them a chance to opt out. "A lot of these meetings at this stage of the game are giving the business units an idea of what's going on in the [privacy] industry," he says.

After that hourlong meeting, Mr. Robinson headed into the office of Ruth Ann Marshall, president of MasterCard's North America Region, to talk about hockey. In March and April, MasterCard ran a sweepstakes with the National Hockey League that allowed cardholders to win free passes to the league's Celebrity Face Off game. Since the contest dealt directly with the personal information of Canadian consumers as well as those in the U.S., Mr. Robinson needed to ensure that the company's U.S. privacy policy would meet the requirements of Canadian laws.

It didn't. Like the U.S., Canadian laws require businesses to notify consumers how their information is being used and give them an opportunity to stop it from being passed along. But the Canadians go further. Any consumer in Canada can request access to the personal data being collected by a company. So Mr. Robinson recommended that MasterCard prepare to give Canadian residents access to their digital selves. That meant contacting information-systems staffers to make sure each person's data could be segregated out and shipped if requested -- which staffers did, for Canadian participants only.

Global Differences

Such subtle differences between privacy laws world-wide pose a constant challenge. Last year, for example, MasterCard unveiled the TradeCard, a credit card that prequalifies companies to buy goods and services from international companies without going through the lengthy process of obtaining a letter of credit. Mr. Robinson was concerned that some countries, such as Hong Kong, give privacy protections to businesses. Unlike with consumers, businesses in the U.S. don't necessarily have to be informed of the fact that their private information may be passed along to other businesses. He made sure MasterCard notified its TradeCard users of the possibility of their information being passed along to other TradeCard members. The company also told users that it wouldn't share a member's information outside the TradeCard offering without the member's consent.

After the meeting with Ms. Marshall, Mr. Robinson headed to the cafeteria for a working lunch with MasterCard's audit team. Toting a packed lunch in his signature fluorescent green bag, he sat down with a group responsible for reviewing the company's business practices. It was a simple meeting to report to him their review of different divisions, making sure the proper privacy policies and procedures were put in place in all the divisions that needed them. In the year Mr. Robinson has held the post, he's crafted about 10 different privacy policies, each catering to the laws of the countries involved.

The auditors, who were making sure MasterCard's units had complied with the Gramm-Leach-Bliley Act, said Mr. Robinson has done a good job. So far, it appears Mr. Robinson is doing something right with respect to privacy: The company says it hasn't received any customer complaints.

-- Mr. Sandberg is a staff reporter in The Wall Street Journal's New York bureau.

Write to Jared Sandberg at jared.sandberg@wsj.com¹

URL for this Article:

<http://interactive.wsj.com/archive/retrieve.cgi?id=SB994959146618010786.djm>

Hyperlinks in this Article:

(1) <mailto:jared.sandberg@wsj.com>

Copyright © 2001 Dow Jones & Company, Inc. All Rights Reserved.

Printing, distribution, and use of this material is governed by your Subscription Agreement and copyright laws.

For information about subscribing, go to <http://wsj.com>

Close Window

Microsoft News

[Product News](#)
[Legal News](#)
[International News](#)
[Consumer News](#)

Corporate Info

[Investor Relations](#)
[Community Affairs](#)
[Microsoft Research Events](#)
[Image Gallery](#)
[Exec Bios/Speeches](#)
[Bill Gates Web Site](#)
[Youth and Learning](#)

Site Map

Search

(Exact Phrase)

[Advanced Search](#)

Top Stories

by Month:

Press Releases

by Month:

Microsoft Passport: Streamlining Commerce and Communication on the Web

REDMOND, Wash., October 11, 1999 -- Microsoft today launched Passport, a single sign-in and wallet service for communication and commerce on the Internet. By creating a single Passport "identity," users can easily access information and purchase goods on multiple Web sites using a single login and password. Brad Chase, **senior** vice president of Microsoft's Consumer and Commerce Group and a key leader in the company's **Internet** strategy, spoke with PressPass about this new service.

PressPass: Passport has been available for a few months on **MSN.com**, and it already has millions of users. What does today's announcement mean?

Chase: Microsoft Passport's single sign-in service has been available since July on a number of MSN sites, such as **MoneyCentral**, Web Communities, Auctions, and Hotmail. Today, we're announcing the broader availability of the Passport wallet service, with more than 50 Internet sites committed to supporting the Passport wallet -- including leading merchants like **barnesandnoble.com**, **Buy.com**, and **Costco.com**. This new service allows online shoppers to purchase items with ease, eliminating the need to repeatedly type the same shipping and billing information when ordering products or services at different Web sites.

