

**Subject:** Perspectives of the Center for Democracy and Technology  
**From:** Ari Schwartz, Center for Democracy and Technology, 202-637-9800,  
ari@cdt.org  
**To:** Internet Caucus Advisory Committee

**P3P and Privacy: An Update for the Privacy Community**  
Tuesday March 28, 2000 by\*

The Center for Democracy and Technology, Deirdre Mulligan & Ari Schwartz  
and  
Information and Privacy Commissioner/Ontario , Ann Cavoukian PhD. & Michael Gurski

## Introduction

The Platform for Privacy Practices (P3P) is not a panacea for privacy, but it does represent an important opportunity to make progress in building greater privacy protections in the Web experience of the average user.

P3P is simply a standard or specification currently under development at the World Wide Web Consortium (W3C). That specification, when implemented in Web sites and browsers, will bring a measure of ease and regularity to Web users wishing to decide when and under what circumstances to disclose personal information. The barrage of privacy issues that bedevil the Internet can be partially addressed with the widespread adoption of the P3P specifications. It offers an important opportunity to build greater technical support for privacy-informed Web users and supports a catalyst on the part of Web sites seeking to incorporate privacy protections into the Web's infrastructure.

While the development process has progressed, companies and privacy advocates have attacked it from many sides for more than two years. For example, two Citibank employees issued a paper expressing a concern that P3P might "let ordinary users see, in full gory detail, how their personal information might be misused by less trusted or responsible web site operators. Such knowledge may cause users to resist giving out information altogether. Some individual business groups have done focus studies on users, and, though the results deserve further study, some concluded that most users would prefer to give out only information needed for the transaction and that they do not like the idea of someone monitoring their browsing behavior." [1] Meanwhile others, such as Karen Coyle, are concerned that P3P might oversimplify and quite possibly misrepresent "the trust interaction, and always in favor of the web site that is asking for an individual's information." [2] Still others, like Jason Catlett, have conducted a premature post-mortem, suggesting that P3P will never be adopted by the critical mass of Web sites necessary to have an impact. Or that, even if adopted, it would be nothing more than an attempt by industry to maximize the collection of consumer data over the Internet. [3]

These various, often contradictory, views of P3P are understandable for two reasons. First, some have over-hyped the standard, claiming that P3P will, on its own, fully address privacy concerns. Second, the development of the specifications has been a lengthy process during which the initial proposal has undergone significant and often confusing changes.

While these concerns have varying degrees of legitimacy, as privacy advocates involved in the P3P process, we have committed ourselves to supporting the development of P3P understanding its strengths and limitations. P3P needs a regulatory or policy context to help protect privacy, it cannot do this by itself. More importantly, it is not, and should not be viewed or trotted out as a reason to discourage regulatory or self-regulatory efforts to protect privacy. As we suggest in this paper, P3P is a means of enabling Web sites to regularize their privacy vocabulary and bring these privacy policies front and center for the Web user's consideration. In other words, we have chosen to work on P3P because we seek to promote greater transparency. In our opinion P3P does not protect privacy, in and of itself. It does, however, help create a framework for informed choice on the part of consumers. Any efficacy that P3P has is dependent upon the substantive privacy rules established through other processes — be they a result of regulatory, self-regulatory or public pressure.

It is our hope that privacy rules continue to be debated and developed, as they traditionally have, through democratic publicly-accountable processes. Individuals and businesses hoping to protect privacy solely through the P3P specification would be wise to review the Fair Information Practice Principles. A quick read should convince even the most optimistic of P3P supporters that P3P is neither designed nor suited for addressing all critical elements of privacy protection. Similarly, individuals who criticize P3P or suggest abandonment should be careful what they wish for. We do not want specification and standard settings bodies determining public policy. W3C does not wish to become the forum for public policy debates. We don't want to cede the development of substantive policy to technical organizations. However, to the extent that we can work with the technical community to build platforms and standards that support our social policies surely we should pursue such opportunities.

Many criticisms have been made regarding the delays in bringing P3P to fruition. Specifications like P3P take time. From its inception P3P was envisioned as a specification with a social purpose. As participants, we believe that the P3P process has been deliberative and thoughtful. W3C and the P3P working groups have actively solicited comments from all interested parties. We have met with interested parties across the spectrum and across the globe. We have sought out and engaged critics on all sides. We believe that doing so is critical to P3P's success, and will continue to do so. This outreach has taken time and effort. Everyone has his or her own agenda and perspective that can be misinterpreted as unnecessarily delaying the process. As advocates we continue to push for the timely finalization of the specification and the future development of P3P.

Part of the task has been to build a common vision and move forward. The Guiding Principles behind P3P embody that vision. The specification is the expression of 'intent' that counts in the P3P process. The Guiding Principles attest to P3P as an effort at bringing Web site privacy policies to the foreground, and to help Web users make informed decisions regarding the disclosure of personal information. We are committed to ensuring that P3P implementations are true to this intent.

While the use of P3P for political purposes and the length of the development period must be monitored, in the end, our greatest concern is that a specification designed to promote greater transparency and support individual choice regarding privacy may die before a single implementation comes to market.

This paper explains where P3P is in development and is a call to all who would like to see privacy on the Internet grow to:

- become directly involved and work to improve the current specification,
- vigilantly watch implementations,
- and, assuming that all goes well, ultimately support P3P's final recommendation to the W3C.

### What is P3P?

Today, P3P is a sleeker, simpler specification than initially proposed. The original P3P specification contained three integrated features: 1) a vocabulary and specification for making privacy statements; 2) a protocol for negotiations between the individual and the Web site over privacy statements; and 3) a standard for storing personal information and controlling its transfer pursuant to 1 & 2. Combined, these features provided an overall framework for automating privacy decisions for Web users and Web sites and transferring personal information. These features were discussed and debated for over 2 years. In the mean time products emerged to help consumers store and manage their personal information. The P3P specification group decided to eliminate the data transfer and negotiation components of the specification and focus on the part of the specifications needed for Web sites to make machine readable privacy statements and deploy client side tools to decipher them for consumers.

