Unclassified **DSTI/ICCP/REG(2001)1/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

07-Jan-2002

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Working Party on Information Security and Privacy

INVENTORY OF PRIVACY-ENHANCING TECHNOLOGIES (PETs)

JT00119007

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

FOREWORD

This inventory of privacy-enhancing technologies (PETs) has been prepared by Lauren Hall, Executive Vice President of the Software & Information Industry Association (SIIA) in co-operation with the Secretariat. It discusses methods of data collection, analyses different types of PETs and makes recommendations to the private sector for encouraging increased development and use of such technologies.

This report was considered by the Working Party on Information Security and Privacy as an important contribution to its work in the area of privacy-enhancing technologies. The Committee for Information, Computer and Communications Policy approved the declassification of this document at its 40th Session on 11-12 October 2001. It should be noted that this paper reflects the views of the author and not necessarily those of the OECD or of Member country governments.

TABLE OF CONTENTS

INTRODUCTION

Technology can play an important role in enhancing the protection of personal privacy online. Using the 1980 OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data as a guide, this paper aims to analyse the availability and variety of privacy-enhancing technologies (PETs), consider the factors affecting adoption of PETs, analyse the relationship between technology and privacy, and form a basis for policy makers to discuss the use and deployment of such technologies.

Privacy enhancing technologies (PETs) commonly refer to a wide range of technologies that help protect personal privacy. Ranging from tools that provide anonymity to those that allow a user to choose if, when and under what circumstances personal information is disclosed, the use of privacy enhancing technologies helps users make informed choices about privacy protection.

PETs can empower users and consumers seeking to control the disclosure, use and distribution of personal information online. PETs can also aid businesses and organisations in enforcing their own privacy policies and practices. In an era of consumer concerns about online privacy, PETs are crucial tools in managing the flow of personal information on global public networks.

This paper discusses methods of data collection, analyses different types of privacy-enhancing technologies and makes recommendations for encouraging increased use of these tools. It also briefly touches on security technologies, many of which were initially designed to protect the confidentiality of information but can also enhance privacy. In addition, many technologies that can enhance security – such as digital signatures or authentication technologies – can enhance the privacy of or ensure the integrity of communications or online transactions, but because they are designed to ensure the identity of the individual, may limit the potential of anonymous online activity.

As a result, because so many technologies can be used in many different ways, it is crucial to recognise the context in which any given technology is used. Different products, different technologies and various functions can serve different purposes depending on the preferences of the user and the implementation of the particular technology. As a result, it is important to keep in mind that consumers and policy makers will need to be educated about and understand the different ways in which various technologies can be used to achieve different goals.

BACKGROUND

The 1980 *OECD Guidelines for the Protection of Privacy and Transborder Data Flows*

The rapid rise of interconnected, global networks and the increasing flow of personal data across national borders have raised awareness among policy makers, consumers and companies about privacy concerns. The *Guidelines for the Protection of Privacy and Transborder Data Flows of Personal Data*, while adopted by the Organisation for Economic Co-operation and Development in 1980, were adopted in an earlier era of technological development and expansion, and remain relevant and topical today. In 1980, the OECD was primarily concerned with the rise of processing of personal data transported across national borders by large corporations and data processing firms; today, the OECD addresses the sharing and distribution of personal data across borders through Internet-based technologies and sites. The eight core principles established by the OECD in the 1980 Guidelines are:

1. **Collection limitation:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data quality:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. **Purpose specification:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use limitation:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the “purpose specification” except: (a) with the consent of the data subject; or (b) by the authority of law.

5. **Security safeguards:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. **Openness:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual participation:** An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him:

   - Within a reasonable time.
   - At a charge, if any, that is not excessive.

- In a reasonable manner.
- In a form that is readily intelligible to him.

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.

8. **Accountability:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

Despite differing national approaches, varied consumer preferences and a wide variety of self-regulatory approaches developed by business, the OECD Guidelines continue to represent a consensus viewpoint on data protection. The OECD reaffirmed that the Guidelines provide an international foundation for privacy at the 1998 Ottawa Ministerial Conference, *A Borderless World: Realising the Potential of Global Electronic Commerce*.

The OECD has long recognised the role that technology can play in enhancing privacy in the online environment. In 1997, the OECD issued a report, *Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet,* which encouraged the development of policies and technologies that would guarantee the protection of privacy of individuals on global networks. Ministers affirmed the important role that technology can play in protecting privacy in the 1998 Ottawa Ministerial Declaration, noting that they would “encourage the use of privacy-enhancing technologies” in OECD Member countries. The challenge for industry, consumers and governments is to effectively implement the principles embodied in the 1980 OECD Guidelines in the face of rapid technological change.

The Demand for privacy-enhancing technologies

Use of the Internet has skyrocketed since 1993 with the introduction of the graphical user interface and the 1995 movement of Internet administration to the private sector. Once a predominantly North American phenomenon, today the Internet is international in nature and use. With telecommunications deregulation, reduced prices for computer hardware, software and Internet access, and increasingly robust services and products available online, Internet usage is expected to continue to grow at brisk rates for the foreseeable future.

Internet usage varies widely, from simple information presented online to complex systems that may host thousands of simultaneous web sites. For individuals, primary Internet access may be through their workplace, a school account or a personal account through an Internet Service Provider (ISP).[1]

As usage grows, so does the commercial viability of the Internet. Companies have been flocking to the Internet for several years, representing businesses in every industry, from small entities to multinational corporations, from every region of the world. The international nature of the Internet makes the global network an attractive, and often lucrative, new alternative for increased market penetration which supports a diverse and expanding set of business models that make categorical or “one size fits all” solutions impractical and in a worst-case scenario, counterproductive.

At the same time, concern over the collection of personal data has grown for a number of reasons.

First, advanced technologies make it possible for data to be collected about individuals that visit web sites, participate in chat rooms or newsgroups, send e-mail or otherwise use Internet services without their knowledge or consent. All the data that is collected is not *directly identifiable personal data*; rather in many cases, it is essential information to support system maintenance and network viability. Nonetheless, consumers are often surprised to learn that such information may be collected.

As discussions about privacy continue in the media, among consumer groups and in a wide range of fora, individuals are often surprised by the amount of information collected about them both online and offline. For instance, they often do not realise how often they are filmed on security cameras in public places, that "electric eyes" may be triggered with automatic doors or that turnstiles on public transportation count and, especially in the cases of pre-purchased long-term passes, that their travels are recorded at turnstiles or tool booths.

Second, much more can and should be done to enable individuals who are concerned about online privacy to utilise the empowering tools that protect them from the unwanted disclosure of personal data (PD). While the majority of the most heavily trafficked web sites have posted privacy policies, industry sectors have developed and implemented self-regulatory initiatives, and some national governments have passed data collection laws, surveys show that many individuals remain concerned. An October 2000 study by the National Consumers League and conducted by Harris International found that 56% of individuals are concerned about the loss of personal privacy.[2] While the Internet has become increasingly user-friendly in recent years, the technical nature is often intimidating for many users who believe that there is little, if anything, that they can do to prevent unwanted data collection, use or distribution.[3]

Third, while recognising that different approaches to privacy among nations is a norm, this landscape complicates the privacy issue for policy makers, businesses and individuals. Europe and the United States, for example, have very different approaches to the issue of privacy (as demonstrated by the recent US-EU safe harbour agreement), creating a significant challenge for companies that serve both European and US customers.