PressPass: How do you see Passport growing as we head into the holiday shopping season? How will the formal launch help the service's expansion?

Chase: We will continue to sign up new merchants. Each site's implementation schedule will vary, but we're strongly encouraging them to go live in time for the holidays. Passport members are able to find out which sites now use the service, and which are coming soon, by checking the directory of participating sites at the Passport Web site. We expect a good number of merchants to be live with the service for the holiday shopping season.

From a business partner perspective, this launch provides Microsoft with the opportunity to tell the industry that Passport is officially "open for business." We're very excited to announce that a large number of leading Web merchants have already committed to supporting the wallet service, and that will certainly attract other online businesses.

Related Links

Press Releases:

- [Microsoft Passport Offers Streamlined Purchasing Across Leading Web Sites](#) - Oct. 11, 1999

Feature Stories:

- [Q&A: Making the Web an Indispensable Part of People's Lives](#) - Sept. 23, 1999

Other Microsoft Resources:

- [MSN on PressPass](#)
- [Passport Web Site](#)
- [MSN.com](#)

PressPass: How is Passport different from competing services?

Chase: Other services now available offer only subsets of Passport's capabilities. Passport offers a more complete suite of services, including an electronic wallet service as well as a single sign-in that provides a login name and a set of mostly optional demographic information that can be used across multiple Web sites. Some of Passport's other benefits include giving consumers the ability to use their Passport identity across many Internet sites, not simply within a proprietary network, and a server-side design, which provides consumers access to their Passport anytime, anywhere, using any Internet device.

In addition, Passport takes a stronger stance on privacy and security. Passport ensures that its members always control the information stored in their Passport, and which Web sites receive it. Moreover, Passport requires all participating sites to adopt privacy policies that conform to industry-recognized privacy standards -- and they are required to post a link to their privacy policy on the front page of their site.

PressPass: What benefits does Passport offer online merchants that their own proprietary systems do not?

Chase: Today, each Web site asks consumers to fill out practically the same time-consuming purchase form. This just isn't a good use of their time and many consumers simply give up, leaving a full shopping cart. Companies that participate in the Passport service are providing their customers with the convenience and simplicity they've grown accustomed to when purchasing offline. A comparison might be made to the evolution of the credit-card industry. Consumers used to carry heavy wallets stuffed with a different credit card for every store. Today, they can use one universal credit card at millions of stores.

One of the reasons businesses have preferred their own wallet systems to date is that those systems match their sites' look and feel. We've addressed that by designing Passport to be highly customizable. As Passport customers purchase goods and services from participating sites, they maintain a continuous association with each merchant's site and brand. Also, we've ensured that Passport is easy to implement. Merchants simply incorporate a link into their purchase pages and retrieve data posted from the Passport server.

PressPass: Microsoft recently agreed with competitors such as Sun Microsystems and AOL on a new technical format for electronic wallets called "electronic-commerce modeling language," or ECML. What will this new standard mean to Passport users?

Chase: The new ECML format is an effort by Microsoft and other e-commerce leaders to make online

purchasing easier for all consumers and merchants. The market acceptance and widespread appeal of electronic wallets has been hampered by a lack of standards. ECML simply defines a set of uniform field names for common commerce data that wallets and merchants can use to improve their communications. Even though wallets using ECML carry the same field names for the data that they manage, the user experience will be different from one wallet to the next. And the sites that support each wallet also will vary. The benefit to Passport members is that many more merchants can easily process the information they receive from consumers using Passport wallets.

PressPass: Microsoft assures that information in the Passport wallet is secure and private. How does Passport help users control how their personal information is used on the Internet?

Chase: Passport ensures that its members always control the information stored in their Passport. Members decide which Web sites receive that information when they choose to sign into or use their Passport wallet.

In addition, Passport makes managing this information much easier for consumers by allowing them to store it in one location. This really makes updates a breeze. For example, let's say you often send gifts to your parents. If they move, all you need to do is update their address once, rather than changing it at every site you frequent.

Passport also helps consumers control the use of their information by requiring all participating Web sites to adopt privacy policies that conform to industry-recognized privacy standards. The sites must also post a link to their policy from their front page, so that consumers have an easy time finding the policy if they want to review it.

PressPass: How much information about my online activities and me personally is shared by Passport and participating Web sites?