P3P 1.0 creates the framework for standardized, machine-readable privacy policies, and consumer products that read these policies. Like all specifications many critical decisions are in the hands of developers. However, the Guiding Principles that inform both the development and use of P3P tools directs builders and users on issues that the P3P working group felt were critical to the soundness of P3P and its purpose. Within the confines of the specification and the Guiding Principles, P3P allows innovation. We hope that tools that read and compare privacy policies as directed by consumers will come to the market. Eventually we hope that other features — such as a way to verify and repudiate policies — can be added to the specification, but for now the purpose of P3P is simply to advance transparency by making notices machine readable.

P3P is in "Last Call" at the W3C with an open invitation at their Web site to comment. Many concerns and suggestions have already been shared. For these we are very grateful. But we need more comments, suggestions and criticisms. The specification is in last call to the end of April, the public still has a chance to comment while implementations are being developed. When this period ends and a few successful implementations have been created, the W3C will vote on recommending it as a Web standard: P3P 1.0. Therefore, there is still time to improve the specification and monitor the implementations as they are created. Details about the public comment period conclude this paper. [4]

### How P3P 1.0 Will Help Protect Privacy

- ***P3P can help standardize privacy notices***

On a P3P 1.0 enabled Web, all privacy policies will have the same basic machine-readable fields that will express a company's privacy practices. While this does not offer privacy protection, if implemented, it could greatly advance transparency and be used to support efforts to improve privacy protection. As stated above, it does not address the full range of privacy considerations. But, it is designed to facilitate the exchange of information about privacy policies in a fashion that maps on to the Internet. P3P does not preclude the use of other technical or legal means of protecting privacy. In fact, the working group has sought input from both builders of privacy enhancing tools and those responsible for implementing and enforcing privacy laws. P3P is just one stone in the foundation. It needs to be used in concert with effective legislation, strategic policy and other privacy enhancing tools. For example:

1. Countries with data protection and privacy laws and others seeking to police compliance with privacy standards could find the automated ability to assess a businesses' privacy statement useful in their broader oversight and compliance program. — Searching and gathering privacy policies could be simplified through P3P. P3P would allow the policies to be collected and analyzed in a standard machine-readable format. Governments and organizations would be able to simply search through P3P statements to find companies whose notice does not meet privacy standards in various areas. In the current version of P3P, companies could even point to regulatorybodies that oversee them to help route privacy complaints.
2. Users could more easily read privacy statements before entering Web sites. — Today, it is often difficult to find privacy notices. Once found, they are frequently written in complicated legalese. P3P implementations could allow users to assess privacy statements prior to visiting a site, and allow users to screen and search for sites that offer certain privacy protections.
3. Cutting through the legalese — A company's P3P statement cannot use difficult to understand or unclear language. The standardization and simplification of privacy assertions into statements that can be automated will allow users to have a clear sense of who does what with their information.
4. Enterprising companies or individuals could develop more accurate means of rating and blocking sites that do not meet certain privacy standards or allow individuals to set these standards for themselves. Several companies already rate and block Web sites that do not meet certain privacy standards. Today, creating the tools and knowledge that support these products is difficult and time consuming. By providing an open standard, P3P 1.0 could enhance the transparency, accuracy and detail of existing products, and could encourage an influx of new privacy enhancing products and services.

***P3P can support the growth of more privacy choices, including anonymity and pseudonymity***

Full anonymity is an important protection for privacy on the Internet. The ability to use the Internet with a pseudonym is also critical. These options must be supported and promoted. However, with anonymity or pseudonymity a person would be hard pressed to be involved in the full diversity of interactions occurring on the Internet. For privacy to be part of the

Internet infrastructure, we must deploy tools that assist individuals in controlling personal information when they choose to, or need to, disclose it. P3P 1.0 can be used with anonymity tools to allow users to have more control over their personal information. A user should be able to be anonymous in one context and identifiable in another. The ability to have Web sites' privacy notices parsed and interpreted by a privacy tool can assist individuals decision-making regarding when and to whom to disclose personal information. Today, reading policies is a time consuming, cumbersome and sometimes impossible task. P3P 1.0 would help change that.

### **What P3P Will Not Do:**

#### ***P3P cannot protect the privacy of users in jurisdictions with insufficient data privacy laws***

The W3C is a specification setting organization; it does not have the ability to create public policy nor can it demand that its specifications be followed in the marketplace. While different members of the W3C may have different reasons for engaging in the process nothing in the P3P Specification or the P3P Guiding Principles presumes that P3P is designed to replace public policy or a public policy process. Accordingly, P3P is designed to allow for statements about data practices, which are in turn directed by law, regulatory procedures, self-regulation or other forces.

We believe that better data privacy laws and further self-regulatory efforts are necessary to protect consumer privacy internationally. As privacy advocates, we believe that — armed with more information — individuals will seek out companies that afford better privacy protection. Recent consumer pressure on companies that collect personal information like there is no tomorrow, show that the public will act to protect their privacy if given simple, practical tools and advice to aid them. It also shows that companies can be made to moderate or reverse their policies and practices, if only temporarily. P3P can and should be used in concert with public policy to help protect privacy.

#### ***P3P cannot ensure that companies follow privacy policies***

If a company says that they are going to do one thing and does something else, no technological process can stop them. Deception must be stopped through public policy processes, legislation and the courts. Even in the United States, a country with limited consumer privacy protections, the Federal Trade Commission has brought cases against companies that do not follow posted privacy policies.

P3P would make privacy policies transparent. It does not ensure that the policies are followed. No technological process can ensure that companies comply with law or statements they choose to make. But, P3P will lead to greater openness, more informed Web users and therefore greater accountability.

