4

"Customizable Privacy": A New Approach to International Regulation of the Internet

*Nathaniel Heller**

This paper examines the growing divergences in the regulatory regimes governing e-commerce and electronic privacy in the major commercial markets – the United States, the European Union, and Japan – and suggests that the existing regulatory frameworks are not sustainable as a long-term international regime. The paper then suggests a new approach to governing international e-commerce and Internet privacy, known as "customizable privacy."

Introduction

The explosive growth of the Internet and e-commerce in recent years has presented national regulators with the difficult task of devising regulatory regimes that balance the needs of consumer privacy against the needs of businesses to tap the inherent efficiencies of the Internet. One of the great strengths of the Internet and e-commerce is the ability of firms to make available to consumers personally tailored product sets and services based on the preferences of each individual user. Hence, each time a user logs on to Amazon.com, she is presented with a list of CDs that the site believes she would be interested in purchasing based on her previous purchases on the Web site.

But such customization presents extreme challenges to personal privacy, even cases where the use of such personal data is seemingly innocuous. For instance, many hospitals have begun to equip certain wards with digitized "charts" to replace the traditional paper versions used by doctors to monitor patient progress. There are many private

Nathaniel Heller, School of Foreign Service, Georgetown University

sector firms and not a few public health experts who argue for linking up hospitals to a nationwide data exchange network that would allow any doctor in the country, particularly in the emergency room, to instantaneously look up a patient's medical history and allergies. But how do governments and regulators ensure that those same hospitals do not sell such data to insurance companies, who could then proceed to adjust medical insurance premiums to reflect certain prognoses?

What if this network became global, linking all hospitals around the world? Whose "rules" would a given hospital follow? The local country's, those of the patient's home country (as with a tourist who falls ill), or some supranational set of rules and regulations agreed to by all countries? Clearly, the pace of Internet regulation has not kept up with the pace of international Internet-based business. Until the right approach is found for regulating the Internet across borders (its inherent nature anyway), users around the world will be stuck conducting commerce and communication in an environment that is poorly protected and ripe for abuse. Worse yet, the histories of Internet regulation in the major world markets are vastly different, providing national regulators with the challenge of developing regulatory frameworks that apply equally well to disparate users and markets.

Given the fact that widely different regulatory regimes govern the major commercial regions of the world and that those regimes are often at odds with each other, a new approach to governing privacy on the Internet must be found. The Internet is by nature a global, individual-empowering phenomenon. An effective regulatory regime for Internet privacy, therefore, should be applicable worldwide while also respecting individual consumer preferences. One such approach, developed below, is that of "customizable privacy."

History of Privacy Protection in the United States

The right of privacy, as a legal claim enforceable in law, is part of the historical tradition in the United States. In 1890, Samuel Warren and Louis Brandeis argued in a *Harvard Law Review* article that privacy was the most cherished of freedoms in a democracy. These lawyers suggested that "recent inventions and business methods" and the pressures of modern society require the creation of a "right of privacy" which would protect "the right to be let alone" (Warren and Brandeis 1890, 193). This right of privacy outlined by Warren and Brandeis came to be known as the 'American Tort.'

Historically, the United States has developed privacy rights, enforceable by law, to address public concerns. However, recent government administrations have been unable to adequately coordinate online privacy policies in the wake of the rapid changes that have occurred in technology. There are hundreds of privacy measures pending before Congress every single day. Some bills address the privacy rights related to medical records. Others extend privacy protection for financial data. There are even bills to protect the privacy of genetic information, as well as proposals that would preserve general consumer privacy.

Domestic Demand for Privacy Protection

Today, there is a growing demand for privacy protection in the United States. In a study at the beginning of the online boom, the respected Harris pollsters found that of people who were not online, 70 percent indicated they would be inclined to start using the Internet if "the privacy of [their] personal information and communications would be protected (*Privacy and American Business* 1998, 6)." In light of this statistic, it is not surprising that only a quarter of Internet users purchase items online (IntelliQuest 2000). Another Louis Harris & Associates study found that 53 percent of Americans believe that the "government should pass laws now for how personal information can be collected and used on the Internet." Of those polled, 23 percent said that the "government should recommend privacy standards for the Internet but not pass laws at this time." A mere 19 percent believe that the government "should let groups develop privacy standards but not take any action now unless real problems arise (Louis Harris & Associates, 1998)." Additional empirical evidence follows:

- In 1998, Alan Westin, a leading privacy scholar and professor of Public Law and Government at Columbia University, found that 81 percent of Internet users were apprehensive about the invasion of privacy online (Harris and Westin).
- In 1998, a seminal study by AT&T researchers sampling more than 350 people found 87 percent of experienced Internet users were somewhat or very concerned about threats to their privacy online (Cranor, Reagle, and Ackerman).
- In 1999, 70 percent of respondents in a national survey conducted by the National Consumers League reported that they were uneasy about providing personal information to businesses online (Harris & Associates, 1999).

