

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-intense 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).