### **Why Do We Support the Development of P3P?**

Even the best possible P3P1.0 implementation will not bring instant privacy protection to the Web. But it will bring clear progress. It will also inform the privacy debate by providing focus on Web sites and their privacy policies

Suffice it to say that establishing the technical terms for a social protocol is a complicated matter. P3P, in attempting to provide an automatic, common Web language to describe the collection and use of personal information, has been grappling to find a way to do just that. Much work remains to be done. Many members of the computer industry believe that P3P will increase consumer trust. They have donated time and effort to P3P. The Center for Democracy and Technology and the Office of Information and Privacy Commissioner/Ontario — along with other international privacy advocates, such as Joel Reidenberg of Fordham University and Marit Kohntopp of the Office of the Privacy Commissioner Schleswig-Holstein — have chosen to commit resources to P3P because we believe it is a component of improved privacy practices on the Internet. We intend to ensure that privacy remains the top priority in the drafting of the P3P specification and the deployment of products built upon it.

If, after the P3P vocabulary is completely stable, there few or poor implementations, we will step back from P3P. However, we will do so with the knowledge that P3P's failure was not from our lack of effort.

Even with P3P, countries with lesser protections must strengthen their Laws. Yet standardized machine-readable privacy policies will still be an important tool for Internet users. With a little commitment and leadership from the privacy community, we can make P3P a step towards building privacy into the global Web architecture.

We encourage you to join us as we move forward. To do so, simply read the most recent version of the specification at: <http://www.w3.org/TR/P3P/> and send your comments to: [www-p3p-public-comments@w3.org](mailto:www-p3p-public-comments@w3.org)

### Endnotes

\* CDT and the Office of IPC/Ontario are members of the P3P Policy outreach working group at the W3C. This paper represents only the viewpoints of the two organizations and is not an official document of the working group of the W3C.

[1] [http://www.w3.org/P3P/Lee\\_Speyer.html](http://www.w3.org/P3P/Lee_Speyer.html)

[2] <http://www.kcoyle.net/p3p.html>

[3] <http://www.junkbusters.com/standards.html>

[4] W3C members who would like to become more actively involved can join the P3P working groups.

**Subj:** Online Privacy: Perspectives of Information Technology Association of America  
**From:** Mark Uncapher, Vice President, ITAA, 703-284-5344, muncapher@itaa.org  
**To:** Internet Caucus Advisory Committee

Excerpt From ITAA Online Privacy Statement: Internet Regulation & Digital Opportunity

***Technology***

***Technological solutions will give consumers even greater flexibility to exercise their privacy preferences. The Platform for Privacy Preferences or "P3P" being developed by the World Wide Web Consortium at the MIT Laboratory for Computer Sciences is new browser technology that would allow consumers to set their privacy preferences online. The browser would then automatically query online sites to determine whether those preferences are being met. This is an industry-supported initiative that is seeking to use technology to empower consumers to an even greater extent than they are already.***

Similarly the introduction of new computing appliances will change the way consumers access the Internet. As a result we caution against regulations that assume the continuation of a Personal Computer based technology model. For example, consumers are likely to access hand held or automotive devices differently than the PC. Rules intended for PCs could inhibit this innovation.

---

<sup>1</sup> See <http://www.w3.org/P3P/>

**Subj:** Online Privacy: Perspectives of Microsoft  
**From:** Bill Guidera, Microsoft, 202-263-5914, bguidera@microsoft.com  
**To:** Internet Caucus Advisory Committee

### **Creating Technologies for Privacy in the Online World: Microsoft's Commitment to P3P Fact Sheet, May 2000**

Microsoft Corp. has committed to developing business and consumer tools based on the P3P standards specification. These tools will be a significant advancement for Web sites and consumers in promoting better communication and understanding of how Web sites collect and use personal information. Web site operators will find it easier to write privacy statements that are comprehensive, easy-to-find and compliant with fair information principles. Consumers will have more information for making decisions about sharing information with Web sites based on their personal preferences.

The business tool, tentatively called the Privacy Statement Manager, will enable Web site operators to describe the site's privacy practices, following the fair information principles of notice, choice, access, security and enforcement. The operator will use this service to create a privacy statement that is not only text-based (human-readable), but which also creates an Extensible Markup Language (XML) document that is machine-readable. This will be available as a free service on [www.microsoft.com](http://www.microsoft.com).

The consumer tool, tentatively called the Privacy Choice Manager, will enhance a consumer's ability to select the personal information privacy preferences that are most meaningful to him or her in a flexible but comprehensive way. Each consumer will be able to select preferences concerning the collection, use and distribution of their personal information. Microsoft will develop the Privacy Choice Manager as a "proof-of-concept" browser-helper object. Microsoft will investigate market acceptance and the best opportunity to integrate the Privacy Choice Manager into upcoming releases of Microsoft® products.

The P3P standards are what tie all of this together. With both the Web site privacy practices and the consumer's preferences expressed in a standard vocabulary and syntax, the Privacy Choice Manager can compare and evaluate policies and individual preferences to help the consumer make better informed decisions about sharing personal information.

Once a consumer has run the Privacy Choice Manager and connects to an Internet site that has posted its privacy statement as an XML document, a couple of things will happen. First, the consumer's machine will find the privacy statement and compare the Web site's practices with the consumer's preferences. If there are any mismatches, the application will provide feedback to the consumer, specifying where their preferences and the Web site's practices don't agree and warning the user that they may not want to provide personal information to that site. If there are no mismatches, the tool will signal to the consumer that the Web site is compliant with their personal preferences.

A significant feature of these P3P-based tools is their interoperability. Microsoft strongly encourages other companies to develop similar P3P-based tools for their products in order to provide the broadest consumer benefit. Microsoft will participate in W3C interoperability-

testing events in June and September 2000 to demonstrate the functionality of the tools and ensure that they interoperate with tools from other companies.

**About Microsoft**

Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to empower people through great software — any time, any place and on any device.