For consumers and individuals, the differing approaches to privacy in different jurisdictions present a special challenge. A consumer using the Internet may not realise that he or she is visiting sites that may or may not be located in their home country, and, as a result, may not understand that the data protection environment to which they may be accustomed may not apply to the site with which he or she is sharing information. This situation may become particularly worrisome when the consumer is sharing sensitive data.

Of course, no technology can address the myriad of privacy laws in every country, region or jurisdiction. It would simply be impossible given the differing approaches and the limitations of technologies. For example, it is often difficult to identify where a web site visitor is coming from, where the country of origin for a given consumer might be or for a web site to keep up with the often rapidly changing regulatory and consumer preferences in every country around the world. As a result, privacy-enhancing technologies installed on an individual consumer's computer, configured to respect perhaps both the consumer's personal preferences and national law, may be an effective means for addressing privacy concerns, particularly if combined with a wider respect and recognition of internationally-accepted privacy principles.

1. METHODS OF DATA COLLECTION

Data can be collected in a variety of ways. With continuing advances in technology, there can be no doubt that new techniques will emerge that facilitate data collection. As such, this list considers only some of the most widely used techniques and should not be considered exhaustive.

In addition, it is important to recognise that in terms of transparency, significant progress has been made to date. With growing concern from individuals, many web sites – and certainly most of the most popular web sites – now prominently display links to their privacy policies, clearly disclose their data collection practices and provide information regarding the use of collected data. There has been, in recent years, a growing awareness by online sites that individuals not only look for, but also make decisions based upon, the existence and content of posted privacy policies.

Data collection and analysis technologies and methods can be highly useful in enhancing the online consumer experience, improving services and developing more customised content, products and services.

Commercial web sites collect information through both voluntary and passive means. Voluntary measures include registration pages, surveys and other online forms. With voluntary means, some action on behalf of the user is generally required and the user is aware that data is being provided and/or collected. Passive measures typically include aggregate data collection and site usage selection; the user may not be aware that this generally non-personal information is being collected. The use of cookies is often characterised as passive, but because all commercial browsers allow users to reject all cookies or accept certain cookies only after the user has approved the acceptance of the cookie, the use of cookies can also be active.

Passive collection of transactional data

Non-personal data revealed just by surfing a site tell a good deal about online activities. Web servers can collect information about what pages a user looked at, how long a particular page was displayed on a screen, the URL of the most recently visited site and the URL of the next site requested.[4]

None of this information is inherently personally identifiable. In fact, much of this anonymous information is aggregated and used for marketing and site analysis. For example, it may be very helpful for a web site operator to know that their home page received 100 000 hits one month from 54 000 unique visitors, but that a page highlighting last-minute sales or news on a particular topic received only 2 000 hits.

Much of this information is collected to allow those responsible for maintaining the site to perform necessary system maintenance, auditing, and optimise performance to an individual’s computer and connection speed and other system functions. This information is needed to ensure that a web site is performing properly and providing timely access to visitors. Some information may be collected as part of the normal functioning of the web server software itself and stored in maintenance logs used for ensuring system reliability.

Personal collection of personal information

Some personally identifiable information can be collected through passive means, especially if a user has configured his or her web browser in certain ways. Some web sites collect information from individuals who store their email address or name, for example, in their browser. Users may not know or be aware that this information is being collected. It should be noted, however, that most sites with privacy policies that do collect this information do disclose those practices, and that users can avoid having their information disclosed by simply not including this information in their web browsers, as it is not required for the proper functioning of any browser application.

Active collection of transactional or personal information

Many sites actively collect transactional or personal information by deploying specific technologies or business processes on their web sites. Several approaches are quite explicit and require user participation in order to collect information, such as through online forms or user accounts. Others may be less obvious to a web site visitor, such as cookies, "web bugs" or clear .gifs.

User accounts

Some web sites allow users to establish an online account. Generally, account information is stored at the web site itself, including a username and password. User accounts often are used when a user will likely need to access historical information or data collected offline, such as for an airline frequent flyer programme or a retail e-commerce site. When the user visits a site, he or she is generally prompted to log in, usually by providing a password and username. Upon successful login, the user is granted access to the information stored in his or her account.

To establish an account, a user may have to provide basic contact information, preferences and credit information, if the site charges for its services. Many of these sites often collect and maintain user usage and order history, clickstream and personal information necessary to complete the user's transaction or requests. Preference information also aids a web site in determining which offerings are most attractive and useful for its visitors, as well as which offerings are not. By determining consumer preferences based on clickstream data – both what the consumer is interested in and what he or she is not interested in – the consumer experience can be greatly enhanced. Such data collection is legal and often desirable for consumers, and sites with privacy policies often disclose that such data is collected. In any case, a site that provides notice about its data collection procedures, whether voluntarily or as prescribed by law, should disclose its clickstream data collection procedures.

Because of the significant overhead investment, maintenance and security requirements for large-scale systems, generally only companies that need to maintain this information on their own server for operational reasons implement user accounts.

Online forms

Online forms are a common method for collecting information from consumers. Forms can be used in almost countless ways – from collecting data from a user who has requested more information about a company's products or services to participating in an online survey. The use of forms is widespread and their utility limited only by the imagination of a web site designer.

In some cases, a site may request that a visitor register even if the service, product or content offered is free. Generally, registration brings additional benefits not available to unregistered users. A site that provides online electronic greeting cards, for example, may allow its registered users to create personal address books or establish a calendar of important events, enhancing the site's utility to the user and creating a reason for the user to return to the site in the future.

In many cases, registration is not required to use a site, but the additional services are not available to non-registered users. The choice is up to the consumer. Many e-commerce sites, for example, will allow an individual to place an order without creating an account. However, the user may not be able to return to the site and take advantage of advanced customer services, such as checking delivery status, using gift certificates or storing shipping addresses online for future use. Users that do not register may have to re-enter vital information multiple times, be unable to take advantage of loyalty programmes, be unable to resume a previous transaction, browsing or shopping experience or be able to modify their online preferences.

The benefits for companies in collecting this information is clear. By asking the visitor to fill out a registration form with personal information such as name, address, how the user learned about a web site or preferred topics, companies can develop valuable customer profiles and analysis. This data can in turn be used to improve web site content and refine the services or products provided.

Cookies

Many web sites use "cookies" to deliver client-side information and enhance the user experience. Cookies are text files that allow a web server to store and retrieve information on the client side of the server-browser (client) connection.

In most cases, data stored in cookies is not detrimental to the protection of personal data. Rather, it is essential to providing an enhanced customer experience. A cookie may, for example, track whether a specific user has visited the site previously. Depending on the information in the cookie, the web site may offer “first-time” visitor information, or, alternatively, thank the visitor for returning. This information is not necessarily personally identifiable, especially if the browser has been used by others or if the computer is shared, as in an office environment.