- In December of 1999, a Cyber Dialogue study found that more than one-third of Internet users believed that the online submission of personal data was an invasion of privacy (CyberDialouge).
- In a survey taken in September 1999, Americans were asked by a *Wall Street Journal-NBC* poll what they feared most in the 21st century. Options included terrorism, overpopulation, and global warming. It is remarkable that the loss of privacy received 29 percent of the vote, the largest share of responses (Swire 1999).

The now infamous example of DoubleClick further attests that Americans are concerned about privacy protection on the Internet. Double Click, an online advertising firm that captures information on consumer behavior, purchased Abacus Direct, an offline company that maintains a large database of personally identifiable information. In early 2000, DoubleClick announced that it would cross-reference online customer information with Abacus Direct's offline database. Within weeks, it faced four lawsuits due to alleged violation of privacy. Further, the Center for Democracy and Technology launched an e-mail campaign against some of the Web publishers that belonged to the Double Click network. These companies included *The New York Times*, Alta Vista, and Comedy Central. Over 4000 e-mails were sent to publishers asking them to refrain from providing DoubleClick with personally identifiable information (Parker 2000). Ultimately, DoubleClick renounced its intention to cross-reference information, and the Federal Trade Commission, which had launched an investigation, did not pursue further action.

International Pressure for Privacy Protection

Privacy is a fundamental human right recognized in all major international treaties and agreements on human rights. The United Nations Declaration on Human Rights acknowledges privacy as a basic right internationally. It states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Similarly, the right to privacy is recognized in the International Covenant on Civil and Political Rights, where Article 17 states, "No one shall be subjected to arbitrary or unlawful interference with his privacy...everyone has the right to protection of the law against such interference or attacks."

Empirical suggests that citizens around the globe are calling for more robust privacy protection measures. A survey from the Graphic, Visual-

ization, and Usability Center (GUV) reveals that 72 percent of Internet users worldwide believe there should be new laws to protect privacy on the Internet. The poll also found that 82 percent of users object to the sale of personal information. The survey suggests a sharp increase in privacy concerns since the last GVU poll and that privacy in the United States is the highest priority concern for Internet users (GVU 2000).

In addition, the October 1999 IBM Multi-National Consumer Privacy study conducted by Louis Harris & Associates reveals that most Internet users (63 percent worldwide average) have refused to furnish information to Web sites when privacy policies are unclear or misuse of private information is perceived (IBM 2000).

European Dimensions

The European Union (EU) has been well ahead of U.S. efforts to develop a unified Internet regulatory regime. On October 24, 1995, the European Commission (EC) published the Directive on Data Protection (95/46/EC), an attempt to unify the data privacy regimes of the separate European Union countries and enact a comprehensive set of regulations. The European approach differs markedly from the American system, where the regime consists of unrelated laws ranging from financial data protection to health records to laws governing the rights of children on the Internet.

The European approach to regulation of the Internet provides many more rights for the user than does the *ad hoc* American regime or the emerging Japanese one (see below). After the Data Directive went into effect in October of 1998, any company in any country using personal data of an EU citizen had to comply with various conditions. These stipulated that personal data could only be used if it was collected for identifiable purposes, was not used for purposes other than the originally stated intentions, and if the user gave consent. Furthermore, the subject of the data can demand to know at any time what data has been collected and what it is being used for. He or she can also demand that the data not be used for direct marketing purposes (European Commission 2000, Sections II, IV, V, VII, and IX).

The most important and severe implication of these requirements came in Chapter IV, Article 25 of the Directive, which spelled out the consequences of a violation of the new data privacy standards. In the event that a non-EU country is deemed by European authorities to not meet the new levels of privacy protection, the Directive requires EU member states to take action to stop the flow of information to the third-party country. This draconian response was what led to the immediate start of negotiations

between United States and European authorities to prevent a European data embargo on the United States.