#####

Microsoft is a registered trademark of Microsoft Corp. in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

**For more information, press only:**

Tonya Klause, Waggener Edstrom, (703) 757-4501, [tonyak@wagged.com](mailto:tonyak@wagged.com)

Rapid Response Team, Waggener Edstrom, (503) 443-7000, [rrt@wagged.com](mailto:rrt@wagged.com)

**Subj:** Online Privacy: Perspectives of Online Privacy Alliance  
**From:** Tim Lordan, 202-638-4371, tim@privacyalliance.org  
**To:** Internet Caucus Advisory Committee

## RULES AND TOOLS FOR PROTECTING PERSONAL PRIVACY ONLINE

What is online privacy? Online privacy gives you the power to control the release of personal and financial information over the Internet. Although there are new developments every day to help you protect your privacy, *right now* there are many things you can do to protect the personally identifiable information that is gathered about you when you surf and shop online.

First, follow some common sense rules online that will help you protect your privacy and the privacy of your family. Then, check out the growing range of new technological tools available to help you to control the information you share, surf anonymously and remove your name from e-mailing lists.

### Rules to Remember for Protecting Personal Privacy:

- **Look for a privacy policy** on every Web site that asks you to register or provide information. Take a minute and carefully read the policy. A credible privacy policy should be easy to find and easy to understand. Most ethical Web sites put a link to a privacy policy right on the home page. The policy should tell you exactly what information a Web site collects and what it is used for. If the Web site shares the information with anyone else it should tell you and give you the option of restricting such use. A privacy policy also should tell you about the security used to protect your personal information and how you can look at the information that is collected about you. These days, all consumer Web sites that treat information ethically have privacy policies. Look for them and use them. If you don't find a privacy policy, email the Web site and ask them to post one.
- **Look for a privacy seal** . These seals, which are a recent innovation, give assurance that a Web site is abiding by its posted privacy policy. BBB*OnLine* (a subsidiary of the Council of Better Business Bureaus) and TRUSTe seals provide a mechanism to handle complaints by consumers who feel their privacy has been violated. The seals also mean a company has instituted systems for practicing what it preaches about privacy protection. If you don't find a seal at a Web site, write to the site and ask for one.
- **Do not under any circumstances give your password to anyone** . Hackers and scammers often try to entice you to give you password through a variety of tricks. Be careful. Use different passwords at different Web sites and change your passwords every now and then.
- **Use a secure browser** that complies with an industry security standard, such as Secure Sockets Layer (SSL) that encrypts or scrambles purchase information.

- **Print a copy of your purchase order** and confirmation number for your records when shopping online. Other tips are available at [www.bbbonline.org](http://www.bbbonline.org) and at [www.truste.org](http://www.truste.org).

## PRODUCTS AND SERVICES

The market for privacy protection products is growing and companies are responding with a host of technological tools and services. One of the changes expected to have significant impact is the **Platform for Privacy Preferences (P3P)**, being developed by the World Wide Web Consortium. P3P will allow surfers to communicate their preferences in sharing personal information with Web sites. With P3P, your Internet browser could review a company's privacy policy electronically and issue you a warning if it can't find a privacy statement. It will also alert you if the Web site wants more information than you have indicated a willingness to disclose.

Other "privacy" products work in different ways. Some of these are available free and many can be downloaded. Here is a partial list of those that are available now or expected to be offered in the next few months.

*The Online Privacy Alliance does not endorse any of these tools, but encourages you to review what's available and decide which product and/or service best fits your needs.*

## ANONYMIZERS AND INFOMEDIARIES

Tools for protecting privacy can be divided into two kinds; those that work to shield your identify and those that help you negotiate with a Web site over what personally- identifiable information is shared. **Anonymizers** make you "anonymous" by giving you an untraceable alias. While a useful tool for some consumers, anonymizers can protect lawbreakers. As *The New York Times* wrote: "The technologies are morally neutral. They could be used, for example to commit a crime or to report one anonymously."

**Infomediaries**, a new and relatively untested technology, allow you to exercise choice in what sorts of personal information is shared at each site you visit. They require that you create a detailed personal profile to enable the technology to negotiate the release of personal information on your behalf.

Services also exist for removing your name from online mailing lists and directories. Get more information from: [www.junkbusters.com](http://www.junkbusters.com), [help@infoUSA.com](mailto:help@infoUSA.com) and [help@bigfoot.com](mailto:help@bigfoot.com).

**Anonymizer** products include:

**Anonymizer**, one of the best-known and oldest products, allows you to surf anonymously. It also offers anonymous email and Net access. Visit [www.anonymizer.com](http://www.anonymizer.com).

**Freedom** from the Canadian company, Zero Knowledge Systems, will charge \$50 a year to provide up to five online aliases and allow anonymous profiles. Because the Montreal-based company does not have to follow U.S. law, Freedom can use stronger

encryption than similar American products. Not even Zero Knowledge can trace surfing, posting or chat room visits back to the user. It will be available later this spring.

**Crowds**, developed by Bell Labs and AT&T Labs, uses a virtual "crowd" of people to hide your identity while Web surfing. Users are placed in random groups and each time you instruct a browser the command is randomly routed through the machine of someone else in the group so that it is impossible to track a group member individually. Information on Crowds is available from the AT&T Web site at [www.research.att.com/projects/crowds](http://www.research.att.com/projects/crowds).

The **Onion** routing system, under development by the Naval Research Laboratory, keeps third parties from tracking your surfing activities by randomly routing messages through a series of routers before the message reaches its destination.

Among the new **infomediary** products being offered are:

**DigitalMe**, a software product that will be available soon from Novell, stores your personal information and uses it to automatically fill out forms at Web sites, letting you review them before they are submitted. The software, available by download in June, will keep track of your passwords and names used from site to site. Check out the new product at [www.digitalme.com](http://www.digitalme.com).

**Jotter**, a new desktop tool bar, allows you to employ an automatic form for shopping online, reminds you of your IDs and passwords and locates privacy policies on Web sites so that you can see how a company or organization handles personal data. Information on the new product can be found at [www.jotter.com](http://www.jotter.com). The software can be downloaded free from the Web site.