Cookies also greatly enhance online functionality, as many common e-commerce functions would be impossible without the use of cookies. An example is helpful. When a user visits an e-commerce site and adds products to his or her virtual shopping cart, the information regarding what products the customer has identified while he or she continues shopping, fills out shipping information.[5] The information about which products may be in the shopping cart is stored on the server itself, not on the user's computer. The server then retains control over the information about the individual and his preferences, while the user's computer only contains information that will allow the server to link the session information stored at the site with the individual user. These techniques, known as state management, are necessary to keep track of which users are selecting which options. Without state management, it would be impossible to conduct online commerce or provide a seamless user experience.

Cookies may also be used to ensure that a web page is properly delivered to a user. Web pages can be complex, comprised of text, graphics, images, frames and other elements. Delivering each web page may represent a number of separate requests from the client computer. For example, the client computer may request the initial delivery of the page, of separate graphics or images, or embedded frames that comprise a single page. Cookies, stored on the user's machine, help a web server recognise when a page has been properly served to the individual.

Cookies used to control the user environment are generally temporary. These cookies are often not permanently stored on a user’s computer and are only used to control the user’s session. They do not typically contain any personal information.

Persistent cookies are stored on a user’s computer until their expiration date. A persistent cookie typically stores more complex information, such as user login information, account identification or other unique data. The data stored in a persistent cookie may or may not be personally identifiable.

Cookies facilitate consumer web site use (as opposed to online user accounts or storing the temporary information on the web server itself) because they allow the site to utilise the resources of the client computer, rather than the web server. For a site that may be hosting thousands of simultaneous users, the ability to share computing resources with the individual improves performance for all users.

However, it is recognised that cookies are the target of criticism. One issue that is often highlighted is that cookies can be written to the user’s computer without the user’s knowledge if the browser is so configured. Cookies have received negative coverage in the press and from privacy advocates, and significant misinformation about cookies circulates widely on the Internet. Some see cookies as an invasion of privacy, some fear having a remote computer store data on their computer, some believe (incorrectly) that cookies can pass along viruses or otherwise do damage to their machines.

Generally, cookies can only provide information to the web site that stored the cookie originally. In other words, a cookie created by web site A cannot be read by web site B. This practice, defined in several Internet RFCs,[6] virtually eliminates the danger of one web site reading information stored by another.[7]

Like many technology features, though, cookies can be implemented both to enhance and improve the consumer experience as well as for more problematic uses. The fact that a site uses cookies is neither “good” nor “bad” as technology itself is neutral. However, cookies can store a good deal of information about individual browsing habits, and because they can be deployed in so many different ways, can raise concerns among consumers.

Users have many tools available to control cookies and the information collected through the use of technology. Users that fail to manage their cookies, to at least occasionally review the cookies stored on their systems or use cookie management tools may find that some sites collect more information than they are comfortable with.

All popular browsers have some form of cookie management tools built in, allowing a user to reject all cookies, accept all cookies or decide to accept cookies on a case-by-case basis. Users concerned about cookies should be encouraged to use these features, which are available to all web users. In addition, all browsers allow users to review the cookies stored on their systems, and to delete those that they no longer wish to keep or find offensive. Sites like the OECD Privacy Policy Generator that ask specific, detailed questions about cookie usage also help increase transparency about the use of cookies. For those seeking more robust features, cookie management tools are more fully explored in the following section on specific PETs .

Web bugs (Clear .gifs, 1x1 .gifs, Invisible .gifs or Beacon .gifs)

Web bugs are small images, generally one pixel, that are placed on HTML pages[8] that are often used to track usage and provide information to the party that places the image.

Generally, these images are used to determine how many hits a page receives. Web bugs are most often used to gauge web traffic, how many times a page has been viewed, and other administrative or site monitoring requirements. A web usage monitor will report how many times the image was accessed – a standard piece of non-personal data used in system maintenance. They may also, however, be used to solicit additional information, including the URL of the page on which the image is stored, the type of browser being used, the time of viewing, the client IP address, or to retrieve information stored in cookies. Such images may be used in any HTML code, whether on a web page or in HTML email.

Because these images typically cannot be seen nor blocked by traditional cookie blockers[9] or other similar technologies they have raised concerns among privacy advocates. The increasing use of HTML e-mail has added to the concern.

Web browsers

The advent of web browsers was a crucial step in making the Internet and global networks accessible to individuals and the general public. Before the development of web browsers and HTML, the Internet was largely limited to academics, engineers and computer aficionados. Without web browsers, the Internet would never have developed into the valuable information medium that it has.

Web browsers have become increasingly complex and robust since their introduction in the early 1990s. Web browsers now integrate e-mail client software, include FTP capabilities and support a wide variety of plug-ins.[10] In using the features of the web browsers, some users choose to store personal information, such as e-mail addresses or a name, in their preferences settings. This information may be accessible to a web server; the browser will provide this information to the web server when requested.

Users of more advanced e-mail clients such as Microsoft Outlook, web-based e-mail, AOL or other proprietary online services need not enter this information into their web browser customisation features. Some users that rely on e-mail clients bundled with Internet browsers must enter at least their e-mail address in order to have their reply-to addresses properly appear or the sender’s identity be properly represented to recipients of their e-mail messages. While designed as a convenience feature, the ability to request and receive information stored in a preferences or setting file may be the source of the disclosure of one’s e-mail address or other information that the user chooses to provide.

Benefits of data collection

Ministers gathered in Ottawa in 1998 noted the benefits of electronic commerce to all stakeholders, recognising that for electronic commerce to flourish on a global basis users must work together to achieve practical solutions to the challenge of a borderless world.

When considering the privacy issue, policy makers, advocates and industry often point to a conflict between businesses’ need for information about their consumers and the desires of individuals to control their personal information. This distinction is perhaps too limiting and unfairly characterises business and consumers as opposed on the issue of privacy. In fact, the private sector has, along with the development of PETs, championed the widespread adoption of privacy policies and promoted effective self-regulatory efforts.

The following section highlights some of the key benefits of data collection.

User convenience

Collecting information about an individual user creates the opportunity to provide customised, personalised service to each web site visitor. As examples of the variety of ways the Internet meets consumer demands, many portals, online shopping and news sites offer visitors the opportunity to create accounts or use other technologies to customise their online experiences.

Amazon.com, for example, can be set to remember a customer's name and previous purchasing history. This ability to welcome returning customers and provide a custom home page with suggestions for products allows Amazon.com to build customer loyalty and address critical inventory control operations through tailored messages that promote a product that an individual might like or special offers based on a user's preferences. CNN.com allows users to prioritise the issues and news topics in which they are most interested. And many e-commerce sites allow a user to create accounts and store credit card numbers, shipping addresses and billing preferences, simplifying the use of the site's functionality in the future. Many of these features have analogues in the offline world. For example, a consumer is far more likely to frequent a neighbourhood book store where the owner is familiar with his or her literary preferences, or the corner coffee shop where the counter clerk always remembers his or her name and how he or she takes their coffee. In many ways, the ability to personalise and customise the online experience provides a "neighbourhood" or friendly feel to what might otherwise be a cold and purely businesslike transaction for the consumer. Of course, consumers who prefer more anonymous or less familiar experiences certainly have that option, too.