Were the Directive's mandates implemented literally, all Internet traffic involving any private data would have ceased on October 1, 1998 between the United States and the European Union. Obviously, both sides had a vested interest in avoiding such an embargo and worked to find a solution. Eventually, the United States and European Union reached a middle ground known as the Safe Harbor Principles. This was a self-regulatory mechanism managed by the U.S. Department of Commerce. Via Safe Harbor, American companies can self-certify that they have implemented privacy protections to the satisfaction of the European standards. The list of Safe Harbor companies currently in compliance is small but continues to grow and includes many large American technology and Internet companies (United States Department of Commerce 2002).

The Safe Harbor negotiations were often acrimonious and took almost two years to complete by the time they were settled in July 2000. Furthermore, the solution provides little more than window dressing in the form of American self-certification. There are no provisions in the agreement for oversight agencies, enforcement procedures, or dispute settlement mechanisms. In short, the Safe Harbor negotiations are an excellent example of how differing regulatory regimes can create substantial problems in international e-commerce.

The Japanese Example

Though Japan boasts some of the most cutting-edge Internet technology, its Internet regulatory regime is far less robust than those of the United States and the European Union. Japan's approach to Internet privacy has historically centered on guidelines issued by the Organization of Economic Cooperation and Development (OECD) in 1980. These guidelines have formed the basis for a variety of other international data protection regimes, including the ad-hoc U.S. regime. Among other principles, the OECD rules dictated that all data be collected in a fair and lawful manner with the consent of the user; that the data be relevant to the purposes for which it is used; and that it not be disclosed except with the consent of the user or by authority of law (Unites States 1998). The Japanese government released its own version of privacy protection based on the OECD Guidelines in 1989 entitled "Concerning the Protection of Computer Processed Personal Data in the Private Sector (United States 1998)."

The expansion of Internet use in the 1990s gave rise to new fears about personal data infringement and led to many new efforts from developed nations to strengthen personal data protection (MITI). As noted above, the EU's Directive banned the transfer of personal data to third countries if they did not offer an adequate level of protection. In light of these developments, Japan's Ministry of International Trade and Industry (MITI) organized a "Working Group on Privacy Issues" that was charged with revising the 1989 guidelines (MITI, 2). The revised guidelines, released in March 1997, allowed for increased consumer access to their information, auditing mechanisms, and measures to improve consumer education (Unites States 1998).

The Japanese government promoted a self-regulatory approach towards implementation of the new rules (MITI). MITI intended for the private sector to develop voluntary measures to regulate itself based on MITI's guidelines. In keeping with this policy, Japan's Cyber Business Association created the "Guidelines for Protecting Personal Information in Cyber Business" in December 1997, concerning the handling of personal information in Internet-related commercial transactions (Cyber Business Association 1997). These guidelines closely mirrored MITI's. There were however, some key differences.

The Cyber Business Association's guidelines stressed that although browser numbers and access logs could not be used to directly identify an individual (and thus are not defined in MITI's rules as "personal information"), they could be cross-referenced with other data to identify individuals. Hence, the guidelines emphasized the need to make clear to users that this type of information can be collected and used, and that this information could be indirectly used to identify individuals (Cyber Business Association 1997). Moreover, these guidelines encouraged member companies to inform users about how this personal information was collected and used (Cyber Business Association 1997).

Another example of Japan's self-regulatory approach is embodied in the Japanese Direct Marketing Association's (JADMA) guidelines. While following the basic structure of MITI's restrictions, JADMA inserted some important additions.

According to JADMA's rules, personal data containing information about a user's race, family lineage, religious beliefs, health records, and sexual habits should never be collected (JADMA 1998). Member companies are also required to obtain consent from data subjects when they collect personal data by furnishing a written notice. Furthermore, the JADMA rules stress responsibility when lending personal data to a third

party, a common occurrence in e-commerce when two firms partner to provide a single product or service to a customer.

In recent years, however, the Japanese government has taken a more active role in privacy protection. In February 1998, MITI established a Supervisory Authority for the Protection of Personal Data to monitor a new system granting "privacy marks" to businesses committed to the protection of personal data in accordance with the MITI guidelines (Privacy International, 1). The agency responsible for administering the privacy marks, the Japan Information Processing Development Center (JIPDEC), is a joint public/private agency. Companies that do not comply with industry guidelines will be excluded from relevant industry organizations and will not be given the privacy mark. The assumption is that market forces will punish the negligent firm. The role of the Supervisory Authority is to actively investigate violations and make suggestions to industry authorities. Some observers view this approach as government-directed co-regulation rather than voluntary self-regulation (Greenleaf 1998).

