PROGRESSIVE POLICY INSTITUTE

Policy Report
April 2001

Online Privacy and a Free Internet

Striking a Balance

by Shane Ham and Robert D. Atkinson

As the Internet becomes an ever greater part of daily life, concerns about the protection of personal privacy while online grow stronger. The nature of the concern varies widely, from worries about identity theft to a general sense of unease about Web site operators "spying" on Internet users. These fears are having an impact on the New Economy; according to a recent poll, over half of Internet users in the United States have at least occasionally altered their online behavior because of fears about their privacy.[1] For this reason, Congress is gearing up to debate online privacy legislation.

The Progressive Policy Institute (PPI) has long espoused several principles with regard to online privacy: public policy should encourage private sector leadership, allow for regulatory flexibility, distinguish between sensitive and non-sensitive data, and be technology neutral. Most important, any online privacy legislation should balance the need to protect consumer privacy with the need to encourage the growth of a free and freely available Internet supported by targeted marketing. Just as advertising supports free television, the Internet must be used as a marketing tool if the content is to remain free. The recent shakeout in the "dot com" business sector and the plummeting prices of technology stocks make this reality all the more urgent: Internet companies must become profitable to survive, and if Web sites cannot derive significant revenue from marketing to support their operations, many will have no choice but to charge subscription fees. If overly strict online privacy legislation cuts into marketing revenues, the Internet as it currently exists -- a vast repository of free and easily accessible information -- may cease to exist.

It seems clear that some kind of privacy legislation is inevitable, though it is not at all clear that legislation will pass in the 107th Congress. PPI believes that a balanced online privacy law must:

- refrain from dictating what Web sites can do with information about users;
- require Web sites to notify users of their privacy policies, with software that automatically conveys the policies constituting legal notice;
- mandate that Web sites allow users the ability to restrict the use of their personally identifiable information by "opting out";
- not set mandates for non-personally identifiable information;

- not require Web sites to serve users who choose to opt out;
- not mandate standards for protecting data or making it available to users;
- mandate strong federal preemption of state online privacy laws to prevent a patchwork of conflicting online regulations;
- set reasonable federal guidelines for penalties that can be imposed on violators; and
- give "safe harbor" to Web sites that participate in approved "seal programs" in which third parties certify the compliance of Web sites with privacy policies.

What is Online Privacy?

The Internet is an incredibly diverse medium, consisting not only of Web sites and e-mail but also instant messaging, chat rooms, bulletin boards, public databases, peer-to-peer networking (such as Napster), voice communication, video conferencing, remote game playing, and more. Moreover, many different kinds of data can be collected: personal information such as name and address; sensitive information such as credit card numbers or pharmaceutical prescriptions; "clickstream" data that record which pages a user visits and for how long; and so on. Once the data is collected, the information can be used in many different ways: to determine which kinds of banner ads a user will see; to offer online coupons or other discounts for competing products and Web sites; and even to determine the base price at which an item is offered (known as "dynamic pricing"). Though all of this takes place online, and each method of collection and use of the data raises certain privacy concerns, developing a single comprehensive privacy rule to cover every online activity would be impossible.

Many of these activities are the subjects of specialized privacy debates. For instance, privacy violations through e-mail often come in the form of unsolicited commercial e-mail ("spam"); legislation has been introduced to limit spam.[2] Public databases (such as bankruptcy records) often display Social Security numbers; legislation has been introduced to limit such displays. The bulk of the privacy debate, however, centers on data collected while a user visits a Web site. For the purposes of this paper, we will use "online privacy" to refer to Web sites only.

Why All The Fuss?

Perhaps the biggest obstacle to finding a balanced solution to the online privacy debate is determining exactly what is being balanced. Privacy advocates, such as Junkbusters and the Electronic Privacy Information Center (EPIC), argue passionately that Internet technology allows marketers to gather information on individuals to an unprecedented

degree, and they're correct. The problem is that privacy advocates can identify no harms beyond the loss of privacy itself, a sort of Orwellian angst. They hold privacy to be an intrinsic good; an inherent civil right due all Americans. Anything that violates privacy is innately bad. (Internet users also mistakenly believe that violations of online privacy can lead to identity theft, a crime that is impossible without access to Social Security numbers or other protected credit data.)

But the facts about Internet privacy could just as easily lead to the opposite conclusion: that marketers having more information about individuals is a benefit, not a harm. By gathering information about individuals, marketers are able to wring the inefficiencies out of the information costs of bringing buyers and sellers together. Just as catalog companies use more precise information to better target their catalogs to likely buyers, Web advertisers use information to better target banner ads and other marketing to likely buyers. And in an Internet economy now much more dependent on sales and real revenues than venture capital, ensuring that Web sites can make money from marketing revenues is key.