All of these features enhance the online experience for individual users by making the use of these sites more convenient and timely.

Enhanced marketing and business development

The online environment is an extremely competitive one, as many e-commerce retailers have learned in the past several months. Gaining market share by building customer loyalty, expanding the customer base and increasing the number of transactions per customers (in other words, creating repeat sales) is crucial. Because customer retention is far less expensive than customer recruitment, creating an ongoing relationship with a customer is often a deciding factor in online commercial success.

Providing customised services, responding quickly to consumer concerns and respecting customer preferences are all important elements for a business seeking to develop a relationship with its customers. To do so, companies need to fully understand their market and consumers. That knowledge can only be obtained through the collection of data from existing customers.

Customers benefit from these marketing techniques. A frequent traveller, for example, may benefit from an airline that offers discounts or other benefits to its most loyal customers. A site may be able to offer personal customer service online or store user preferences. These tools encourage customer loyalty and enhance the potential success for online commerce.

User experience enhancement/consumer protection

The collection of data not only enhances the browsing experience for individual users through personalization, customisation and provision of enhanced services from a given web site, it may also play a crucial role in protecting consumers or enhancing their online experiences.

An example may be illustrative.

Consider an online travel agency where a user has recently purchased an airline ticket for a trip to Paris, France. If the same user then mistakenly books a hotel room in Paris, *Texas* for the same dates that the user is presumably travelling to Paris, *France*, the system could ask the individual to confirm that the hotel reservations in Paris, Texas are accurate. Such a proactive intervention could prevent a user from being unexpectedly charged for hotel reservations that he or she did not need, or from arriving in Paris with incorrect lodging arrangements.

2. PRIVACY-ENHANCING TECHNOLOGIES

Despite the recognised role that personal data plays in promoting key technical and commercial operations, individual users remain concerned about the risks associated with the sharing of their personal data. As noted in the 1998 OECD Ministerial Declaration, privacy-enhancing technologies (PETs) are an important element in promoting the protection of personal data; moreover, they enable users to make informed choices about privacy. PETs that provide users more control over their personal information can help alleviate many of the concerns that consumers have identified as barriers to the growth of electronic commerce. PETs are also able to allow consumers to exercise the broadest possible choices. PETs allow users to make more subjective and detailed decisions concerning their information.

PETs vary widely in their functionality, capabilities, technical structure and usability. However, all PETs aim to give the individual user or technology manager the capability of controlling if, how much or under what circumstances information is disclosed.

At the same time, it is important to realise that PETs cannot, and are not designed to, address every consumer or policy maker's concern about data collection. PETs are simply one of many tools available to consumers in the online environment, and as this paper discussed, one that consumers should be encouraged to use if they have concerns about data collection.

The biggest limitation of PETs is simply lack of consumer awareness. PETs have recently gone through a significant shakeout. As a result of increasingly difficult market conditions for all start ups and low awareness and uptake by consumers, a number of PETs have either gone out of business or have significantly revised their operations. In short, consumers must be aware of the availability and capabilities of PETs in order to benefit from their features, just as a consumer must use his or her seatbelt in order to be better protected in the event of a car accident.

In addition, even consumers that choose to use PETs must be encouraged to use them consistently. Many users in search of simple, efficient online experiences give up using PETs after a short period, negating the benefits that a PET can have.

Finally, consumers must choose the right PET or other technology to address their particular concern. For different consumers, the primary concern could be anonymity, conducting trustworthy transactions, control over personal data or transaction security. As illustrated in this paper, there are a wide variety of PETs and security enhancing tools, and consumers must understand that not every PET will address all of their concerns. For example, while an e-mail encryption program may work well at keeping electronic correspondence confidential, it will do little to help the consumer manage cookies or keep clear .gifs from displaying on a web page. Governments, industry, consumer groups and privacy protection authorities and experts all have a role in helping consumers make the right decisions about which PETs are best suited to address their individual concerns.

Consumer concerns about data collection

Consumer concerns can be generally categorised into several areas.

Sharing of data with third parties

Consumers who have provided personal information to a particular site, organisation or business should not have that information shared with a third party (*i.e.* one not involved in or associated with the site, organisation or business in question) without their permission or knowledge.

Security fears

Users often are concerned that the data collector may not adequately protect personal information from accidental or malicious disclosure. Lack of security or misinformation about available security may deter consumers from providing information across the Internet. Well-publicised disclosures of consumer information, including credit card information, from a few popular web sites has increased public fears. While the fear has increased, awareness of the need for security or how to evaluate security has not increased dramatically.

Lack of knowledge about data usage

The rapid growth of electronic commerce demonstrates that consumers are willing to provide information, even personal data, in exchange for services, personalization features or customised content. However, many consumers are concerned about how information that they provided will be used by the receiving organisation. A consumer, for example, may be very comfortable knowing that personal information is used to create customised news updates, but less willing to provide the same data if used for unrelated marketing purposes.

Consumer "profiling"

Businesses often use consumer information to create customer profiles. Profiles may be personal (*i.e.* related to a specific individual consumer) or aggregated (*i.e.* where common characteristics are used to identify a specific demographic). Profiles can be beneficial to consumers and greatly simplify their online experiences, but the concept of "profiling" has received extremely negative coverage in the media. Some consumers are uncomfortable being categorised, having their order history stored, or having a web site maintain personal information. In addition, some consumers seem particularly concerned with the practice of data collected at one site being combined with offline information or data collected from other online sites or stores.

Identity theft

The sharing of particularly sensitive information, such as credit or financial data, is of particular concern to many consumers and policy makers. The abuse of personal information may, in some circumstances, result in identity theft. While identify theft can occur online or offline, there has been a rise in identity theft in recent years. It is unclear to what extent this rise is attributed to poor data security, increased information theft or abuse, or if it is simply easier for criminals to share the information necessary to steal an individual's identity on global networks. Whatever the case, increased awareness about the crime of identify theft has undoubtedly made some consumers more hesitant to share personal information.

Security and privacy

There is, of course, a close relationship between security technologies and privacy technologies. That the concepts of privacy and security are so closely related is a common source of confusion for many. The two are not separate, and for the purposes of protecting individual information cannot be separated, but at the same time they are not interchangeable technological concepts.

The OECD recognised in the 1980 Guidelines that security was a crucial element in protecting privacy. Without strong security, personal information cannot be properly secured from misuse or abuse.

It is important to note that when the technology community[11] refers to security, it is generally referring to the protection of the data from accidental disclosure, misuse or abuse, and destruction or corruption of data, whether personally identifiable or otherwise. Security may apply to the storage, transmission, backup or other transactions involving data. Security solutions, products and services typically seek to prevent the introduction of viruses, eliminate network vulnerabilities, limit access by unauthorised users and authenticate data, messages, or users.