Chase: First, the only information that can be shared between Microsoft and the participating Passport sites is the demographic and wallet information that a member has provided. When a member signs into a Web site, Microsoft sends the site that member's zip code, country, and city or region. The member may also choose to provide his or her nickname, e-mail address, age, gender, and language preference when signing in.

Separately, when members decide to use their wallets to buy something online, only the specific billing and shipping information selected for that particular purchase will be sent to that site. The site may ask consumers for additional information, such as their dress size or airline seating preference -- but this information is not stored in the member's Passport and, therefore, is not shared with other sites that the

member chooses to sign into or purchase from.

When a member chooses to sign into a site, his or her information is subject to that site's policies. A quick check of the merchant's privacy policy -- using the link on the home page of the site -- will provide what consumers need to know to understand how the merchant will use their Passport information, including their e-mail and mailing addresses.

PressPass: How does Passport fit into Microsoft's new "Everyday Web" Internet strategy?

Chase: The "Everyday Web" is Microsoft's vision of making the Web an essential and valuable part of people's lives. Passport's role in this strategy is to make common activities, such as shopping online and getting access to information or communications services, significantly easier. These activities usually require the consumer to share information with a site. Passport's single sign-in and wallet services provide the key for making these exchanges easier, faster, and more secure. And, consumers can access their Passport wallet anytime, anywhere, using any device connected to the Internet.

The "Everyday Web" vision for businesses is to provide a comprehensive and integrated suite of services to help companies leverage the Internet to increase their sales and profits. For them, Passport's services provide an opportunity to improve their customers' experience by streamlining purchasing and simplifying sign-in and registration. Not only will this allow online merchants to increase their revenue, it will help them build stronger relationships with their customers.

©2001 Microsoft Corporation. All rights reserved.
Terms of Use Privacy Statement

Passport Fact Sheet

Overview

Microsoft® Passport is a suite of e-business services that makes using the Web and purchasing online easier, faster, and more secure for its members. Passport provides its members with single sign-in and express purchase capability at participating sites, reducing the amount of information to be remembered or retyped.

Passport can increase sales for businesses and help build stronger relationships with customers by streamlining the purchase process and by providing a high-quality, more secure online experience for a large member base. Passport protects the security of members' personal information and online transactions by using powerful encryption technologies and by requiring participating sites to adhere to comprehensive privacy policies that conform with accepted guidelines.

Passport offers the following services:

- **Single sign-in**—Passport members can create one sign-in name and password for use across participating Passport sites. Members save time and avoid repetitive data entry by storing basic demographic information that can be shared with Passport sites. When members sign in to a participating site, Passport sends the members' ZIP Code, country, and city or region information. Members can also choose to provide their nickname, e-mail address, age, gender, and language preference.
- **Express purchase**—Consumers can enjoy an easy and fast online purchasing experience by storing their billing and shipping information in their Passport. When using express purchase, Passport members see the contents of their Passport and can send their encrypted information to a participating merchant site with a single click.
- **Kids Passport**—Kids Passport is part of the Passport single sign-in service, and is an example of Microsoft's ongoing initiative to provide children with a positive, safe online experience. Kids Passport helps parents protect their children's privacy online by allowing parents to decide whether their children can use Passport participating Web site services that collect and/or disclose personally identifiable information. These services include newsletters, discussion groups, pen pal programs, wish lists, and contests.

Key Consumer Benefits

Web users commonly complain about the inconvenience of both retyping the same information at every site and keeping track of multiple sign-in names and passwords. Through its single sign-in and express purchase services, Microsoft Passport helps create a more secure, convenient environment for members to access information and make online purchases. Consumers who use Passport enjoy these benefits:

- **Fast sign-in and purchasing**—Passport eliminates the need for its members to remember multiple sign-in names and passwords. During Web sessions, members need to type their sign-in name and password only once. A single click gives members access to other Passport sites until they sign out. Once members are signed in, online purchasing is simple. Clicking the express purchase button displays the contents of a member's wallet, and a second click sends billing and shipping information to the merchant. By providing

some basic demographic information, members can also expedite site registration and purchasing requirements.

- **Easier online experience across multiple devices**—Passport information is stored in a single location and is easily accessible for review or update from a wide range of devices, including personal computers, WebTVs, handheld devices, and kiosks. In addition, a single device can support multiple Passport members.
- **Security and privacy**—The information stored in a member's Passport is strictly under that member's control (or the parent's control for Kids Passport members). Members can update the information at any time and can also decide which Passport sites to share the information with. All sensitive information is encrypted and transmitted securely using the Secure Sockets Layer (SSL) protocol. Also, each participating Passport site must adhere to specific privacy and security guidelines and must provide a link to their own policy on the front page of the site.