Eliminating inefficiencies and decreasing costs benefits the economy, of course, by lowering the relative costs of marketing, but it also benefits consumers. Buyers experience these benefits every day in a very tangible way. In the supermarket, for instance, if a customer purchases a bag of pretzels, a computer attached to the register will print out a coupon for pretzels, usually from a competing brand; when sellers compete for a buyer's business, the buyer always wins. Such targeted marketing can also work on the Internet. An avid golfer who visits golf sites on the Internet would not be surprised to find advertisements for golf products on those sites. When that same user visits a news site to check the headlines, he would also probably prefer to see banner ads for golf products than for, say, bowling products. Internet technology allows for such personalization, weeding out the constant bombardment of advertisements that a given individual finds uninteresting or irrelevant.

Of course, people do find an inherent value in privacy and on a daily basis strike a balance between their privacy and marketing efficiency: it is unlikely, for instance, that anyone would allow marketers to put cameras in his or her house in exchange for deep discounts on household products. Different people have different comfort levels, but everybody draws the line somewhere. The heart of the online privacy debate, therefore, is not whether a line should be drawn (it should), but rather who should have the power to draw it, the government or the individual user. Making these kinds of trade-offs is important when considering online privacy legislation.

The History of the Online Privacy Debate

In 1997, the Clinton administration released online privacy guidelines in its *Framework for Global Electronic Commerce,*[3] which were in turn based on the privacy principles developed in 1995 by the Privacy Working Group of the Information Infrastructure Task Force (IITF). In the report, the Clinton administration correctly eschewed federal regulation of online

privacy at such an early stage in the development of the Internet, instead emphasizing vigorous self-regulation and development of privacy-enhancing technology. Though sanguine about the chances of self-regulation, the report recognized that a failure by industry to adequately deal with privacy concerns in a self-regulatory regime would lead to "increasing pressure" for a more direct federal role.

The pressure began to increase a year later when the Federal Trade Commission (FTC) released its survey of online privacy practices.[4] The survey showed that only 14 percent of all Web sites that collected personal information -- and only 73 percent of the most popular Web sites that did so -- had privacy policies. The FTC argued that those numbers demonstrated the weakness of a self-regulatory regime. A similar survey conducted two years later, in May 2000,[5] showed considerable improvement in disclosure of online privacy policies: 88 percent of all Web sites and 100 percent of the most popular Web sites now had privacy policies, though not all of them gave consumers a choice in how their personal information was used. But by then the FTC was through with self-regulation. Its May 2000 report called for legislation to mandate compliance with the four fair information practice principles: notice, choice, access, and security. (Hereinafter, the "FTC privacy principles.") The FTC also asked Congress to give authority to promulgate online privacy regulations to "an implementing agency."

Since then, state legislatures and state attorneys general have stepped into the fray, seeking to create 50 different regulatory regimes for online privacy.[6] Their position is being echoed by conservative states' rights activists, who oppose federal (rather than state) control over the Internet privacy regulations for ideological reasons.[7] (Some state officials refuse to toe the federalism line, including Utah's Republican governor and former National Governors' Association chair Mike Leavitt, who said, "The mantra of the 21st century has to be local control but central coordination."[8]) The European Union (EU) also got involved, negotiating a safe harbor agreement deeming U.S. companies that abide by seven data privacy principles specified in the agreement as being in adequate compliance with the restrictive EU Data Directive.[9]

The promising Platform for Privacy Preferences Project (P3P) technology, which would allow consumers to set privacy preferences in their Web browsers and automatically compare them to Web site privacy policies, was delayed as the World Wide Web Consortium (W3C) struggled to complete the P3P specification; earlier deployment of P3P-enabled Web browsers would have done much to ease consumer fears about online privacy and altered the debate.[10] However, the P3P specification is ready to be implemented and will be incorporated into Web browsers and other privacy-enhancing software this year. (For a more detailed explanation of P3P technology, see the appendix.)

The issue of online privacy exploded into the public consciousness early last year when online advertising agency DoubleClick announced plans to merge its anonymous profiles of Internet users with personally identifiable catalog purchase information from the Abacus Direct database by linking the profiles to name and address information gathered in online transactions. A wave of bad publicity and a threat of action by the FTC forced DoubleClick to delay its plans. DoubleClick and other similar advertising

companies have since joined together to reach a settlement with the FTC that calls for self-regulation requiring the companies to give consumers notice and the right to opt out of data collection.[11] However, at this time, none of the participating companies collect personally identifiable information.