These are critical tools in protecting stored or transmitted personal information. Without the ability to secure personal data, an individual cannot be assured that his or her data is being properly protected once shared with an online site, business or organisation. Without security technologies, it would be difficult – if not impossible – to protect data and provide privacy tools to individuals, corporations and other organisations. The ability to provide consumer choices about data collection and to secure collected or stored data relies on the widespread availability of strong security technologies.

Beyond the requirement that personal data be protected by reasonable or adequate security safeguards, privacy protection includes limits of a “legal” nature to the collection, handling, storage or transmission of personally identifiable or aggregates data collected from individual users. Whether personal information is collected, how it is used or shared, what options a user may have, whether a user may access stored information, and who has access to that stored data are all issues addressed in the discussion of privacy.

Personal privacy-enhancing technologies

It is important to recognise that privacy preferences often differ significantly, as individuals have different concerns or prerogatives regarding the treatment of personal information. It is also important to note that in the following inventory of technologies and consumer options, some are software tools that are stored on the individual’s hard drive, some are deployed on a user’s network or some are online services. As such, even when using privacy-enhancing services that are provided online or downloading PET software, consumers should take care to carefully review the privacy policies of the hosting or providing site.

Cookie managers or blockers

Cookie managers or blockers are applications that allow the user to know when cookies are being written to his or her hard drive, to manage the acceptance of cookies, and to view what information is stored in an individual cookie. Cookie managers or blockers vary widely in their usability and features, but all give the individual more control over cookies stored on their personal computers.

Cookie managers or blockers can help users determine which sites have placed cookies on their computers, when the cookies were placed and the expiration dates of the cookies. They also allow users to delete or retain a particular cookie. However, because the data in many cookies is indecipherable to the average user, cookie managers may be limited in their effectiveness or usability to users who wish to know exactly what information is being stored on their computers in cookie files.

It is important to note that all commercial browsers allow an individual to determine whether he or she wishes to receive cookies. No additional applications are necessary as this functionality is inherent to the browser. In addition, because cookies are simply text files, any user can view any cookie stored on his or her hard drive. However, the data stored in cookies is generally difficult, if not impossible, to understand for the common user as the data may be encoded to simplify communications with the web site that originally placed the cookie.[12]

Cookie managers are widely available commercially, and several products are available as freeware or shareware.

Ad blockers

For users who do not like and appreciate the targeted advertisements that many sites provide, software to block the delivery of online advertising is available. These applications keep ads from being delivered to the end user and thus, from tracking a client. However, because ads can take many different forms, these applications vary in their ability to completely block advertisements from being delivered to the user.

Ad blocking software may be appropriate for users who have slow connections and do not wish to use valuable bandwidth downloading advertisements. The blocking software also benefits those who are fundamentally opposed to Internet advertising or individuals who wish to prevent their children or other users from viewing online advertisements. However, while several commercial products are available, ad blocking software has seen somewhat limited adoption. Significantly, relatively little personal information can be collected simply from viewing an advertisement.

Encryption software

Encryption software allows the user to encrypt – or scramble – digital data. Users may opt to use encryption to protect the contents of their e-mail messages, stored files and online communications. Once encrypted, only users that have the appropriate digital keys may “unlock” the encrypted information. The digital keys most often take the form of a token which may be incorporated into browsers, biometric identifiers, smart cards and other storage devices depending on the complexity or sophistication of the particular application. Encryption software varies widely, both in terms of available strength[13] and functionality.

Encryption products that combine hardware and software solutions are popular, especially in complex or advanced communications solutions, telecommunication equipment, copyright protection schemes, biometric authentication, smart cards and some firewall products. Hardware-software solutions for individual use, however, are relatively uncommon at this time.

Encryption software can be very useful for the individual user. Not only can encryption protect individual stored files, it can also be used for authentication purposes and to ensure private communications. A powerful tool, encryption can be used in a wide variety of circumstances to provide privacy and security for an individual user.

At the same time, users unfamiliar with sophisticated technology may find encryption products difficult to use. Even relatively advanced, user-friendly encryption products designed for retail distribution may be confusing for those unfamiliar with the technical capabilities afforded by encryption technologies.

Software publishers have developed widely varying products. Effective use of encryption generally requires some effort on behalf of the individual user.

Even so, encryption products and the integration of encryption into standard consumer applications creates an effective and efficient tool that can significantly enhance consumer privacy and the security of an individual's data. Empowering users with robust PETs requires the availability and usability of strong encryption.

Encryption software is widely available and comes in many forms, including hard disk or file encryption, e-mail encryption, personal firewalls, authentication tools and communications utilities.

Web-based technologies

Anonymizers

Anonymizers are web-based services that offer anonymous web surfing by acting as an intermediary between the client and the web site. Generally, an anonymizer service prevents a web site from being able to identify the IP address of the visitor or planting cookies on an individual's computer. However, for that very reason, anonymizers may also prevent a user from accessing personalised services or taking advantage of certain functionality that requires persistent cookies in order to function properly, such as online account access or using purchase histories.

Anonymizers can be extremely useful for consumers browsing the web or for sending anonymous e-mail. Simple and easy to use, anonymizers are widely available on the web and, in many cases, may offer some version of their services for free. For those seeking to keep their web surfing habits confidential, anonymizers can be an excellent choice.

It is worth noting, however, that anonymizers do not necessarily guarantee that personal information will not be disclosed. Just because a transaction is anonymous does not mean that it is private. Because the anonymizer acts as a go-between an individual Internet user and the web sites or other Internet services he or she is using, data in a server log could be used to recreate a user's surfing habits. While anonymizer services implement business practices that prohibit such practices – such as regularly deleting their web logs and not keeping backups of system files that may disclose personal information or be used to help identify an individual – anonymizer services are not inherently foolproof.

In addition, anonymizers create certain concerns for law enforcement officials or others charged with ensuring responsible online usage. Because anonymizers can hide the identity of an individual – or at least make it very difficult to determine an individual's identity – anonymizers raise concerns about accountability or the enforceability of online usage policies.

Anonymous e-mail services are also widely used, allowing users to send e-mail without disclosing their own e-mail address or the originating e-mail address. A resource page can be found at http://www.publius.net/rlist.html.

Platform for Privacy Preferences Project (P3P)

The Platform for Privacy Preferences Project (P3P) is a proposed standard developed by the World Wide Web Consortium (W3C) that is designed to give users more control over their personal information by allowing P3P-enabled browsers and servers to analyse privacy policies. The proposed P3P standard is based on XML[14], allowing the creation of common vocabulary for identifying privacy practices.

Because P3P is a technology built upon the XML platform, it allows browsers and servers to “negotiate” before completing a request for data delivery. Once a web page is requested by a given browser, for example, the browser will only deliver the page back to the user if the P3P preferences set in the browser are matched by the web site. Because a consumer’s preferences are set by the individual and the policies of the site are defined by P3P, users are not required to analyse the privacy policies of every site that they visit.