Key Business Benefits

One of the most significant benefits of Microsoft Passport is the ability to streamline the purchase process, making it easier for people to shop online. According to Jupiter Communications, 27 percent of consumers abandon items they put into a "shopping cart" at a Web storefront because they find the process of filling out forms to be too difficult.*

Passport also provides the following business benefits:

- **Streamlined sign-in and registration processes for a large member base**—Passport simplifies sign-in and registration, lowering the barriers to e-commerce for the millions of consumers who are Passport members.
- **High-quality, more secure online experience**—Passport uses secured servers and encryption technologies to transmit members' information, providing consumers with a more secure Web experience.
- **Increased customer acquisition and retention rates**—Passport provides the ability to deliver personalized content based on core Passport profile data.
- **Extensive customization**—Merchants can tailor the Passport sign-in and express purchase pages to match their site design, providing a seamless experience to their customers. Customization options include prominent branding, flexible background color, detailed purchase information, and the ability to add additional purchase fields.
- **Easy implementation**—Passport has been designed for easy implementation in merchant site operations. In addition, express purchase uses the industry-standard Electronic Commerce Modeling Language (ECML) data format to facilitate transactions between electronic wallets and merchants.
- **Attraction and retention of young visitors**—The Kids Passport service can help operators of Web sites increase their acquisition and retention of young visitors, as well as help them comply with the recently enacted Children's Online Privacy Protection Act (COPPA).** Kids Passport also eliminates the need for businesses to develop their own parental consent solution, which can be costly and time-consuming.

Privacy and Security Issues

The security of Web users' personal information is of utmost importance to Microsoft. Passport members control their information, and the sign-in process is protected by SSL encryption. Participating sites never receive members' passwords, and all Passport cookies are strongly

encrypted. Passport also uses SSL to transmit sensitive purchase information from Microsoft to participating merchants. Merchant sites may store the information on their own servers, but the use of such information is governed by the merchant's privacy policies.

In addition, Passport provides the following privacy and security considerations:

- **No monitoring or reporting of sites visited by individuals**—Passport does not maintain a record of the sites that individual Passport members visit. During members' Internet sessions, Passport servers receive information confirming that the sites are valid, participating sites. This allows the servers to sign members out of each site when they request it. However, Microsoft does not store this information on an individually identifiable basis following the end of a session. Microsoft servers do log strictly aggregate statistics (such as the cumulative number of requests from any given IP address or URL), which enables Microsoft to focus on adding sites to the Passport network that Passport members prefer. Microsoft does not track or report data tied to any individual user.

Note The Passport service does track parental consent status for users under the age of 13 to assist participating sites in complying with COPPA laws. Microsoft does not sell, rent, lease, or otherwise report this data to any third parties and does not use this data for any purposes other than running the Kids Passport service as described on the Passport Web site.

- **Sharing of information**—The only information Microsoft can share with participating sites is the information stored in a Passport, and this is only done when members choose to use Passport at those sites ("expressed permission"). In cases where a site requires additional information, members decide whether to provide it; if they do, the exchange is strictly between the member and that site.
- **Information required for Passport registration**—To obtain a Passport, the following information is required: sign-in name, password, ZIP Code, e-mail address, country, region or city, and a secret question and answer the member chooses. Nickname, gender, age, preferred language, and purchasing information (such as credit card numbers and billing address) are optional.
- **Consumer control of information**—Passport members decide which sites they want to share their demographic information with by signing in to only those sites. Members have access to their information at all times if they want to review or change it.
- **Separate treatment of sign-in and billing/shipping information**—Passport separates members' sign-in information from their purchasing information such as credit card numbers and addresses. Only the demographic (sign-in) information is provided to a site when members sign in. Members grant permission to share their information when they click the Passport sign-in link on that site and sign in. Billing and shipping information is only transmitted to a site when members use the express purchase service.
- **Use of cookies**—Cookies are a simple, safe, and convenient technology. Passport's use of cookies allows members to minimize or eliminate the need to repeatedly sign in and register at participating sites, and it allows Microsoft to confirm that members have signed out successfully. When a member signs in to a Passport site, an encrypted cookie containing the member's sign-in name and basic demographic information is temporarily placed on their computer. A site-specific encrypted cookie is placed on the computer with each additional Passport site the member signs in to during the session. When the member signs out, all Passport-related cookies are deleted from the computer. As these cookies are deleted, Microsoft provides the member with confirmation that he or she has successfully signed out of each site.