Throughout the debate, industry maintained a relatively unified position advocating self-regulation over legislation, except where sensitive information is involved, such as financial, health, or children's data. However, that unified front has begun to show cracks. While the Information Technology Association of America (ITAA) maintains the position that self-regulation should be given more time to work, AeA (formerly the American Electronics Association) is advocating legislation and the Information Technology Industry Council (ITI) advocates a nebulous middle ground, calling for a "deliberative" approach. As the debate becomes more contentious, however, it is reasonable to expect that rifts will form between companies with business models that depend completely on collection of personal data (such as network advertisers and permission-based e-mailers) and companies that use the data primarily on a transactional basis (such as click-and-mortar Web sites like WalMart.com).[12]

Two years ago, PPI released a policy report, *Online Privacy Standards: The Case for a Limited Federal Role in a Self-Regulatory Regime*, in which we advocated giving self-regulation a chance before enacting legislation that might hinder the growth of the Internet. While significant progress has been made in offering Internet users notice of Web site privacy practices and choice in how personal information is used, changes in technology, in Internet economics, and in public opinion have shifted the center of the debate from "self-regulation vs. legislation" to "what legislation would be best." For these reasons, we believe now is the appropriate time to revisit the online privacy issue and begin to consider the elements of a balanced online privacy law.

As Congress stands ready to begin debate on this issue, three primary legislative proposals have emerged: a bill by Senator Ernest "Fritz" Hollings (D-SC), a bill by Senators Conrad Burns (R-MT) and Ron Wyden (D-OR) and a bill by Senators John McCain (R-AZ) and John Kerry (D-MA). These proposals are discussed in greater detail below. Other online privacy bills are expected this year from Rep. Zoe Lofgren (D-CA) and Rep. Edward Markey (D-MA), both of which may have a significant impact on the debate.

What Does It Mean To Regulate Online Privacy?

It is a mistake made by many when discussing online privacy legislation to assume that all parties mean the same thing when they say they want to "regulate" privacy. The most general use of the term is to assume that regulation is the opposite of self-regulation and therefore any government role, no matter how restrained, constitutes regulation of online privacy. Used in this sense, enforcement actions brought by the FTC in the last few years under its "unfair and deceptive" trade practices authority against Web sites that failed to adhere to their stated privacy policies would constitute regulation.[13]

The term more commonly refers to mandating compliance with some or all of the four FTC privacy principles: notice, choice, access, and security. This definition of regulation represents a wide range of legislative solutions. Does choice mean that users must give affirmative consent to use personal data (opt in) or that consent is presumed unless the user revokes it (opt out)? Should security be mandated by law? The numerous possibilities in implementing the FTC principles means that two people can favor "regulation of online privacy" in this sense and mean very different things, but the basic parameters of the debate are set.

Privacy advocates, on the other hand, define regulation more expansively. They feel that it is not enough to simply mandate that Web sites give notice and opt-in choice; to them, regulation also means legislative restrictions on the use of personal data.[14] Though regulating information practices is a main goal of privacy advocates (and is the approach taken in Europe), we believe it to be an excessive step for several reasons. First, use limitations are unnecessary as long as consumers are notified in advance of the uses of their personal data and can choose not to share their information if they don't agree with those uses.[15] Second, regulating information practices will limit the development of Internet business models, thereby restricting the growth of the Internet and possibly reducing the amount of content available free of charge. Most important, placing legal restrictions on information practices takes away a consumer's ability to trade their personal information for discounts, free content, or anything else of value. While many privacy advocates believe that consumers are not sophisticated enough to make these choices, we believe that such an attitude smacks of paternalism and takes away from adult consumers choices they are perfectly capable of making on their own. For these reasons, with a few very limited exceptions, the major legislative proposals before Congress do not seek to regulate what companies can do with personally identifiable information (PII). Instead, they seek to give consumers control over how their information will be used. (See below for further discussion of current legislation.)

It is therefore important to be specific when discussing "regulation of online privacy" -- the definitions of the term can vary widely.

The FTC Privacy Principles: Which Should Be Mandated?

The four privacy principles put forth in the FTC reports -- notice, choice, access, and security -- form the basis for any discussion of online privacy legislation; the debate over legislation will largely focus on whether and to what extent these principles should be mandated.[16]

Notice

It is widely agreed that the most important step in protecting privacy online is to give Internet users full notice of all data that will be collected and the purposes for which that data will be used. So accepted is this principle that all three major legislative proposals

include it, and the FTC study cited above found the vast majority of Web sites that collect personal information (and all of the heavily visited sites that do so) already have privacy policies posted on their sites. Given the widespread adoption of privacy notices, it may seem almost redundant to mandate them, but the reality is somewhat more complicated.

Unfortunately, notice as it is practiced today is not very effective. Privacy policies for the major commercial Web sites tend to be lengthy documents written in dense legal language. It can be difficult for the average Internet user to decipher the practices of both the Web site and of any third parties that the Web site might share data with, such as advertisers. Moreover, to view a privacy policy users typically must interrupt their activities to click on a link that may or may not be placed in a prominent spot on the Web page. To receive notice, then, users have to stop what they're doing to hunt for a link to a wordy policy that they can't easily understand; it's not surprising that few users bother to do so.