A company defines its privacy policy in the terms established by the P3P standard. Elements include POLICY, ENTITY, DISCLOSURE, REMEDIES, DISPUTES, STATEMENT, CONSEQUENCE, PURPOSE, RECIPIENT, RETENTION, DATA-GROUP and DATA elements. Each element has required attributes that further define the privacy policy of the covered site. The combination of core elements and different attributes creates significant flexibility for both web sites and consumers. With a wide range of possible choices and combinations of elements and attributes, consumers can develop privacy preferences that accurately reflect their own personal choices and communicate those preferences to P3P-enabled web sites.

To assist companies in developing P3P compliant products, several companies have created P3P policy editors or development tools that greatly simplify the development of compliant products.

A user must have software that allows the browser to translate and understand the P3P specification. Once configured to an individual user’s preferences, the interaction of P3P between servers and the individual can be largely invisible to the user, greatly simplifying consumer usage. Here, too, many companies are developing client-side P3P tools that are increasingly available.

P3P is a rapidly advancing standard that is being utilised in a growing number of settings. The growing use of P3P is due to a number of factors.

First, P3P allows a company to define its privacy policy through technology. Doing so directly addresses one of the most fundamental concerns of many privacy advocates, namely that many privacy policies are difficult for users to understand or that users may not comprehend the full implication of the legal or complex language often found in privacy policies. P3P eliminates a great deal of confusion as the terms are fixed.

P3P also allows a user to define his or her privacy preferences technologically. The user can configure his or her software to reflect what information, if any, he or she wishes to disclose and how the data can be used. Such flexibility allows a user to establish the boundaries of PD collection based on what he or she feels is appropriate. The ability of a consumer using P3P to create a privacy profile that reflects his or her personal, national or cultural preferences greatly empowers an individual in his or her online activities.

Second, P3P requires little ongoing user intervention. Once a user configures his or her own computer, the analysis of privacy policies at P3P-enabled web sites is relatively seamless. While a user may, depending on the functionality of the P3P client software, on occasion override his or her established preferences in order to access a non-P3P site, the user can be confident that his or her configured preferences will be respected on an ongoing basis.

Third, P3P respects the ability of both companies and individuals to establish different privacy practices. P3P is quite flexible, and allows a company to define its practices and the user to define his or her data collection preferences. P3P empowers individual users to create a unique set of privacy preferences while at the same time using technological safeguards to ensure that those choices are respected.

P3P is still emerging as a viable technology in a rapidly evolving market. Many companies have committed to the integration of P3P into their respective product lines, but P3P implementation remains relatively limited.

The limited adoption of P3P by the marketplace to date is attributable to the still evolving nature of the private sector standards process, the need to respect the fact that a diversity of business models operate globally on the Internet and the traditional pace of technologies that are heavily influenced by network effects. At this time, the only browser that is P3P compliant is Internet Explorer 6 by Microsoft. Consumers with P3P client tools will find that for now, relatively few sites have implemented P3P privacy policies. If a user limits his or her preferences to only visit P3P-enabled sites, he or she may find that their online browsing options are limited. At the same time, companies considering P3P may determine that because of the lack of widespread P3P client tools the investment in retooling their own web sites and privacy practices may not be justified at this time.

Network effects in the technology market are well-documented and well-understood. Inevitably, it will take some time before P3P usage becomes widespread. At the same time, given the support of P3P by a key Internet standards body (W3C) and the broad support and interest in P3P in technology, privacy and consumer communities, many believe that P3P will achieve critical mass in the near future.

A listing of participating sites can be found at http://www.w3.org/P3P/compliant_sites.

Privacy networks

Privacy networks, like anonymizers and proxy servers, prevent a web site from seeing the identity of the web site visitor. However, many of these services have added features that distinguish them from relatively simple anonymizers.

Privacy networks generally rely on the use of pseudonyms or alternative identities. A user generally has an account with the service provider that contains his or her true identity. The service provides the user with a pseudonym that may or may not include accurate demographic information. The user then uses the subscriber network to host its home page, Internet service provider or web surfing starting point for any Internet session. The privacy network reveals only the pseudonym identity to any web site that the user visits.

Typically, privacy networks provide users with significant choice about what information is revealed about them. Some users may choose to include, for example, basic demographic information, allowing web sites that they visit to know their age, gender or geographic location; other users may choose to block this information from being shared.

A privacy network will typically store cookies served to the user on the privacy network, preventing the delivery of cookies to the individual’s computer. The privacy network thus enables users to utilise customisation, personalised services and other convenience benefits without having to have such information stored on their personal computer hardware.

Privacy networks may be Internet-based services, where the individual user subscribes to the service and accesses the services through his or her own Internet service provider. Alternatively, some privacy networks are making their technologies available to large corporate customers, including privacy corporations that wish to limit the disclosure of private information about their employees to third parties, or to Internet service providers who wish to incorporate such services into their own offerings.

For many users, privacy networks offer significant promise because they allow an individual to reap the benefits of personalization and customised services without compromising personal privacy. Consumers inherently understand that companies need data about their markets and appreciate corporate interest in using that data to improve and enhance their products and services. The ability to create an alternative identity that reflects an individual’s choices, preferences and demographic information without having to disclose more personal details to an online site – such as home address or phone number – is an attractive solution for many. Many see privacy networks as an effective tool in balancing these competing interests.

In the corporate market, many network and Internet service providers consider the use of privacy network technologies as a benefit that they can provide to their individual consumers. For many, implementing such tools is considered as a competitive advantage that will enhance their own offerings. While integrating these technologies into a corporate or ISP network is technically complex and generally requires a significant investment, many companies believe the investment to be a cost-effective approach to addressing consumer concerns and helping their consumers make informed choices about privacy and data protection.

Information brokers

Information brokers – often referred to as infomediaries, account aggregators or other terms – are companies that act as a broker for personal information. Because this market segment is evolving, there are several different approaches encompassed within the concept of an information broker or infomediary. This description attempts to provide a broad overview of the various approaches.

The information broker or infomediary approach has been both sharply criticised and widely praised as a viable alternative for individuals seeking to protect their own privacy. This paper does not make a value judgement on the business models of these companies. In light of the fact that some industry observers view this approach as a positive addition to the protection of personal data, it is noted that these tools do meet the basic definition of a PET in that these services attempt to ensure that consumers have greater control over the disclosure of their personal information.

Brokers or infomediaries are typically subscription-based or fee-based services. An individual creates an account with the company, which then tracks through software an individual’s online actions, including surfing habits, purchasing history and other data. The services serve as the primary repository of this information.

The individual, however, remains in control of the information, and may direct the company to share information with a particular site and deny information sharing with another. The broker acts on behalf of the individual, not the vendor, and can provide significant consumer benefits and conveniences because of the wealth of information collected. In addition, these companies are significant sources of demographic data for corporate marketers who may be interested in analysing non-personal information about a particular market segment. Through data analysis, the company can provide demographic information without having to disclose PD of individual clients.

If an individual determines that he or she no longer wishes to have the company act as a broker on his or her behalf, the user can cancel the service or subscription. Once the service is cancelled, the information is generally removed from the company’s database.