Availability

Microsoft Passport services are available immediately and are currently in use at many leading Web sites. New participating sites are added frequently and are listed in the [Passport Site Directory](#). The Passport Implementation Overview and Software Development Kit (SDK) are currently available in English for interested businesses at <http://www.passport.com/business/>.

#####

*"Digital Wallets: Pursuing Dual Wallet Strategy Before Leverage Is Lost," Ken Cassar, Lucas Graves, Marc Johnson and Robert Sterling, Jupiter Communications. February 1999.

**The Children's Online Privacy and Protection Act, in effect since April 21, 2000, requires all child-oriented Web operators to obtain parental consent before collecting, using, disclosing, or displaying the personal information for anyone under the age of 13. The law also requires general-audience sites to follow these guidelines when the site has actual knowledge that the user it is collecting personal information from is a child.

The information contained in this fact sheet relates to a product that is subject to change at any time. Accordingly, the information may not accurately describe or reflect the current state of the product. The fact sheet is provided for informational purposes only, and Microsoft makes no warranties, express or implied, with respect to the fact sheet or the information contained in it.

Microsoft, WebTV and MSN are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries.

Other product and company names herein may be trademarks of their respective owners. **For more information, press only:**

Waggener Edstrom, **Rapid Response Team**, rrt@wagged.com, 503-443-7000

[For Consumers](#) | [For Business](#) | [For Press](#) | [International](#)

© 1999-2001 Microsoft Corporation. All rights reserved.
[TRUSTe Approved Privacy Statement](#) | [Terms of Use](#)

MS Passport: Straight to the FTC

By [Farhad Manjoo](#)

2:00 a.m. Aug. 16, 2001 PDT

Privacy advocates filed an updated complaint with the Federal Trade Commission on Wednesday charging that Microsoft's Passport service harms the privacy and security of "over 100 million" computer users, and that, consequently, it constitutes an "unfair and deceptive" trade practice.

[Passport](#) -- a "sign-in service" that allows Internet users to log on to participating services without re-entering information each time -- is integrated into Microsoft's upcoming Windows XP operating system. It is also central to Microsoft's own Internet services, such as Hotmail and MSN, and it is part of the company's [.Net initiative](#).

See also:

[Discuss this story](#) on Plastic.com

[Big News, or Windows Dressing?](#)

[XP Not Privy to Computer Privates](#)

[Microsoft's Mixed Bag](#)

[MS Scoffs at Windows Worries](#)

[Icons Cluttering Up Windows Space](#)

[Keep an eye on Privacy Matters](#)

The [new filing](#) (PDF) amends the groups' [July complaint](#) (PDF) to the FTC, in which they said that Passport's proliferation in Windows XP would allow the company to "profile" consumers online.

In the new filing, the Electronic Privacy [Information Center](#), [Junkbusters](#) and other privacy groups say that after tinkering with the system and reading a lot of press reports about XP, they found more objectionable things.

They discovered, for example, that "Passport provides no mechanism for users to cancel their account and permanently delete their personal information from Microsoft servers."

The complaint adds that people "who have requested that their personal information be removed from Microsoft servers have been told by the company they will have to wait one year for their accounts to expire" -- which the groups say is not acceptable.

They also state that "Microsoft is attempting to eliminate anonymity on the Internet to enable .Net, a distributed computing platform.... If unchecked, Microsoft's distributed computing platform will result in users being required to identify themselves to merely surf the Internet."

At a press conference at the National Press Club in Washington, Marc Rotenberg, EPIC's executive director, said that "it's not our goal to unnecessarily delay the launch of XP," but the fact that they have found all these problems with Passport indicates that "there might be a lot more here that we don't know about, which is why we need the FTC."

The FTC is only empowered to prevent "deceptive" practices on the part of companies. In their statements on Wednesday, the groups tried to explain why they thought Microsoft's privacy policies were unlawfully deceptive.

As Jason Catlett, the president of Junkbusters, put it: "They're saying it's going to be secure when it's not. They're plainly on the wrong side of the FTC act. They're collecting information under false pretenses by misleading consumers, and that's just illegal. They should be on the right side of trade practices law -- but that might sound like a lot to ask of a company like Microsoft."

Microsoft, naturally, disagreed. "Microsoft shares EPIC's views that privacy is important," spokeswoman Tonya Klause said, but the groups' complaints are "unfounded."