Placing the privacy policy behind a link on the Web site's main page can also be a problem. For users to be able to make a decision based on their knowledge of a Web site's privacy policy, the notice must be given *before* the user hands over information. By the time a user follows a link to a privacy policy, however, it is entirely possible that information has already been shared, most likely by placing a browser cookie or reading a previously placed cookie.[17] If the notice is given too late for a user to prevent the transfer of information, the notice is less effective.

Technology can play a big part in solving these problems. With the release of P3P-enabled Web browsers later this year, Internet users will be able to compare their privacy preferences with a Web site's privacy policy before visiting that Web site, and the entire process will be automatic, requiring no additional effort on the user's part. "Cookie cutter" software, available as part of a Web browser or as an add-on, can give even more control over browser cookies to those users who want it. Effective and robust notice is possible, but any legislation mandating notice must consider both the challenges to effective notice and the technology available to meet those challenges.

Choice

Without the ability to choose whether to hand over personal information to a Web site, knowledge of a Web site's privacy policy is less valuable. It is not inappropriate, therefore, to think of "notice and choice" as a single issue in the online privacy debate, although choice is usually discussed separately because it is much more controversial than notice.

The choice debate usually breaks down between those who believe users should have to give permission before their personal data can be used for non-transactional purposes (opt-in) and those who believe permission should be assumed unless the user specifically revokes it (opt-out). Privacy advocates generally tend to support opt-in, a standard put forward in the Hollings proposal. On the other hand, industry, if it favors any requirement, tends to support opt-out, the approach taken in the Burns-Wyden and McCain-Kerry proposals.

Of these two choices, opt-in is the least desirable model for online privacy choice. As long as notice is provided before user information is collected, opt-in does not offer additional protections. If the user truly understands every facet of a Web site's privacy policy and decides to enter the site and allow the collection of information, then it is fair to say that consent has been given. In a sense, two negatives add up to affirmative consent: opting out of an opt-out equals opting in. (An opt-in standard would make sense if users found it difficult to learn of privacy policies and exercise choice, and therefore incurred real harms.)

An opt-in standard does, however, threaten the continued growth of the Internet. Especially now that the "dot com bubble" has burst and pressures on Internet businesses for profitability are so high, Web sites depend on revenues from targeted ads. Because they are 200 to 300 percent more likely to lead to a sale, target ads can provide a Web site with ad revenues five to 10 times higher than non-targeted ads. Users typically do not mind having their data collected -- or are willing to trade their data for discounts, services, free access to content, customized ads and offers, and so on -- but very few users are willing to interrupt their Web surfing and go out of their way to give permission. (The offer of extraordinary perks can entice some users, as permission-based e-mailers have learned, but overall the opt-in rates would likely be less than 10 percent.) **Mandating an extra step to opt-in to data collection is likely to effectively dry up the flow of data that is keeping the Internet free. For these reasons, PPI strongly opposes an opt-in standard.**

Opt-out is therefore a preferable standard, but if an opt-out requirement is going to be mandated by law, it must be clearly defined. Some additional aspects that must be defined for an opt-out requirement include:

- **Web sites should be allowed to make their opt-out system granular; that is, to offer users as many yes/no decisions as the operators like, rather than one comprehensive opt-out decision.** For example, Yahoo! allows users to build one personal profile and apply it to all of its services: e-mail, Web hosting, auctions, and so on. If a mandatory choice law passes, Yahoo! should be allowed to offer opt-out for each individual service rather than an "all or nothing" opt-out that applies to every Yahoo! service. (Of course, Yahoo could offer a one-click universal opt-out if it so chooses.)

- **Because privacy is unaffected when users remain anonymous, a distinction should be made between personally identifiable information (PII), such as names and addresses, and non-personally identifiable information (non-PII).** Privacy rules should not be applied to non-PII such as anonymous demographic data like gender and zip code or to clickstream data (which Web sites a user visits) linked only to a browser cookie.

- **If the user chooses to opt out, the Web site should not be required by law to provide the same services as it does to those who do not opt out.** The New York

Times, for example, requires users to register before giving free access to the Web site. To force the New York Times to give access even to those users who refuse to register, as Senator Robert Torricelli (D-NJ) proposed last year,[18] would be to condone free ridership by privacy-sensitive individuals. If a company wants to provide a different level of service or refuse access to the site for opt-out users, it should be free to do so.