Following the trend in Japan moving away from industry self-regulation and toward government intervention, the Japanese government passed legislation in 2001 that holds corporations accountable for information gathered over the Internet. The law, known as the Personal Data Protection Bill, is the first piece of Japanese legislation to regulate the unlimited use and unauthorized sale of personal information on the Internet (Nikkei Weekly 2000). Companies that fail to improve data management practices would face prosecution.

The key concept of the bill is to place responsibility on companies for protecting data. Previously, only individuals who mishandled personal information were prosecuted. Now, however, the companies that employ such violators will also be held liable for failing to prevent abuse of data. The law follows the basic framework of the original OECD Guidelines of 1980, especially with regard to limitations on data collection and use. It makes provisions for the fair and lawful collection of data and limitations on the purpose and use of the information. It also calls for proper management of personal data. This means that companies must keep the information up-to-date and must supervise employees who come into contact with this data (Japanese Embassy, Washington 2000). Further, it includes a restriction on the transfer of personal data to a third party unless the user consents or ownership of the company is transferred.

The law also calls for a degree of openness in transactions using personal data. Companies are obligated to provide individuals with the purpose for which the information will be used, the name of the employee responsible

for the data, and the procedures necessary for individuals to access their information. Moreover, employees shall disclose personal data to those individuals who request it (assuming the data is theirs).

Finally, the legislation obligates companies to set up a structure to settle disputes about the processing of personal information. In terms of enforcement, the law maintains that the authorities concerned shall collect reports from corporations and order them to suspend processing if a violation is detected.

While the government has expanded its influence over the regulation of Internet privacy, some in Japan fear that personal privacy protection may actually be *eroding.* The Communications Interception Law, passed in 1999, allows Japanese law enforcement officials to access private e-mail accounts in investigating crime (Global Internet Liberty Campaign Newsletter).

So far, this law has been widely unpopular in Japan. Polls showed that a majority of the public did not support the bill for fear of privacy loss. In July 2000, over 100,000 people signed a petition for the repeal of the law (APC Networks 2000). Many ISPs and privacy groups have joined the fight because of privacy concerns or because of the burden it could place on their companies. Under the statute, government agents must include an observer from the ISP at all times during the tap. However, several corporations, including NTT DoCoMo (the country's largest mobile telecommunications carrier), are refusing to send such witnesses (Global Net Liberty Campaign Newsletter 2000) out of protest. Meanwhile, Internet privacy groups, such as Japanese Net Workers Against Surveillance Taskforce (NAST) have organized public protests asking legislators to repeal the new law (The Industry Standard 2000).

Similarly, journalists are protesting the above mentioned Personal Data Protection Bill, claiming that a clause in the bill would allow the government to censor journalistic exposes and prevent unpopular stories from being published. The furor stems from language in the law that exempts news organizations from being prohibited to sell personal information of a third party. Without this exemption, the sale of newspapers or magazines containing personal information would be illegal (i.e. a newspaper containing a sex scandal about a politician being sold for 25 cents). However, because the government is the entity that defines what "reporting" is (and therefore what media outlets are exempt) critics claim the clause effectively gives the government a veto over any story of a personal nature (Lai 2001). As a result of these developments, there is an air of uncertainty surrounding the future of Japan's Internet privacy protection regime.

Privacy Protection Options

The differences outlined above between the American, European, and Japanese Internet regulatory regimes are serious. As the Safe Harbor agreement demonstrates, all sides must find ways to ensure that international private data flows do not become subject to conflicting jurisdictions and regulatory hurdles, a development that would significantly harm international commerce and welfare. Against that backdrop, there are at least three ways of addressing and implementing a global regime to govern private data flows on the Internet.

There are two extreme options for international regulation of the Internet: allowing market forces to govern the Internet through self-regulation, or absolute privacy protection mandated through legislation or government fiat. A better, innovative approach to international governance of the Internet is "customizable privacy," which puts firms and users in control of privacy.

Self-Regulatory Protection

Self-regulation entails industry-led efforts to protect consumer privacy by establishing codes of practice. Private sector entities promote a self-regulatory approach to privacy protection due to the transaction cost efficiencies offered by information collection and usage. Capturing customer information lies at the heart of the opportunities offered by the knowledge-based economy.