Responding to their specific concerns, Klause noted that the next release of Passport -- version 2.0, which will be out "within weeks" -- will feature an account-deletion feature. She added that Passport only asks for the barest of information from users -- an e-mail address and a user's country, state and zip code. All of the .Net services are completely "opt-in," she noted.

And to the extent that one of those extended .Net services (such as the online wallet service, called MyWallet) asks for more than an e-mail address and a zip code, "this information is completely private, secure, not mined, sold, rented, or ever used for secondary purposes. It's not mined at all, period."

Considering this, she said, the groups' comments "demonstrate a misunderstanding of the products, services and technologies that they're attempting to challenge. EPIC continually alleges unfair and deceptive trade practices when what's at issue, really, is a difference over the best way to implement privacy -- which is an ongoing discussion."

Klause's claim does have merit: Reading the groups' complaint, it is indeed possible to find instances where they misunderstand the technical issues, or exaggerate the nature of Microsoft's sins.

For example, the privacy advocates take issue with XP's support of digital rights management, which is a scheme built into the system to protect against the copying of audio, video and other copyrighted content.

"Microsoft concedes that this system will be used to monitor Internet users and [has stated](#) that XP will enable an 'aggressive Internet surveillance program ... that searches for unauthorized distribution of eBook content 24 hours a day, seven days a week,'" the complaint said.

But that citation is taken dangerously out of context -- it suggests that XP will monitor "Internet users," when in fact the entire paragraph (from a Microsoft site) says that an "intelligent Internet search tool" will scour the Internet for copied e-books. This type of thing might be anathema to free-loving Internet users, but it really doesn't have anything at all to do with Passport or XP.

Klause added that the groups didn't bother to look at the [sections](#) of the Windows Media Player privacy statement that describe Microsoft's anti-piracy procedures, which she insists do maintain a user's privacy.

When pressed, some of the privacy advocates admit that their quarrel with Passport is really more over its existence than its implementation. Catlett said he thinks Microsoft's current behavior is "deceptive" and, therefore, illegal. But even if the company does make the concessions privacy advocates are demanding in this complaint, "there would still be very large concerns over their very large database."

"You have to ask if it's possible to have a system like Passport that's secure," he said. "A better architecture would be one where instead of having all the personal information in some gigantic database, personal information is stored on someone's PC and only goes out when a person consents. There are architectures like that but MS didn't try to use it."

He said the central database "imposes a privacy risk, and when you add Microsoft's horrendous record on security, that's not a good thing."

But Klause said that a central database is necessary for some of the services being proposed for .Net. "Central architecture allows roaming and connectivity to the information on any device at any time," she said. "You should note, too, that individual PCs could never have the kind of security that you could implement on a database."

That's a statement with which many will disagree, but many things in computer security and privacy are up for debate, Klause said. "We welcome a frank and in-person dialogue with the privacy advocates who have to date not bothered to reach out to us," she added. "They seem intent on bringing their issues to the press. We share their concerns about consumer privacy."

But Catlett insisted that Microsoft's practices would be best curbed by a regulatory agency. "We hope that they will quickly order Microsoft to make some changes," he said. "I don't know how likely it is. The FTC is the de facto protector of privacy and if they drive past this bleeding corpse on the sidewalk, they're obviously asleep at the wheel."

Related Wired Links:

Microsoft Opens Its Windows

July 11, 2001

MSN: Some Chat, Others Chafed

July 10, 2001

Browser Blocks Ads and More

July 6, 2001

Real MS Verdict: Jackson Blew It

June 29, 2001

MS Breakup Order Reversed

June 28, 2001

MS Monopoly Vigil Intensifies

June 26, 2001

Explore.

To print: [Click here](#) or Select **File** and then **Print** from your browser's menu

This story was printed from [Enterprise](#),
located at <http://www.zdnet.com/enterprise>.

Your stolen Passport

By *Wayne Rash*, [Enterprise](#)

September 26, 2001 9:37 AM PT

URL:

The way Dave Thomas describes it, he and his staff were trying to track down a series of unusual bugs in Windows, when they stumbled across something that really worried them. There, on their screens along with the code they were debugging, was the name and password they'd just used for Microsoft's Passport service. Worse, it was in plain text, and readily accessible. As he looked more deeply, he realized that creating a worm that could recover that information would be, in his words, "trivial."

Thomas, who is CTO of the Oregon-based software quality assurance company, Bugtoaster, says that he wasn't really trying to get into the security business, but that this was something too obvious to let pass. It was also too important.