Access

Giving consumers both access to data that is collected about them and the right to correct inaccuracies in that data has been an important advance in recent years. The Fair Credit Reporting Act (FCRA), for instance, mandates easy and inexpensive access to consumer credit reports, as well as minimum levels of service that the credit reporting agencies must give to help consumers clear up any mistakes on their report. Privacy advocates would like to extend those rights and benefits to Internet users. The principle is sound, but the analogy is not.

There are two major differences between the data in credit reports and the data that are typically collected online.[19] First, credit reports themselves contain information (such as Social Security numbers or account numbers) that can serve to verify the identity of the person requesting access to the data. The identifying data collected online, on the other hand, is usually available to the general public. To give online access to requestors based only on their name and address causes a greater privacy risk than it solves: anybody who looks up a user's name and address in the phone book can access that user's data. The more important distinction, however, is that credit report data is used as the basis for major decisions affecting consumers, such as whether to grant a loan, extend insurance coverage, or offer a job. With such high stakes for consumers, the need to know the scope and accuracy of the data in credit reports is of utmost importance. Online data, on the other hand, is used strictly for marketing purposes. If an advertiser thinks an Internet user likes tennis when in fact the user prefers racquetball, what exactly is the harm?

Access requirements, therefore, should be constructed by balancing the benefits to Internet users against the risks and costs to the companies that hold the data. Allowing access to online data can be enormously expensive: databases need to be redesigned, large customer service staffs must be hired, stringent security safeguards must be put into place. While that expense is justified for data that is covered by the FCRA, it is of much more questionable value for data collected from Internet users and used for marketing purposes only, and it makes no sense at all for non-PII. Moreover, P3P-enabled browsers will allow users to automatically reject Web sites that do not provide access to PII; in this instance it would be better to let the market address access rather than the government.[20]

Security

There is no doubt that protecting personal information from hackers and unscrupulous employees is important, but unlike the other three FTC privacy principles, security has a

"backwards" incentive structure. With the exception of sensitive health and financial account or credit data (which is already subject to data security laws[21]), the data collected online is almost always more valuable to the company that collects it than it is to the Internet users. Having invested the time and money to develop and deploy systems to gather information from Internet users, the last thing that Web site operators want is for someone to come in and steal the data from them.

In this light, it seems unnecessary to mandate data security standards for either PII or non-PII. Such standards would not increase incentives for the companies that gather the data to provide added security; most of those companies are already doing everything they think prudent to protect one of their most valuable assets. On the other hand, mandating standards or types of security technology could cut back on their flexibility to adopt new technologies, thereby stifling innovation and providing enticing targets for hackers.[22]

Policy Recommendations for Online Privacy Legislation

Constructing an effective online privacy bill that balances user privacy and continued growth of the Internet -- a bill that will satisfy reasonable privacy advocates and responsible industry members -- is no small task. (Satisfying both extremist privacy activists and industry is, we believe, impossible.) PPI believes that a sound and effective privacy bill will have the following elements:

1. Require Web sites to give notice of their privacy policies. Informed decisions about online privacy are key to consumer confidence, and the key to informed decisions is effective notice. Web sites should be required to give comprehensive, easily understood notice of their information practices -- what data will be collected and how it will be used -- before users are required to hand over any of their information. The most effective way to give notice is through machine-readable P3P policies, and we strongly support the adoption of P3P for all Web sites that collect data from users. However, because the standard is still new and relatively untested, we do not believe that P3P should be mandated for commercial Web sites at this time. On the other hand, **a Web site that posts a valid P3P-compliant privacy policy should be deemed in compliance with any mandatory notice provision.**

2. Require Web sites to give users a choice in the use of their personally identifiable data with an opt-out requirement. An opt-in standard would pose real risks to the economics of the Internet. An opt-out standard, combined with effective notice, would provide just as much protection as an opt-in standard, without the attendant risks to the economic viability of the Internet. (Of course, if Web site operators choose to have an opt-in mechanism, they will be free to do so.) An opt-out requirement should be keyed to specific collections and uses of PII rather than to the Web site itself.[23] As in the Yahoo! example above, it is sometimes appropriate for a Web site to have multiple opt-outs rather than a single universal opt-out; this is a choice that should be left to the Web site operator.

3. Do not require Web sites to deliver content, services, or other benefits to those who choose to opt-out. Many Web sites require that users give up certain information in exchange for services, discounts, or access to content. Because these sites are financially supported by targeted advertising, they have only two alternatives to collecting information from users: collect cash payments from users or shut down. If the law required Web sites to continue providing their services or content for free even if the user does not consent to trading personal information for it, it would be tantamount to mandating the provision of the service for free. Needless to say, if such a requirement were imposed, many sites would likely cease operation. Any privacy legislation, therefore, should be free of such a mandate; users who want to access such Web sites without providing information would still have the choice of offering something else of value (such as cash) or could choose not to visit the site.[24]

4. Do not mandate limitations on the use of data. Though privacy advocates feel that the only true privacy protections are laws limiting what Web sites can do with personal information, such limits would entail the same problems as mandating opt-in: risking the economic viability of the Internet and limiting the freedom of Internet users while providing little, if any, added protection. If users are given effective notice of a Web site's information practices and an opportunity to opt-out of those practices, there is no need for legal restrictions. The potential harm of such restrictions, however is great: limiting innovation in Internet business models and taking away users' ability to trade their information for free content or services.