First, data mining – the ability to capture and organize information in order to predict purchasing patterns– enables targeted marketing. Second, catering to customer preferences by using the information collected about them not only increases the chance that purchases will be made, it also facilitates a more complete customer experience. Third, the transfer of customer data to appropriate members in the supply chain helps to create efficiencies related to demand forecasting. For example, giving information to suppliers enables computer hardware companies to seamlessly integrate the efforts put forth by its partners: chip manufacturers, screen developers, and logistics providers. This practice also allows these companies to accurately forecast inventory levels, creating favorable cash flows.

Proponents of self-regulation believe that the market is capable of meeting all consumer privacy needs. Large corporations argue that customer demand will force industry actors to provide competitive options for privacy protection. To its credit, the private sector has taken multiple initiatives to promote self-regulatory privacy protection. Most

organizations post privacy policies on their websites. Self-enforcement organizations such as TRUSTe, BBBonline, and WebTrust are emerging and provide seals of approval to qualifying companies.

Unfortunately, the evidence shows that self-regulation is not enough. A June 1998 report issued by the Federal Trade Commission (FTC) pointed out that industry efforts to encourage voluntary adoption of fair information practices have not been successful. The Commission's survey of over 1,400 websites found that a vast majority of businesses on the Web- upward of 85 percent – collect personal information from consumers. Only 14 percent in the Commission's random sample of commercial websites provided notice with respect to their information practices. The study evinced that only two percent constitute a comprehensive privacy policy (Federal Trade Commission 1998). A follow-up FTC study in 1999 also found that a vast majority of Web sites fall short of meeting fair information practice standards. This study demonstrated that only a handful of websites are covered by seal programs such as TRUSTe (Federal Trade Commission 1999).

Further, a June 1999 privacy study by Mary Culnan, an electronic commerce professor at Georgetown University, suggests that "an effective self-regulatory regime for consumer privacy online has yet to emerge (Culnan, 2000)." Additionally, the self-regulatory approaches that are promoted by industry and the government are not receiving much support from consumers and users of the Internet. Survey after survey– as outlined above – evinces that Internet users, both in and out of the United States are tired of the fine print on privacy protection.

Absolute Privacy

Special interest groups such as the Electronic Privacy Information Center (EPIC) advocate prohibiting disclosure of private information under almost all circumstances where the user does not know about such disclosure. These organizations are concerned that both private and public sector entities engage in over-collection of personal information. These groups support two approaches to advancing privacy protection: the use of impenetrable technologies and all-inclusive legislation.

Both techniques are not workable and contain especially troublesome international implications. The use of impenetrable technologies such as data encryption raises a host of issues concerning national security and export licensing. Both the Clinton and George W. Bush administrations have come under heavy lobbying from both public interest groups as well software exporters who have argued on opposite sides of the issue. At

varying times, encryption technology has been classified as both a "munition" as well as a normal export that should not be subject to stringent export requirements. Put simply, parliaments and legislative bodies around the world will never be able to keep up with the pace of software development; hence, legislation governing encryption software is untenable.

All-inclusive legislation is equally burdensome and untenable as a method for regulating the Internet. The all-inclusive legislative approach is attractive because it sets stringent privacy standards in a clear manner, creating a baseline for compliance as well as uniform rules of enforcement. Civil liberties groups argue that laws should be designed for the least educated consumer and should apply to all forms of information use and collection in order to ensure that abuses never occur.

However, heavy-handed, blanket legislation is likely to be burdensome for the American economy. The free flow of information is a hallmark of American society and industry and has culminated in significant technological advancements. Allowing privacy protection to become a barrier in commerce would be an unfortunate consequence of legislation. It would not be efficient to require a Web operation to prompt consumers to provide consent each time a particular piece of information is collected.

Online bookstores collect consumer information in order to offer value added services such as customer ratings on books or lists of books that customers with similar tastes have enjoyed. Overarching restrictions on information collection and dissemination to third parties would discourage industry efforts to meet increasing specialized customer demands. Multiple business sectors routinely share information to expand business opportunities and to enhance customer satisfaction. For example, airlines will often share information with partners such as rental car firms or hotels to provide their customers with travel-related discounts. As with encryption, legislative bodies will never be able to shape policy that is flexible and dynamic enough to keep pace with changes in the Internet.