Intelligent agents or software “bots,” applications that can act on behalf of a consumer based on his or her expressed preferences, are similar, but not covered in detail in this paper.

Some privacy advocates argue that while the broker concept may empower users, significant risks remain because these companies are largely unregulated (except to the extent that they collect sensitive or legally regulated information) and that consumers must rely on the stated policies of a private company for reassurance that their data will be protected. Those that believe they offer a viable alternative for consumers note that the business model of a broker is entirely dependent on the company creating a trusting relationship with individual consumers. The market, they argue, will ultimately ensure that these companies do not violate the privacy of their customers. The powerful forces of a competitive market create a strong incentive for these companies to rigorously respect the preferences of the individuals they represent.

This remains a relatively small market at this time, and it is unclear whether consumers that are unwilling to trust a company with a posted privacy policy will be any more willing to allow the broker to collect their personal data.

Network-based technologies

Many privacy-enhancing technologies can be deployed on corporate networks, private LANs or WANs. These technologies allow corporate or large-scale network managers to limit the information disclosed from individuals on a given network.

Proxies and firewalls

Proxy servers and firewalls are technologies that typically are located between the individual consumer and the Internet. In a corporate environment, they may be located on the local area network (LAN) at the point where the LAN is connected to the Internet, at the ISP, or somewhere in between. Proxies and firewalls can also greatly enhance security in a network environment.

Firewalls and proxies are quite similar in terms of their functionality, though firewalls typically include additional security features not found in proxy servers.[15] Generally, however, both can prevent the disclosure of an individual’s IP address or other personal information by acting as an intermediary between a web site and an individual computer.

The key difference between firewalls and proxy servers is how they deliver information to an individual browser. Information requested through a firewall – whether it be a web page or streaming video – is delivered directly back to the individual user. The firewall may scan for viruses, restrict certain types of content or implement additional security features, but the information is sent back to the individual computer that initially requested the data.

In a proxy environment, the proxy server acts on behalf of the individual user and hides the identity of the client computer from the web site. When an individual requests a given web page – www.oecd.org, for example – he or she is actually passing the request to the proxy, which in turns makes the request to the actual OECD web server. The OECD web server, in this example, would deliver the page and information back to the proxy, which in turn delivers the page to the individual user.

These technologies are widely deployed on corporate networks. They are readily available, often bundled with network, web site and other Internet products and services. Firewalls for individual PCs are also widely available on the retail computer software market. Because these products were originally developed for security purposes, their functionality and flexibility are often not as robust as other products developed specifically to address privacy issues. However, their widespread usage and deployment ensure that they will remain at a minimum a crucial element of any privacy-enhancing technology solution.

Proxies and firewalls are widely available from computer security firms, and are often bundled with network or web software.

Privacy networks

Privacy networks are described in detail above. Of note, however, is the fact that many privacy network companies are working with Internet service providers, corporations and popular web sites to incorporate privacy network technologies to provide these types of services to their own employees, customers or subscribers. Privacy networks, then, need not only be Internet-based services for individual consumers, but may be integrated into the closed networks of various organisations or businesses.

In addition, many companies that offer online services are providing new capabilities for their consumers that provide additional control over personal data. Microsoft's Passport services and AOL's Magic Carpet – both of which give consumers new options in how each service uses their PD – greatly simplify the online experience by remembering consumer preferences, eliminating the need to re-enter repetitive information and increasing the opportunities to provide the consumer with a friendly, familiar and seamless online experience. While some concerns have been raised about the comprehensive nature of these services – Passport, for example, is being widely deployed on both Microsoft and non-Microsoft owned web sites – the convenience afforded to an individual user at all of his or her favourite sites is compelling for many users. But as with any online service, the user should carefully check, review and evaluate the options available to him or her in the service's respective privacy policy to ensure that he or she is comfortable with the uses, choices and options available to him or her.

3. RECOMMENDATIONS

The 1998 OECD Ministerial Declaration established that PETs can play a crucial role in giving users greater and more flexible control over personal information. The OECD has consistently recognised since then the importance of PETs in numerous declarations, papers and conference documents, as outlined throughout this paper. In encouraging the use of PETs, both governments and the private sector have important roles to play.

The use of PETs in implementing national law

Policy makers have long questioned whether PETs can play a role in implementing data protection laws and if so, to what extent technology can address the issues raised in such regulation. To some extent, the answer to this important question is yes, PETs can serve an important purpose. However, it is important to realise that PETs cannot alone address the requirements of data protection laws.

PETs can significantly empower consumers concerned about data collection. Privacy is an inherently personal issue, and each individual consumer may have very different privacy preferences. And while national laws may establish baseline data protection rules, consumers will inevitably have unique preferences about data that may or may not be collected about them. Here, PETs can serve as an important complement to national data protection laws for those consumers with specific concerns or who prefer more privacy than the general law allows.

At the same time, however, PETs cannot implement every national data protection law or even broad international guidelines. There are simply too many differences in national laws, exceptions in certain circumstances, nuances or differing treatment for disparate types of data for any single technology (or even combination of different technologies) to address the myriad of rules and regulations that inevitably accompany data protection laws. Generally, software applications and technologies address very singular and/or specific concerns, while data protection laws cover a wide variety of PD in a wide variety of circumstances. As a result, PETs are ill-suited to be utilised to implement what are often very broad, comprehensive national laws.

However, PETs can play some role. CEN (Committee for European Standardization) has undertaken a comprehensive review of whether technology standards can be used to implement the EU Data Directive. As work here continues, there may be the opportunity to use PETs to support the implementation of the EU Data Directive (though it may not address US or other national laws), and may encourage the development of other standards to address different regulatory initiatives.

PETs should be seen, then, by both governments and consumers, as a secondary tool for privacy protection. Consumer engagement – namely checking privacy policies and establishing one’s own privacy preferences – are crucial elements without which PETs are largely ineffective. In addition to national law (where consumer and governments determine such an approach is appropriate) and proactive consumers, PETs can be beneficial.

In addition, there are constructive ways that governments can support the development and use of PETs, including:

- Ensuring consumers that users of PETs are not discriminated against in criminal or civil investigations. There is a natural tendency to believe that a consumer who uses robust encryption or anonymizing technologies, for example, on his or her computer must be "hiding something." Data protection laws should recognise that consumers who opt to use such tools may simply be protecting the accidental disclosure of their personal information and not hiding activities of concern. While this may create difficulties for law enforcement or investigating personnel, the ability of individuals to use PETs should be protected.

- Recognise the important role that PETs can play in assisting individual consumers to implement their personal privacy choices in any data protection or privacy related legislation. Such efforts will help raise awareness about the availability of PETs for consumers who may not be aware of their existence.

- Data protection policies should look favourably on web sites that utilise or make available PETs to their consumers. Whether a site provides robust choices for a consumer or incorporates privacy tools into its own infrastructure, companies that take these additional steps to help empower consumers should be given favourable consideration in consumer complaints or other similar situations.