5. Do not regulate non-personally identifiable information. In terms of personal privacy violations, there is a vast difference between collection of information that is linked to an individual user and the collection of data that will only be used on an anonymous basis. Collection of anonymous data (such as zip code or gender), almost by definition, cannot harm anyone.[25] While notice should apply to all types of data collection, any choice requirement (such as mandatory opt-out) should apply only to data that identifies an individual, such as name, address, e-mail address, phone number, and so on.

6. Do not mandate standards for access or security. Though it is important to provide consumer access to sensitive health and financial data and to keep that sensitive data secure, laws are already on the books to do so. For all of the reasons listed above, mandating access and security standards for less sensitive data collected online is an unnecessary and burdensome step that, perversely, may actually do more harm than good to the privacy of Internet users.

7. Preempt states from making their own online privacy laws. Traditionally, states have been responsible for protecting consumers, and that made sense in an era when buyers and sellers were almost always in the same state when the transaction took place. The Internet, on the other hand, is fundamentally a cross-border technology. Unfortunately, most states

are unwilling to give up their traditional consumer protection authority when it comes to the Internet. To allow states to create their own online privacy laws is to require every Web site to comply with the laws of every state. This is an unreasonable burden. More importantly, it is an unnecessary one. Federal legislation will be sufficient to protect the privacy of Internet users in every state and therefore should include strong preemption prohibiting states from making more restrictive or conflicting online privacy laws. States should, however, retain enforcement power; state attorneys general should be allowed to bring suit against Web site operators in their states that violate the federal privacy laws.

8. Place appropriate limits on penalties. The key problem with any online privacy regime, from self-regulation to the most restrictive legislation, is enforcement: holding companies to their stated (or mandated) practices. To ensure compliance, both the FTC and state attorneys general must be able to penalize Web sites that violate their posted privacy policies. On the other hand, the large number of Internet users and the large number of potentially violating transactions that occur every day present potentially ruinous liability for Web site operators. To keep the risks low, reasonable limits should be placed on civil penalties, and provisions should be made to differentiate genuine mistakes from negligence or willful misconduct.

9. Give a safe harbor to Web sites that participate in a privacy seal program approved by the FTC. Considering the potential liability faced by Web site operators, it is important to add a safe harbor to give them guaranteed compliance with the law. The FTC should be given the authority to approve of private seal programs (such as TrustE or BBBOnline), and any Web site that is a member of the approved seal program would be deemed compliant with a law regarding notice and choice. Such a provision would not only increase certainty for Web site operators, it would also cut back on the enforcement burden for the FTC and state attorneys general. Any online privacy law will have problems with enforcement, because complaints require intensive investigation into the business practices of the alleged violator. Because seal programs stand by the practices of the Web sites that display the seal, the programs themselves will play a vital role in ensuring that Web sites live up to their privacy policies. Rather than send complaints to an overburdened FTC, Internet users could file complaints with the seal program, which in turn would be required to revoke the seal (and therefore safe harbor) if a violation is confirmed.

10. Address online privacy for government Web sites separately. Services delivered on government Web sites differ from those offered by commercial Web sites in two significant respects: governments can require that you provide sensitive information (such as driver's licence numbers and Social Security numbers) and disclosures of such information is typically covered by existing laws. (States have their own laws, and federal agencies are covered by the Privacy Act of 1974.) It would be inappropriate to hold private and government Web sites to the same standard, although we believe that, both as a matter of principle and as a practical matter of encouraging digital government, privacy standards

for government Web sites should be quite strict. Online privacy for government Web sites is an important issue that should be addressed, but should be done through separate legislation.

The Main Privacy Bills

As of the publication date of this report, none of the main privacy bills had been re-introduced in the Senate (though the McCain-Kerry and Burns-Wyden bills have been introduced as House counterparts with language identical to the bills in the 106th Congress). While it is likely that all three bills will be changed at least slightly from their previous versions, we expect that the bills will be substantially similar when reintroduced this year.