Customizable Privacy

Public-private partnership is key to resolving the legitimate consumer concern of privacy protection. For issues like medical information, it is safe to assume that almost every consumer would want it to remain private. However, clear-cut assumptions cannot be made about other types of consumer profile information. For example, an individual may be completely comfortable sharing that a preference for a coffee whereas another individual might consider this to be her own, and no one else's business.

Consequently, two public policy initiatives are recommended: (1) Policy makers should enact flexible legislation that allows consumers to "customize" their Internet experience to reflect their individual privacy preferences, and, (2) Firms should acknowledge the current market situation where customers are calling for appropriate privacy protection and implement this legislation in a way that would attract customers. Fortunately, there is an approach to developing an effective international Internet privacy framework that both addresses the privacy needs of all users while helping firms to leverage privacy as a "differentiator." This can be thought of as "customizable privacy."

Statutory legislation à propos medical records, financial information, insurance data, social security numbers, and genetic facts should be enacted to protect consumer interests. Beyond those specific instances, a framework of "customizable privacy," described below, should be put in place.

The Privacy Preference Continuum

In designing workable international privacy architectures, regulators should realize that one size does not fit all on the Internet. Privacy preferences constitute a continuum along which all users lie. For some users, giving up private data in exchange for value-added products and services is a perfectly acceptable arrangement. For others, the very thought of providing any sort of private data to a third party is anathema. Between these extremes lie the majority of users. Preferences vary by person as well as by country. According to data gathered by a leading consulting firm only one-third of respondents in the United States said they would be willing to share their location data with third-party companies, even in situations where they could selectively choose those companies. In Japan, however, the results indicated that 60 percent of respondents would share location data, while users in European countries tend to fall in between the American and Japanese scores (Accenture 2000).

"Customizable privacy" is an architecture that allows each customer to specify the degree to which he or she is willing to share private data in exchange for a predetermined and agreed upon provision of services and content. Based on a firm's disclosure of what a customer's private data will be used for and with whom it will be shared, the customer can "opt in" to their preferred level of Internet privacy. The more data the customer is willing to share, the more user-specific and personalized the Internet services and content that can be provided. Public notification on how this information will be used will be provided to all users.

The Privacy Matrix

Private Internet data can be grouped into four categories:

- **Real-time location data**: Where you and your device are right now (this has become a reality with the advent of mobile-commerce and location-based Internet services).
- **Historical location data**: Where you and your Internet device have been in the last minute, week, month, or year.
- **Personally identifiable data**: Data that specifically identifies a wireless user, such as the user's name, address, and contact information.
- **Non-personally identifiable data**: Data that cannot identify a wireless user individually but is used to create an anonymous user profile, such as the type of Internet device, the places or websites visited, and the frequency of those visits.

"Customizable privacy" crosses these various types of private Internet data with different products and services offered by Internet firms and allows each specific user to choose exactly what type of private data they wish to disclose in exchange for predetermined products and services. Conceptually, "customizable privacy" can be thought of as a matrix.[1]

	Service A	Service B	Service C	Service D
Real-time location data	*		*	
Historical location data		*		*
Personally identifiable data	*	*		
Non-personally identifiable data		*		*

As with all privacy architectures, "customizable privacy" is built on the four pillars of fair information practices: notice, access, choice, and security. These practices were made explicit by an advisory committee of the U.S. Department of Health Education and Welfare in 1973 and formed the basis for the Privacy Act of 1974, which protects personal information collected and maintained by the United States government. The four practices also formed the basis for the OECD guidelines set forth in 1980 (United States Department of Commerce 1998).

- **Notice** is given to users as to which private data is to be collected when and with whom it will be shared.
- **Access** is provided to users so they can view and correct any errors in that data.

- **Choice** is offered to all users; they can choose to participate or not participate in a given Internet transaction.
- **Security** is provided by the firm to ensure that the customer's private data is kept from unauthorized third parties.

Three Levels of Implementation

While customizable privacy may sound appealing in theory, how can regulators put it into practice? Regulators should bear in mind that customer preferences range along a continuum from "don't care at all about privacy" to "care a lot about privacy." Legislation and regulation should be prepared to offer users at least three ways of engaging in the customization of Internet privacy.