**Lumeria** hides individually identifiable data and then allows you to charge companies to see it. This California-based company believes that if personal information is valuable to businesses then they should pay for it. Information on the product can be found at [www.lumeria.com](http://www.lumeria.com). The free portion of the new service can place you on a "do not contact" list for direct marketers. Lumeria also allows you to surf anonymously by providing inaccurate "cookie" information to Web sites.

**Persona** by PrivaSeek will allow you to surf anonymously and also "sell" your personal information in exchange for discounts at Web sites. PrivaSeek, [www.privaseek.com](http://www.privaseek.com), will get a commission on the transactions. It will be available soon.

### SECURE SERVERS and BROWSERS

Most Web sites offer some protection for sensitive account information, but to be safe you should shop at sites with one of two security methods: Secure Electronic Transfer Transaction or Secure Socket Layer. Both Netscape Navigator and Microsoft Internet Explorer can hook into these standards.

**Secure Electronic Transfer Transaction** (SET) works by using encryption to safeguard your credit card information while it's traveling over the Web. It also uses digital

signatures to ensure the identity of both you and the merchant. One advantage of SET is that your credit card number is not stored in the merchant's browser.

**Secure Socket Layer (SSL)** creates a secure connection for transmitting documents and information such as credit card numbers over the Internet. It is fast and easy for Web sites to set up. SSL may become the accepted standard for Web based transactions that require a high degree of security.

It is easy to tell if you're using a secure site, just look for an "s" on the end of the "http" in the site's Web address ("https"). The "https" will appear when you are on a screen that asks for your account information.

A recent development is **secure HTTP (SHTTP)** a secure method for transmitting individual messages, such as email, over the Web. This differs from SSL and SET, which are primarily used for doing business at Web sites.

For additional information about how to protect your privacy, check out the Call for Action Web site, [www.callforaction.org](http://www.callforaction.org) where they have posted the ABC's of Privacy.

**Subj:** Online Privacy: Perspectives of Privacy Right  
**From:** Paul Sholtz, Chief Technology Officer, PrivacyRight Inc., c/o Amy Hanson, 703-299-9470  
**To:** Internet Caucus Advisory Committee

### Technology Tools and Privacy Empowerment

Empowering individual privacy begins with strong cryptography. Cryptography is used to prevent eavesdropping by randomly scrambling documents and communications. The intended recipients of the information are given the keys decipher the message, which is unintelligible to everyone else.

Some examples of strong cryptography for consumer user include Pretty Good Privacy (PGP), a secure email program developed by Phil Zimmerman and SSL, the secure networking protocol developed at Netscape that powers most secure Web browsers and servers on the Internet.

Ultimately, privacy is also a matter of policy. If an organization collects information about an individual without the individual's consent, or if it uses the information in a way inconsistent with the individual's preferences, a privacy violation has occurred. The Code of Fair Information Practices outlines a set of constructive data practices for organizations that maintain consumer information databases. PrivacyRight is working to bring the CFIP to the Web through hosted data management solutions.

**Subj:** Online Privacy: Perspectives of Barbara Bellissimo, Privada  
**From:** Barbara Bellissimo, Privada, c/o Software & Information Industry Association (SIIA), Ted Karle, 202-452-1600, tkarle@siaa.net  
**To:** Internet Caucus Advisory Committee

### **Protecting Online Privacy: Safeguarding Business and Consumer Transactions**

**Although Web surfers can find a wealth of information online, Web sites can also gain a wealth of information about site visitors – regardless of whether or not the visitors want to share the information.**

**By Barbara Bellissimo, Privada**

In today's networked society, consumers and businesses are increasingly able and eager to access information, buy and sell products and conduct research online. What many people don't know is that the flow of information often goes in two directions. Although people can obtain almost unlimited quantities of information from the Internet, they are also vulnerable to disclosing their own personal data unwittingly. Some consumers and businesses have recognized this danger and have shied away from the Internet because of its security and privacy flaws. With the many different resources on the Internet, it remains difficult to determine which sites are trustworthy, provide anonymous services or protect their customers' privacy.

Without the ability to protect their personal information, consumers will continue to be reluctant about purchasing goods and services from the Internet, and the promise of Internet-based electronic commerce will not be fully realized.

### **Privacy Concerns and Usage Hazards**

Consumers should be in control of who has access to their personal information as they roam the Internet. However, there are currently three common areas where consumers can experience breaches in privacy. These areas include surfing the Internet, sending e-mail and purchasing goods and services online.

Once a consumer logs onto the Internet, there are many ways personal information can be collected and used. Some Web sites can obtain personal information from surfers via "cookies." Cookies allow Web servers to recognize a specific user or machine used to access that Web site. The cookie file is stored on the user's computer and read by the Web server during each subsequent visit to the Web site. Although most Web browsers allow users to turn off the cookie feature, many Web sites cannot provide access or personalized services unless cookies are accepted. The information collected in a cookie can then be used for direct marketing efforts without the consumer's knowledge.

When consumers log onto a Web site, site administrators can often learn their e-mail address, which operating system they use, their computer name, browser type, plug-ins installed, the date and time on the system and even personal data on the person in charge of the domain name. Armed with this

information, companies can create a profile of consumers and track the sites they are visiting, all without consumers' permission. This type of tracking would never be tolerated in the real world as shoppers wander from store to store.

The rapid growth of electronic commerce adds to the complexity of the privacy problem. Online shoppers must provide their address, credit card and other personal information to purchase and receive products and services. Consumers often find that their personal data is collected and used for market research, direct marketing and other purposes once they've bought products online. Sometimes this leads to annoying dinnertime telephone calls pitching products related to those they've purchased online or expressed an interest in by browsing a site.

When individuals send e-mail, their names and e-mail addresses can be collected, recorded, checked against other records and added to their "profiles." Additionally, the e-mail content itself is anything but confidential. The data that companies may gather on individuals can be sold to third parties or shared with partners, allowing these aggregators to associate credit card numbers, reading habits, Web site usage patterns and more. These data are collected, stored and accessed by companies to improve target marketing and advertising efforts. Marketers use data many people would rather keep secret, such as how much they earn, where they shop and what they buy.