Microsoft's Passport service is a core piece of its .NET strategy. Anyone who uses MSN or the MSN Messenger has a Passport. As the Microsoft Internet strategy moves forward, the Passport will serve as a single sign-on for interactions with any company that requires Passport-based authentication, and Microsoft is working hard to sign up as many companies as possible. If Microsoft's plans reach fruition, users will only need to authenticate once with the Passport Data Center (run by Microsoft); then they can travel around the Internet, moving from one Passport-enabled service to another without having to log in again. This is a great convenience for users.

The problem is, it's also a great convenience for hackers and thieves. All they need is your e-mail address and password to go anywhere you go because Passport requires that you use your e-mail address as your user ID; and you use a single password for all Passport-enabled sites. Worse, because Microsoft is also tying its Wallet service to the Passport, they can also spend your money and get your credit card information.

The only upside (if you can call it that) to Bugtoaster's findings is that this particular security hole only applies to Windows 9x and Windows Me. Unfortunately, versions of Windows working off the NT code base are vulnerable, but for different reasons.

Windows 95/ME API reveals clear text

Bugtoaster's discovery is related to the Windows dial-up networking (DUN) application on the client side. An API that DUN shares with other applications retrieves the Passport credentials from an encrypted file. When a Windows 9x/ME user logs into the Passport Data Center, the API passes sign-on information in clear text from one process to another in memory where a worm could easily find the information because it's an area specified in the API for Windows.

While the API often passes log-in information to other services, such as your ISP, hackers with malicious intent have had no incentive to steal this information because there was little to be gained. With Passport and the carte blanche it's designed to give its users, the stakes are completely different.

Windows NT and 2000 don't have the clear text problem, but are still vulnerable

Windows NT and 2000 not totally safe either

One of the benefits of using a version of Windows based on the NT code base (NT, 2000, or XP) is that the API encrypts the log-in information before passing it. But that doesn't mean you're in the clear just because you're using NT or 2000. According to Steve Gibson of the highly respected security firm of Gibson Research, getting the same Passport sign-on information from those operating systems requires a different approach, but he also calls the process trivial. According to Gibson, it's a simple process to capture sign-on information from any version of Windows using a worm that can record keystrokes. Like the data that hackers could have snooped from the API, the only reason it hasn't been done in the past, he says, is that it wasn't worth the trouble.

Now, however, with Passport, the target is much more attractive. While it might have been pointless to get someone's ISP password, Passport opens up broad access to any site that uses it.

In a response to our questions, a Microsoft spokesperson, who requested anonymity, admitted that password information is passed in clear text within Windows 95 and ME when a user logs on to Passport or any other system. While Microsoft also recognizes that a worm, Trojan horse, or other hostile code could invade Windows and capture a user's sign-on information, the spokesman lays the blame on hostile code and not on any weaknesses in Windows 95, ME or Passport. "By design, a program running on a user's computer can in general take any action the user can," he writes in an e-mailed response. "The real issue here is hostile code, not Passport."

According to him, the company doesn't plan to make any patches to the vulnerable versions of Windows to help stop such theft of Windows sign-on information. "Microsoft will not be providing a patch for this because there is nothing to patch," he writes. "Once a user's machine has been hacked, no patch will keep the hacker from gathering the information he or she wants." Future versions of Windows will have security enhancements that prevent such access by hostile code, he said.

Unfortunately, there's not much individual users can do without support from Microsoft. Enterprise users, however, have some options. First of all, discourage the use of Microsoft's Passport services until you're satisfied that your security is protected. The most important way to protect your company is to check your firewalls, and make sure they're screening for unauthorized attempts to send information from any of your Windows computers. One very effective way to accomplish this is to use a personal firewall such as [Zone Alarm](#) from Zone Labs, which can actually block unauthorized attempts to access the Internet. That way, at least, a worm that captures your sign-on information won't have a way to send it out.

If you're a merchant on the Internet, or otherwise run a site that uses Passport, you have some additional concerns. First, you must address Passport's questionable security when you design your site, and make sure you require additional authentication to access personal or financial information. Second, you should be able to authenticate users who don't use Passport, or who don't wish to use it on your site. Finally, you should disclose up front what areas on your site users can access with Passport and other authentication methods, and what the site must authenticate itself.

Beyond that, however, the best thing you can do is to be scrupulous about password controls, educate your employees, and be suspicious of single-sign-on plans that you don't control. And, of course, hope that Microsoft decides to take these problems seriously enough to fix the problem with the current installed base of Windows instead of waiting until future versions are shipped.