Hollings

Last year, Senator Hollings, the ranking Democrat on the Commerce Committee, introduced the Consumer Privacy Protection Act (S. 2606 in the 106th Congress). Of the major online privacy bills, the Hollings bill is by far the most restrictive. The major provisions of the Hollings bill from last year would:

- mandate "clear and conspicuous" notice on type of data collected and purpose of collection;
- mandate an opt-in standard for PII and an opt-out standard for non-PII (anonymous information that will later be linked to personally identifiable information is treated as PII);
- require "reasonable" access and ability to change PII;
- require "reasonable" security and authorize funding for training network security specialists;
- require FTC rulemaking and the establishment of an FTC Office of Online Privacy;
- provide limited preemption of state laws (torts, common law, and fraud laws are excepted from the preemption provision);
- specify a private right of action;
- create limited use restrictions (extend video rental information protections to books and music; extend cable subscriber information protections to satellite subscribers; specify that PII cannot be considered an asset in bankruptcy); and
- require FTC and FCC to study and make recommendations on harmonizing online and offline privacy regulations.

We believe that the Hollings bill goes too far, restricting consumer choice and imposing unreasonable burdens on Web site operators. Although the use restrictions are fairly limited (making the bill less strict than privacy advocates would want), the opt-in standard

for PII, the existence of any standard for non-PII, and the mandatory access and security requirements are unnecessary and will harm the growth of the Internet in the long run. In addition, the bill's weak state preemption provision fails to solve the potential problem of multiple conflicting privacy laws.[26]

Burns-Wyden/Frelinghuysen

Senators Burns and Wyden introduced their online privacy bill in the 106th Congress. Though they have yet to introduce their bill this year, the House companion (H.R. 89, introduced by Rep. Rodney Frelinghuysen (R-NJ)) is identical to last year's bill. It would:

- require "clear and conspicuous" notice for PII (type and purpose);
- require a "meaningful and simple online" process for choice, which can be opt-out or opt-in;
- allow Web site operators to terminate service to users that opt-out;
- mandate limited access to PII that is sold or transferred to third parties (the exceptions to the access requirement are significant, including exempting data that has "no impact" on the individual);
- require "reasonable procedures" for security of PII;
- give FTC authority to approve industry-developed self-regulatory safe harbors (and require that the FTC act on requests for safe harbor approval within 180 days);
- preempt state law but allow for enforcement of federal regulations by state attorneys general;
- not specify private rights of action; and
- require an FTC review five years after implementation.

The Burns-Wyden / Frelinghuysen bill is far less onerous than the Hollings bill, but still goes further than necessary in the limited provisions for access and security. Though these provisions may be considered a compromise between the strong provisions pushed for by privacy advocates and nothing at all, in reality the access and security requirements create regulatory burdens for Web site operators without significantly increasing user privacy or even consumer confidence. Though compromise is admirable (and ultimately necessary) in this complex issue, the costs of the Burns-Wyden compromise do not match the limited benefits.

McCain-Kerry/Eshoo-Cannon

The online privacy bill championed by Senators McCain and Kerry is widely expected to be a starting point for the coming debate due to Senator McCain's chairmanship of the Senate Commerce Committee. The McCain-Kerry bill has not been introduced this year,

a House companion (H.R. 237) by California Democrat Anna Eshoo and Utah Republican Chris Cannon has been introduced. It would:

- require "clear, conspicuous, and easily understood" notice for PII (sets forth eight elements that must be included in the notice);
- mandate an "easy to use, easily accessible and available online" opt-out procedure for PII which must be specified in the privacy notice;
- provide safe harbor for participants in FTC-approved seal programs;
- set civil penalties at $22,000 per violation per day with a limit of $500,000 for a series of related violations;
- preempt state law but allow for enforcement of federal regulations by state attorneys general; and
- require the National Academy of Sciences to conduct a study of online privacy and make recommendations to Congress.

We believe that the McCain-Kerry proposal is the best of the major online privacy bills. The specific notice mandates, flexible opt-out mandate, and strong state preemption get to the heart of the online privacy issue and achieve a balance between the needs of users and the economic realities of the Internet. It is also important that the bill assigns responsibility for further study of the issue to the National Academy of Sciences rather than to the FTC (as the Hollings and Burns-Wyden bills do); this avoids a potential conflict of interest that could arise from the FTC's role in promulgating online privacy regulations.

Conclusion

While it is still too early to determine whether self-regulation of online privacy has failed, it is certain that ill-conceived legislation could do more harm to the Internet than even the worst self-regulatory regime. To prevent that harm, online privacy legislation must balance a user's personal privacy against the costs of complying with an online privacy law; those costs must be justified by a legitimate increase in user confidence. Most importantly, a user's right to trade personal information for access to Internet content and services must not be taken away or the free Internet may cease to exist. If an online privacy law is to pass in this Congress, we believe it should be the McCain-Kerry bill, for that measure comes closest to meeting these goals.

Shane Ham is technology policy analyst for the Progressive Policy Institute. Robert D. Atkinson is vice president of the Progressive Policy Institute and director of the Technology and the New Economy Project at the PPI.