> ***1) Top-level privacy customization:*** Individuals engage in a one-time selection of pre-defined privacy standards, and Internet service providers agree to adhere to these standards. The user identifies his or her privacy standards only once, at the time of signing up for Internet service. Each time the user begins a transaction on the Internet involving private data, the vendor will check to see whether or not the user has made the private data required available. If so, the transaction goes through. If not, the user is notified that the vendor requires more private data than the user wishes to disclose, and the transaction is voided.
>
> ***2) Network-level privacy customization:*** Individuals are given the flexibility to create their own "network" of Internet vendors that adhere to the their particular privacy standards. They will interact only with their "network" of vendors. Transactions involving qualified vendors automatically go through; transactions with non-qualified vendors do not automatically go through, and the user is notified.
>
> ***3) Event-level privacy customization***: Each time an individual is offered or makes a request for an Internet service or product, he or she can make a real-time decision determining whether or not he or she wishes to engage in the transaction based on the particular privacy requirements of the transaction. This is the most flexible as well as the most demanding method of implementing "customizable privacy." No transaction goes through unless the user specifically agrees to it.

The enactment of a "customizable" regulatory regime makes the most sense at the international level, led by the United States, the European Union, and Japan. A conference to develop such an international agreement could be held under the auspices of a special United Nations initiative or the World Trade Organization. The binding agreement could specify that signatories require firms operating in their country to disclose the usage of private Internet data to any user, regardless of national origin, and put in place mechanisms for the user to opt-in to a given service depending on the amount of personal data required. One significant advantage to this approach is that there is no need for any permanent bureaucracy to oversee international e-commerce in any way. Instead, users and firms would essentially negotiate the terms of usage either once (top-level customization), occasionally (network-level customization), or every time the user discloses personal information (entry-level customization). Users are in control of their data, firms are not burdened with excessive government regulations, and governments are not forced to revamp legislation every time an Internet entrepreneur finds the means to leverage personal data in a new and innovative way.

Privacy as a Differentiator

While government regulations are typically thought of as burdensome, a privacy framework such as customizable privacy would allow firms to reach a much broader market than would be possible under a more restrictive privacy regime. "Customizable privacy" allows firms to market any sort of Internet product or service using any type of private data as long as the user is aware of the data usage beforehand. This would allow users with different levels of privacy preferences to benefit from the customization of Internet products.

In addition, firms can leverage privacy as a "differentiator" rather than view it as a regulatory impediment. They can move away from viewing regulatory requirements as obstacles instead use an international customizable privacy regime to develop new and innovative product sets that heretofore would have been considered too risky because of the extensive use of personal data. With the ability to market all products to all users, companies can tout goods and services based on the use of private data as "value-added" rather than as somehow tainted or "shadowy." Thus, customizable privacy avoids having legislation set personal preference standards for users and instead allows users and firms to agree on specific value-added services in exchange for specific personal data.

Convincing businesses of the value of customizable privacy will be an

important aspect in implementing such a regulatory framework. Policy makers should look to build private sector support and coalitions with leading Internet companies to promote the virtues of customizable privacy to both businesses and citizens.

Consumers around the world rank privacy as their number one reason for not using the Internet. Realizing the full potential of electronic commerce while protecting individuals from the manipulation of private information requires unprecedented public-private cooperation. Customizable privacy has the potential to be a workable framework that both meets the needs of both consumers as well as Internet firms. It is an international regime that is blind to color, creed, nationality, income level, or age. The only necessary ingredients are a disclosure of the service, a disclosure of the personal data needed, and an agreement to disclose that data. Thus, customizable privacy crosses national, political, and cultural boundaries by allowing for all degrees of privacy preferences. Customizable privacy offers a long-run policy solution to one of the world's fastest moving regulatory challenges.

Notes

* The author wishes to thank the following colleagues for assistance in the development of this paper: Irene Alvarez, Alejandro Rodriguez Anglada, Alexandra Riboul, Philippe Sachs, and Benjamin Wampold.

[1] The four "Services" below represent Internet products and services that require different combinations of private data.

References

Accenture. 2000. *Internal Survey on International Privacy Preferences for Location Smart Services.* Document provided to author.

Association for Progressive Communications (APC). 2000. "Japanese civil society resists challenges to privacy in communications: Petition for Repeal of Wiretapping Law gets over 100,000 signatures." http://www.apc.org/english/news/archive/jca_001.htm July.

Cranor, Lorrie Faith, Joseph Reagle, and Mark S. Ackerman. 1999. *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy.* http://www.research.att.com/projects/privacystudy.