LIBERTY ALLIANCE project

INDUSTRY LEADERS TO FORM NETWORK IDENTITY ALLIANCE - LIBERTY ALLIANCE PROJECT

Representing Over a Billion Names, ActivCard, American Airlines, the Apache Software Foundation, Bank of America, Bell Canada Enterprises, Cingular Wireless, Cisco Systems, CollabNet, Dun and Bradstreet, eBay, Entrust, Fidelity Investments, Gemplus, GM, Global Crossing, I2, Intuit, Liberate Technologies, Nokia, NTT DoCoMo, Openwave, O'Reilly and Associates, RealNetworks, RSA Security, Sabre, Schlumberger, Sony Corporation, Sprint, Sun Microsystems, Travelocity, United Airlines, Verisign, Vodafone and More Create Multi-Industry Business Alliance

Projectliberty.org Goes Live; All Interested Parties Invited to Drive Specification and Development Process

ProjectLiberty.org - September 26, 2001 - In an unprecedented collaboration between some of the world's largest businesses and industries, representing over a billion customers, employees and business partners, 33 major companies announced today the formation of an alliance, code named Liberty Alliance Project (www.projectliberty.org). The alliance will develop and deploy an open solution for network identity.

The charter members of the Liberty Alliance Project, representing a broad, global spectrum of industries, intend to create an open, federated solution for network identity - enabling ubiquitous single sign-on, decentralized authentication and open authorization from any device connected to the Internet, from traditional desktop computers and cellular phones through to TVs, automobiles, credit cards and point-of-sale terminals. The alliance represents some of the world's most recognized brand names and service providers, driving products, services and partnerships across a wide range of consumer and industrial products, financial services, travel, digital media, retailing, telecommunications and technology.

Any organization interested in supporting the Liberty Alliance Project can visit www.projectliberty.org for details. The Liberty Alliance Project plans to begin immediately in setting out a roadmap to address business practices, privacy, consumer adoption and technology evolution.

"It's recently become clear that the software for managing user identity and authentication is one of the key building blocks of the emerging Internet operating system," comments Tim O'Reilly, founder and CEO of technology publisher O'Reilly & Associates and an activist for open source software and Internet standards. "It's so fundamental that a widespread consensus has emerged that this is a technology that shouldn't be owned or controlled by any one player. Instead, we need an open, distributed system with implementations available from multiple technology providers and identities issued by many parties operating in a web of trust. Project Liberty is an important step in that direction. I'm hopeful that it will provide a forum for interoperability between the proposed identity schemes available from individual software or service vendors."

"Security and identity are facets of almost every big issue in the digital world today," said Esther Dyson, chairman of EDventure Holdings, and former chairman of ICANN, an organization that sets policy for the Internet's infrastructure, including the Domain Name System. "They touch it all: privacy, anonymity, integrity of data and safety of assets, freedom of speech, legitimacy, trust and trust worthiness, branding, visibility of marketers and visibility to marketers. Therefore, it's important for individuals to have a convenient way to identify themselves (and their counterparts)."

The Liberty Alliance Project has three main objectives:

1. To allow individual consumers and businesses to maintain personal information securely.

This enables a decentralized approach to garnering personal or proprietary information, and promote interoperability or service delivery across networks.

2. To provide a universal, open standard for "single sign-on," which users and service providers can rely upon, and leverage to interoperate.

Internet single sign-on will allow users to log in once, and be authenticated for a spectrum of network services supporting the Liberty standard, between and among web sites, as well as network services even if those services are provided by different businesses.

3. To provide an open standard for network identity spanning all network-connected devices.

This allows providers of network services, and the infrastructure that enables them, to adopt a neutral, open standard, available wherever the Internet is available, to enable secure and reliable identity authentication across handsets, automobiles, credit cards - literally any device attached to the Internet.

PRESS ROOM ■

FAQ's ■

MEMBERSHIP ■

INTEREST ■

About the Liberty Alliance Project

The Liberty Alliance Project (www.projectliberty.org) is an organization being formed to create an open, federated, single sign-on identity solution for the digital economy via any device connected to the Internet. Membership is open to all commercial and non-commercial organizations.

Note: Liberty is a code name for this formative initiative. The charter members expect to finalize an alliance agreement regarding organization and joint development of intellectual property within the next 60 days.

###

Company names mentioned herein may be trademarks of their respective owners.