### Privacy Concerns to Businesses

It has become a sound business practice for online companies to adopt a privacy policy to assure consumers about the protection of personal information, while building confidence and long-term customer relationships. In addition, businesses need a degree of anonymity to protect themselves, their employees and their constituents. Just as consumers don't want to be deluged by marketers, businesses cannot afford to lose customers and employees because they're unable to ensure the privacy of these groups. Privacy is currently a market issue, not a regulatory one, so it's in a business' best interest to differentiate itself by safeguarding the privacy of its customers and employees.

Many corporations are seeking privacy solutions to ensure that they can conduct internal communications and competitive research safely and anonymously. By offering their employees online anonymity, businesses may protect themselves from potential lawsuits brought on by employees misusing their Internet access. There are also situations – specifically in the medical and pharmaceutical industries – where corporations can expand their reach by providing sensitive information to individuals without any knowledge of the recipient's identity.

### Privacy Protection Levels

There are several ways to safeguard consumer and business privacy in cyberspace. These methods can be divided into two categories: privacy given by Web sites and privacy taken by Web surfers.

With few laws regulating the types or amount of personal information Web sites can capture,

some groups are voluntarily providing their constituents with a private and safe online environment. The Direct Marketing Association (DMA) has attempted to regulate Web sites by creating privacy-policy guidelines for both traditional and online database marketers. DMA members are required to abide by its guidelines. In addition, TRUSTe, a private organization formed in 1997, governs Web sites in an effort to make privacy a structural and technological component of the Internet. It seeks to create a branded symbol of trust on the Internet using seals of approval. TRUSTe is also a part of the Online Privacy Alliance, which encourages adherence to sets of self-regulating principles aimed at protecting personal information. TRUSTe works to raise awareness and educate the Internet community and promote the values of full disclosure and informed consent.

However, even though Web sites are forcing themselves to create these online disclosure statements with certification badges, privacy is not necessarily guaranteed. Many believe the Internet is too broad and changes too quickly to be policed effectively.

Consumers can take personal steps to avoid providing personal data by making good choices about what data they disclose voluntarily and reading the privacy policies of the Web sites they visit. However, Web surfers need to remember that many privacy policies are intentionally vague and are not always fully implemented.

Without assurances from Web sites, many consumers are taking control of protecting their online and real-world identities. The most basic method is simply creating a fictitious persona for online use, avoiding providing credit card information to unfamiliar Web sites and using a free e-mail account for online shopping, saving personal e-mail accounts for friends and work associates. Consumers should also encrypt e-mail messages whenever possible.

There are also services known as re-mailers. Anonymous re-mailers are free Internet services allowing users to send e-mail without disclosing their names or addresses. The re-mailer will strip the user identification material from the message and re-send it. This technique is not totally private, however; the re-mailer knows the user's information and unless a message is encrypted can read the e-mail. The re-mailer could, under various laws, be forced to reveal the identity of a user.

There are, however, reliable ways to safeguard consumer online identity while Web surfing, shopping and communicating by e-mail. Companies and individuals seeking these reassurances should consider using privacy-enhancing technologies (PETs).

PETs help users maintain control over their personal information while using the Internet. Although the U.S. government and Internet marketing associations continue to discuss how to best set regulations or develop standards for conduct, many companies are turning to PETs. Internet portals, e-mail providers and corporations are especially interested in how PETs can provide their users with the protection of Internet anonymity.

A number of companies have developed products that let users send and receive e-mail and browse the Web anonymously, via encryption and digital identification technologies. This approach ensures that control of personal information remains with the person initiating the transaction. The products completely disassociate real-world identities from online identities, allowing users to communicate with anyone on the Internet without sacrificing their privacy or control of their personal information.

With all the benefits of online privacy and anonymity, it is important to remember that these benefits also come with important responsibilities. My company believes in maintaining the integrity of its privacy-enhancing technology and the rights of consumers and businesses online. At the same time, the company operates in a manner that helps prevent misuse of anonymity. For example, if individuals use their anonymity to break the law, a Privada network operator can utilize a virtual "wire-tap" facility, which upon a court-legislated subpoena can be turned on in order to track down criminal activity from that point forward.

*Barbara Bellissimo is founder and vice president of marketing, Privada and a member of SIIA's Board of Directors. She can be reached at [barbara@privada.net](mailto:barbara@privada.net). This article was printed in the April 2000 issue of Upgrade, a publication of SIIA. Over 9000 copies of Upgrade are distributed to SIIA members worldwide.*

Software & Information Industry Association (SIIA)  
1730 M Street, NW, Suite 700  
Washington, DC 20036-4510  
202.452.1600  
[www.siiia.net](http://www.siiia.net)

**Subj:** Online Privacy: Perspectives of Net Nanny Software, Inc.  
**From:** Nika Herford, Net Nanny Software, Inc., 425-688-3008, [nikah@netnanny.com](mailto:nikah@netnanny.com)  
**To:** Internet Caucus Advisory Committee

### Will Technology Tools Assist Users in Protecting Their Privacy?

Private information has always been subject to varying degrees of collection and dissemination, but the Internet makes this process much faster and more efficient than ever before. Individuals often supply it freely themselves as they surf the Web, enter contests, sign up for services or communicate with others through email, chat and other interactive programs. Businesses, government agencies and other organizations post information and/or share it, often without an individual's knowledge, permission or concern.

Information sharing has its pros and cons, but most people agree that if given the choice, they would prefer to exercise some measure of control over access to their private information. The idea that marketers, insurance companies, and others may be aggregating personally identifiable information to build dossiers on individuals is unsettling. What can people do to protect their private information and online activities from being watched and used without their authorization?