Culnan, Mary. 1999. *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission.* http://www.msb.edu/faculty/culnanm/gippshome.html (June).

Cyber Business Association. *Guidelines for Protecting Personal Information in Cyber Business.* 1997. http://www.fmmc.or.jp/fmmc2/50le.html 17 December.

Cyber Dialouge. 8 April 2000. "eCommerce Data." http://www.cyberdialogue.com/resource/data/ecom/index.html#data.

Electronic Privacy Information Center. 7 May 1998. *Testimony and Statement for the Record of Marc Rotenberg Director, Electronic Privacy Information Center Adjunct Professor, Georgetown University Law Center On The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives.* http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html.

European Commission. 2000. *Directive 95/46/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.* http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html. 27 February.

Graphics, Visualization & Usability Center. October 1998. *10th WWW User Survey.* Georgia Tech University. http://www.gvu.gatech.edu/gvu/user_surveys

Greenleaf, Graham. 1998. "Global Protection of Privacy in Cyberspace." http://austlii-edu.au/itlaw/articles/taiwanstlc.html. 16 June.

Federal Trade Commission. June 1998. *Online Privacy: A Report to Congress* http://www.ftc.gov/reports/privacy3/toc.htm.

Federal Trade Commission. July 1999. *Self-Regulation and Privacy Online: A Report to Congress.* http://www.ftc.gov/os/1999/9907/privacy99.pdf.

IBM. October 1999. *The IBM Multi-National Consumer Privacy Study: A Comprehensive and Comparative Look at Consumers in the United States, Germany, and United Kingdom and their Attitudes Towards Privacy in Everyday Business Transaction.* http://www.ibm.com/services/files/privacy_survey_oct991.pdf.

IntelliQuest Inc. 8 April 2000. "Worldwide Internet/Online Tracking Service 1st Quarter 1999 Report." http://www.intelliquest.com/press/release78.asp.

Japanese Direct Marketing Association (JADMA). 1998. *Guidelines for Personal Data Protection in the Direct Marketing Business.* http://www.jadma.org/e_page/guide_2e.html. 10 March.

Japanese Embassy, Washington. 2000. *Outline of Proposed Basic Legislation for Personal Information Protection.* Document provided to author.

"Japanese Net Tapping Law in Effect." 11 Sept. 2000. *Global Internet Liberty Campaign Newsletter* http://www.fitug.de/debate/0009/msg00200.html.

"Japan's Police Gain Right to Tap Phone, E-mail." 15 August 2000. *The Industry Standard.*

Lai, Hau Boon. 2001. "New Tokyo Law May Put End to 'Exposes.'" *The Straits Times (Singapore).* 1 June.

Louis Harris and Associates Inc. 1999. *National Consumers League: Consumers and the 21st Century.*

———. 1999. *National Consumers League: Consumers and the 21st Century.* http://www.harrisinteractive.com.

Louis Harris and Associates and Allan F. Westin. 1998. *eCommerce and Privacy: What Net Users Want.* http://www.harrisinteractive.com.

Ministry of International Trade and Industry (Japan). February 1998. *Handbook Concerning Protection of Personal Data.* http://jipdec.or.jp/security/privacy/handbook-e.html.

Parker, Pamela. 2000. "DoubleClick's Legal Troubles." http://www.internetnews.com/bus-news/articles/0,1087,3_299771,00.html. 4 February.

"New Online Privacy Survey Confirms 1997 P&AB Findings." *Privacy and American Business.* 5:1 March/April 1998

"Privacy Bill Aims to Limit Data Use." 2000. *The Nikkei Weekly.* 16 October.

Privacy International Organization. *Privacy Watch* http://www.privacyinternational.org/survey/counting-h-n.html#heading8

Swire, Peter. U.S. Chief Counsel for Privacy, Office of Management and Budget. 1999. *Testimony Before the United States Department of Commerce and the Federal Trade Commission, Public Workshop on Online Profiling.* 8 November.

United States. June 1998. *Privacy and Electronic Commerce (Draft).* http://www.doc.gov/ecommerce/privacy.htm.

United States Department of Commerce. 1998. *Discussion Draft: Elements of Effective Self-Regulation for Protection of Privacy.* http://www.doc.gov/ecommerce/staff.htm.

United States Department of Commerce. 2002. *Safe Harbor List.* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

Warren, Samuel and Louis Brandeis. 1890. "The Right of Privacy." *Harvard Law Review.*