- Web sites should not be allowed to discriminate against consumers who deploy PETs, except in cases where the PET prohibits the site from meeting consumer requests. For example, a site should not refuse to display for a consumer simply because he or she chooses not to accept cookies. However, the site should be free to deploy whatever technologies or tools it chooses to be most appropriate. For example, just as a hotel that requires a credit card or other deposit for advance reservations should not be required to hold a room for a consumer who refuses to provide such information, a web site should not be required to provide customised information or facilitate online purchases in the same situation if cookies are the technology deployed by the site and the user chooses not to accept cookies except where the use of cookies provides functions beyond personalization or marketing – such as maintenance of a shopping cart or enhanced security.

Private sector initiatives

The private sector has also long recognised the important role that PETs can play. The wide variety of PETs available demonstrates that companies are responding to consumers seeking such empowering tools. Companies using the Internet understand that privacy concerns pose a barrier to the future growth of electronic commerce. As the private sector seeks to address consumer's concerns and eliminate barriers to future growth, a wide variety of robust PETs for individual, Internet and network use are increasingly being deployed to enable consumers to make informed choices about the collection and use of personal information.

The private sector can evaluate the feasibility of more widespread use of PETs to support the objectives of policy makers interested in exploring the viability of PETs to protect personal privacy. In particular:

- Businesses should evaluate whether incorporating PETs into their corporate networks will help protect the privacy of their users (*i.e.* providing privacy to corporate users). Similarly, Internet service providers should consider whether making PETs available will help alleviate many of the privacy concerns expressed by subscribers.

- Consumer and business organisations should work, in conjunction with governments and public sector organisations, to educate consumers about the availability and use of PETs.

- e-Commerce and other online sites that collect personal information should evaluate whether integrating PETs such as P3P into their own sites is feasible and useful to their consumers.

- Technology companies should consider how privacy-enhancing technologies can be better incorporated into standard online tools, such as browsers, FTP clients and other access-oriented software, hardware and handheld devices.

Conclusion

The private sector and policy makers have long recognised the importance of PETs in aiding consumers in making informed choices about privacy. The OECD has reaffirmed this in several declarations, conference papers and studies in recent years. The consistent recognition of the role of PETs by policy makers has encouraged both consumers and companies to focus attention on PETs and their continued development.

As the market continues to develop a wide variety of robust tools, consumers must be made aware of the utility of PETs. Industry, private sector organisation and governments can help consumers learn about PETs, understand their role in aiding individuals in protecting personal information, and encourage their use. Such efforts can only serve to enhance consumer confidence and support the continued growth of electronic commerce and ensure that the attendant benefits are widely shared among all online users.

NOTES

[1] Van Dusseldorp & Partners reports that current high-speed Internet access subscriber penetration throughout Europe is 1.79%, but will rise to 21% by 2003. According to the UK-based research firm Arc Group, http://www.the-arc-group.com, the fixed wireless market will expand rapidly beyond Europe and the US over the next few years. By 2005, Europe will account for USD 11 billion of the market, the United States for USD 9 billion, and the rest of the world for USD 22 billion.

[2] NUA Internet survey, available at http://www.nua.ie. Reported in “Privacy, Security Major Concerns for US Consumers,” October 6, 2000.

[3] However, it should be noted that at least some consumers believe that they have more control today over their personal information than they might have had in the past. The 1999-2000 Annual Report from the Canadian Privacy Commissioner’s Office found that “In general, Canadians appear to be less concerned about privacy than they were in the 1992 study. By 1999, 47% of Canadians agreed with the statement, "I feel that I have less personal privacy in my daily life than I did ten years ago," compared with 60% in 1992. The number of Canadians who agreed with the statement, "There is no real privacy because government can learn anything it wants about you," dropped to 63% from 81%. The number of Canadians who agreed with a similar statement about business dropped to 57% from 71%. The 1999 study suggests that Canadians are also becoming more sophisticated in their attitudes towards privacy. Fifty per cent said that they now "feel confident that they have enough information to know how new technology might affect their personal privacy", up from 43% in 1992. A majority of Canadians (54%) don't mind companies using personal information as long as they know about it and can stop it. Canadians may be willing to provide personal information in certain circumstances, and may even be willing to sacrifice some of their privacy, but they want to know what they are getting in return. One thing they want is control.” Available at http://www.privcom.gc.ca/english/02_04_08_e.htm.

[4] This is commonly referred to as “clickstream” data.

[5] Generally, the cookie contains the session ID. The session ID is a identifier created by the server that identifies the session. In some cases, the use of a cookie may protect privacy. Consider a situation where a user logs into an online account. A cookie set with a “time out” after a pre-set period of time helps prevent the accidental disclosure of data if the user forgets to log out of a site or is using a shared computer.

[6] Internet “RFCs” are technical protocols and standards drafted and written by the Internet Engineering Task Force, the IETF. RFC stands for Request for Comment.

[7] This functionality is determined by the web browser settings, which limits which web sites can read cookie information based on these common, standard implementation practices.

[8] HTML stands for the HyperText MarkUp Language. HTML is the standard language used to develop web pages.

[9] Cookie blockers are one form of PETs that give users greater control over the placement of cookies on a user’s PC. They are described in greater detail in the section on PETs below.

10 FTP stands for File Transfer Protocol. FTP was one of the early services available on the Internet, used for sharing files among computers across public networks. Plug-ins are applications that support additional web services, such as sound or video.

11 The concept of a "technology community" is a broad one and has no generally accepted definition. However, for the purposes of this paper, the term refers to software developers, information technology professionals, and others involved in the creation, implementation and deployment of technology solutions.

12 Data in cookies is typically coded, encrypted or stored in a format that is not easily recognisable to the user. Some have asked why information stored in cookies is not readily decipherable. The reasons are numerous. First, such data is generally coded in a way to minimise the amount of data that is stored in a cookie, minimising data transfers and speeding the user experience on what are often relatively slow data connections. Second, data that is coded is not accessible to other web sites, and helps protect to some extent the operational nature of a given site from competitive sites. Third, coded data is less likely to be stolen or intercepted by a third party who, like the user, would be unlikely to understand the encoded data. A cookie that includes "USER=8023" is far less likely to identify an individual than "USER=JaneSmith". In this way, the coded data actually may enhance privacy in those situations where personal data may be stored in a cookie as it creates a disincentive for a third party to try and collect data stored on a user's computer. Finally, coded data may prevent a user from altering the settings stored in a cookie, ensuring that its intended use – such as storing account login information or personalization preferences – is not accidentally lost.

13 The longer the bit length of the key, the stronger the encryption. Most security experts agree that at a minimum, 128-bit encryption is necessary to protect data. Commercial encryption routinely uses stronger key lengths, and personal encryption tools with 1024-bit length keys are available.

14 XML, or Extensible Markup Language, is a standard defined by the W3C that provides context to web site data. HTML, HyperText Markup Language is the language used for creating web pages, but is relatively primitive in that it can only control how information is displayed. XML can define what data means in the context of the web page or how it relates to other data, greatly increasing the functionality of a given web page and its data interoperability with other sites, databases and online applications.

15 Firewalls, for example, may incorporate the ability to disable certain services such as FTP, close specific ports, or provide advanced intrusion detection technologies.