There are a variety of technology tools available today to help control the solicitation and distribution of such personal information as names, addresses, phone numbers, email addresses, social security numbers, surfing habits, credit card numbers, school names and designated documents. Deployed on a home computer, browser or online service, these tools vary in their scope and flexibility, but all can be helpful aids to concerned online users.

For example, Net Nanny, which is installed on an individual computer, prompts the computer administrator to enter personal information into a form and assign the desired "actions" that the software should take in the event that an attempt is made to disclose personal information. Protected through the use of an administrator password, these actions include: shutting down the online session; masking out certain words, phrases and numbers; sending warning messages; and providing a time-stamped audit trail of specific attempts to send information. Regardless of which online service, browser or online environment a person uses, Net Nanny watches over his/her online activities and exercises the designated action when necessary. By providing several options, from lenient warning messages to strict shutdown controls, Net Nanny allows the administrator to choose the action that best addresses his/her own unique situation.

Internet browsers and programs like Net Nanny that log Web site visits, are effective complements to the FTC's new rule to protect the privacy of children under 13. Designed to give parents control over the collection, sharing and retention of their children's personal information, the power of the FTC's rule is enhanced if parents know which Web sites they should examine for potential privacy violations. Browsers also offer the ability to prompt users if sites are attempting to install "cookies" on their machines and prevent these "information collectors" from installing if the user decides not to accept them. While many tools provide password protection for their controls, it should be noted that browsers don't password-protect Web site history files, temporary Internet files or cookie settings.

Some online service providers allow master account holders to limit access to interactive programs such as chat, instant messaging, newsgroups and email and prevent the creation of online profiles. While these approaches are somewhat limiting in that they either allow full access or none at all, they are important tools to help prevent disclosure or solicitation of personal information and are realistic for an environment that must cater to many subscribers. A particularly effective granular control offered by some online service providers is the restriction of incoming and outgoing email to a certain list of email addresses. This feature helps ensure that users are only communicating with people they know and trust.

And for people who wish to surf the Web without being tracked, clean their entire computer system of Web-related activity, and send anonymous email, they can try tools offered by companies such as Anonymizer.

### What New Technologies Are On The Horizon?

#### P3P

A privacy standard called P3P, which is currently in development, will allow users to set up privacy preferences through their browser, which will control the use and dissemination of personal information according to a user's specifications. It works by comparing the privacy policy of an accessed Web site to a user's privacy preferences. If the policy conflicts with the preferences, the technology prompts the user to decide whether to override the preferences or surf elsewhere.

### Digital Signatures, Smart Cards, Encryption and the Missing Link: Biometrics

Increasingly, computer users interested in protecting their privacy are turning to security technologies such as smart cards, digital signatures, encryption and an emerging category known as biometrics. Each technology fills an important niche and all improve upon the standard user ID and password model for securing data and preventing unauthorized access to systems.

**Smart cards** are a convenient, credit card sized media that can both store and process data. Often used to verify people for log on purposes, access to medical information, credit/debit bank privileges and access control, the smart card's security is typically a combination of PIN numbers and cryptography keys. While the technology is highly portable and relatively secure, smart cards have no mechanism for binding a physical person to a card for the purpose of truly authenticating an individual.

**Digital Signatures** enable one or more parties to securely sign documents electronically. Important documents ranging from contracts, affidavits, or anything requiring a person's legal signature are not protected from being read, but are prevented from being altered (even if one "bit" is changed). Valid only in states, provinces and countries that recognize them as binding and legal, digital signatures are vulnerable to prying eyes as they travel over the unsecured public network. Therefore, **encryption** is used to scramble its content for transit.

A digital signature requires a trusted third party or certificate authority to authenticate the digital signature if it is challenged. A certificate authority, besides authenticating a digital signature, is a repository for a person's public encryption key. It is the combination of a digital signature and encryption that authenticates and secures a document from being read or altered in transit and after decryption, from being deliberately altered. A digital signature cannot bind a physical person to a digital signature, but rather relies exclusively upon the secrecy of the password. Similarly, encryption cannot bind a physical person to an encryption "key", because it also relies upon the secrecy of the password. While it cannot validate or verify that A or B created or modified the document, it fills a crucial role by protecting data from Point A to Point B.

**Biometrics** is a viable yet emerging technology that is poised to enhance the solutions above and provide a host of other innovative implementations where true authentication of the user is needed. Biometrics involves the authentication of an individual based on a unique physiological characteristic, such as fingerprint, voice, iris, or a behavioral characteristic, such as typing rhythm.

Net Nanny's patented biometric solution, BioPassword , leverages the massive install base of user IDs and passwords and adds another simple and cost-effective element to protect privacy – keystroke dynamics. The opportunities for incorporating biometrics into our everyday lives are vast – e-commerce, home security, online banking, gun safety, car security, ATMs, phones. The days of compromised passwords and incomplete solutions are drawing to a close. Combining a biometric (what you are) with a smart card (what you have) and PIN number (what you know) creates a secure scenario that is virtually impossible for someone to crack. It finally solves the problem of binding a physical person to a device or signature.

Some people are concerned that biometrics itself may endanger people's privacy. The idea of storing a fingerprint, voiceprint, iris scan or some other uniquely identifiable characteristic in a database is an uncomfortable proposition for some. Like many new technologies, there will be a period of adjustment, especially for the more intrusive biometric solutions. BioPassword is perhaps the least intrusive solution on the horizon because it leverages the acceptance most people have for typing. It simply asks a user to type in his user ID and password 15 times initially and the software takes a mathematical measurement of the individual's typing rhythm. Thereafter a user need only type in his user ID and password once to gain entry. Voice and facial recognition software are two other biometric solutions that will probably enjoy more widespread acceptance than fingerprints, iris or retinal scans.

Privacy protection requires diligence on the part of the individual and constant innovation on the part of technology companies. Implementation of forthright business practices and oversight by watchful governmental agencies and other watchdog groups will help establish acceptable strategies for collecting and managing data online. User-friendly filters and authentication technologies will continue to evolve, but the key is encouraging people to educate themselves about the issues and pay attention to where they are going both online and offline and with whom they are sharing their information. The irony is that the biggest culprits may very well be our own neighborhood grocery stores or banks.

### ADDITIONAL RESOURCES

<http://www.netnanny.com/family>

<http://www.getnetwise.org>

<http://www.anonymizer.com>

<http://www.ftc.gov/kidsprivacy>

P3P Platform for Privacy Preferences <http://www.p3p.org>

RSA security <http://www.rsasecurity.com/> (encryption)

PGP international page <http://www.pgpi.org/> (encryption)

Biometric Research <http://biometrics.cse.msu.edu/>

International Biometric Group <http://www.biometricgroup.com>

BioAPI <http://www.bioapi.org>

Smart Card Industry Association SCIA <http://www.scia.org/>

CardTech/SecurTech <http://www.ctst.com/>

Smart Card Resource Center <http://www.smart-card.com/>

**Subj:** Online Privacy: Perspectives of Computer Professionals for Social Responsibility  
**From:** Karen Coyle, CPSR, 510-987-0567, kcoyle@ix.netcom.com  
**To:** Internet Caucus Advisory Committee

*Excerpt from "Some Frequently Asked Questions About Data Privacy and P3P" See full text at: <http://www.cpsr.org/program/privacy/privacy.html>*

## **P3P**

### *What is P3P?*

*P3P is the "Platform for Privacy Preferences," a new Internet protocol being developed by the World Wide Web Consortium (W3C). Protocols are the rules around which Internet software is developed. This means that the P3P functions will be implemented as part of the functioning of the World Wide Web, and most likely it will be intergrated into Web browsers like Netscape and Internet Explorer. P3P defines a standard way that the privacy practices of Web sites can be defined and that a consumer's personal data can be requested.*

### *What are "privacy preferences"? Is this the same as "privacy protection"?*

*No, privacy and privacy preferences are very different concepts. Most people consider privacy to mean that others, especially strangers, do not have access to information about you. In the privacy preferences model, your personal data is not inherently private since modern transactions often consist of an exchange of personal information for goods and services. Engaging in that exchange is an exercise of ones' privacy preferences. So if you sign up for an online information service, such as a daily newspaper, you might be exchanging information about who you are (your email address and some demographic information) and your reading habits for the access to those newspaper articles.*

### *What is the problem P3P is designed to solve?*

*An article by the main developers of P3P states: "Many online privacy concerns arise because it is difficult for users to obtain information about actual Web site information practices.... Thus, there is often a one-way mirror effect: Web sites ask users to provide personal information, but users have little knowledge about how their information will be used." P3P is not designed to eliminate or reduce the exchange of personal data, but to give the Internet user a way to exercise some discretion over the exchange of that data based on the stated data gathering and use policies of that Web site. Will P3P give me more privacy when I use the Net? No. P3P will allow you to exercise personal data preferences. It does not make your Internet use more private than it is today, although you may be better informed about what data is being collected and why.*

### *Are privacy practices really the problem?*

*It is known that consumer concerns about the safety of using the Internet are a barrier to the development of electronic commerce. When polled, many Internet users indicate that they do not purchase items over the Internet because of privacy and security fears. If successful, P3P would help users overcome these fears and therefore increase the number of consumers who use the Internet for purchases. Privacy practices is only one factor in the consumer/retailer relationship, however. Consumers develop trust relationships with companies, whether they are home-town stores, national chains, or catalog retailers based on the company's reputation and the customer's previous experience, not with their privacy practices. Many people do mail-order shopping even though they know that the companies they are dealing with sell their address to other mail-order companies. P3P seems to be designed for situations in which that trust relationship does not yet*

*exist. However, what isn't clear is whether knowing how the data will be used will resolve this conflict.*

***How will P3P work?***

*The first implementations of P3P have not yet been released publicly, so we don't have details about how it will look to Net users. We do know that P3P will probably be incorporated into Internet browsers like Netscape and Internet Explorer, and perhaps will be used in other Internet software. The P3P protocol does state that the software must install with the maximum "privacy" as the default. Users will provide their personal information (name, address, etc.), probably in a form, and will indicate their "privacy preferences." When the user surfs to a Web site that uses P3P, the data request of the Web site will be compared to the user's preferences. If they match, the requested data will either be transmitted to the Web site or the user will be asked to fill a form with the information.*

***What problems doesn't P3P solve?***

*P3P actually covers only a very specific part of the online interaction: the transmittal of privacy practices to a user, and the comparison of these to the user's preferences. P3P does not increase the security of Internet transactions. It does not make it safe to send credit card numbers over the Net. It doesn't protect consumers from Internet eaves-dropping that gleans passwords and consumer data as it travels over the network. Security must be provided by other software such as the Web browser. It does not provide any enforcement of the privacy practices that are promised by the Web sites, nor does it give individuals any information about the trustworthiness of the site they are visiting. It does not address whether information gathered on the Net will be combined with information gathered elsewhere to create a more detailed profile of the user. It does not reduce the amount of personal data that is gathered from Internet users and it is not intended to do so.*

**Links**

**P3P**

The W3C <http://www.w3.org>

The P3P Page <http://www.w3.org/P3P/>

**Privacy Information**

CPSR's Privacy Page <http://www.cpsr.org/program/privacy/privacy.html>

CPSR's SSN FAQ <http://www.cpsr.org/cpsr/privacy/ssn/ssn.faq.html>

The Privacy Rights Clearinghouse <http://www.privacyrights.org/>

The Electronic Privacy Information Center (EPIC) <http://www.epic.org>

U.S. Federal Trade Commission's privacy page <http://www.ftc.gov>

The Global Internet Liberty Campaign's Privacy and Human Rights <http://www.privacyinternational.org/survey/>

-----  
*This document prepared and maintained by Karen Coyle, with generous help from Andy Oram, Rick Barry, Harry Hochheiser and Marc Rotenberg. Send comments [ktoyle@cpsr.org](mailto:ktoyle@cpsr.org)*