For further information about PPI publications, please call the publications department at 800-546-0027, write the Progressive Policy Institute, 600 Pennsylvania Ave., S.E., Suite 400, Washington, DC, 20003, or visit PPI's Web site at: http://www.ppionline.org.

Appendix: What is P3P?

The Platform for Privacy Preferences Project, commonly known as P3P, is a technical specification that allows Web browsers (or other software) to automatically determine the privacy policy of a Web site and either warn the user or block the site entirely if the policy does not fit with the user's preset privacy preferences. Now that the specification is set for widespread use, software companies will develop two categories of P3P software:

1. User software -- which can be integrated with a Web browser -- will allow users to set their own privacy preferences or use preset preferences that were established by a third party that they trust (such as BBBOnline or users' Web-savvy children). Microsoft is slated to launch a P3P-compliant version of its Internet Explorer browser this year.

2. Policy generators are used by Web site operators to transform their human-readable privacy policies into machine-readable policies (in XML format), usually by answering a lengthy electronic survey. IBM has developed a beta version of a policy generator.

In practice, P3P technology will act like a warning signal built into a Web browser. When a user visits a Web site, the browser automatically and almost instantaneously will check the site's privacy policy, compare it to the user's preferences, and display a warning if the policy is unacceptable. Early implementations will probably focus on blocking cookies that have unacceptable privacy policies. Future generation browsers should be able to evaluate a web site's full privacy policy.

It's important to note that although private companies will develop implementation software, P3P itself is not a company or even a specific technology. P3P is a specification developed by the World Wide Web Consortium (W3C), an international group that agrees on interoperability standards for Web technology. P3P should be thought of as a standard, like HTML (which was also developed by W3C).

What does P3P do?

P3P is primarily a tool for **notice and choice**, though choice here means the choice to turn away from Web sites with insufficient privacy standards rather than "opting out." (Opt-out is still available, of course, but it is not handled automatically in this early version of the specification and may never be.) The specification requires the companies to declare whether they collect a lengthy list of personal data elements (such as address and date of birth) and what happens to the data if they do. Machine-readable policies are more effective than the legalistic privacy policies found at most sites because:

- the browser is guaranteed to read and understand the P3P policy, whereas most users never bother to read the plain language policies;

- the privacy policy is delivered to the user and a choice is made *before* any user data is transmitted to the site;

- P3P can make separate decisions on the policies of individual elements within a single Web page (i.e., you can accept the cookie that Travelocity wants to place on your browser and reject the cookie that the DoubleClick banner ad wants to set);

- it all happens automatically and behind the scenes, so it doesn't interfere with the user experience.

The specification also requires P3P-compliant privacy policies to disclose what kind of **access** is given to the collected data, **dispute resolution** procedures, the **parties** receiving the data, and the circumstances and time limit for **data retention**. If these policies do not match the user's preferences, the site is automatically blocked.

What does P3P not do?

The basic philosophy of P3P technology is that the user has the power to make privacy decisions, but it does not set any minimum standards or dictate what privacy practices must be followed with respect to opt-out / opt-in, user access to data, data quality, or data security. There are a number of enhancements that will be made in future versions (such as the ability to automatically negotiate a privacy policy with a Web site), but these issues are inherently outside the scope of P3P. P3P also has no built-in mechanism for enforcement; Web sites can still say one thing in their P3P policy while doing another. But "automatic" enforcement of privacy practices is impossible; enforcement requires an audit of a Web operator's data practices and therefore is an issue even under the strictest regulatory regimes. P3P policies would be binding, however; if a Web operator does not handle user data as detailed in the P3P policy, the operator would be subject to enforcement action by the FTC for unfair and deceptive trade practices.

Opposition to P3P

Some privacy advocates, such as EPIC and Junkbusters, oppose the deployment of P3P technology. Until now their objections have not received much attention outside of the P3P development community, largely because they believed the specification would never be completed. However, when Microsoft releases its Internet Explorer version with built-in P3P later in 2001, their objections will become part of the larger privacy debate. Among their most vocal objections are:

- **P3P does not mandate fair information practices**. This is true, as far as it goes. P3P does not require government regulation of data practices as the Europeans have done, though it is not inherently incompatible with such regulations. If properly

implemented and widely adopted, P3P may make the regulation of data practices unnecessary by empowering consumers to make their own choices and creating collective market pressures that will drive the practices of companies.

- **P3P is merely a delaying tactic by industry to appease the public and stave off regulators.** This is an unfounded assumption, but there is a very real chance that the implementation of the P3P specification will be so weak and ineffective that this statement will seem true in retrospect. This is why strong leadership is needed to get companies to use P3P policies, to encourage the independent development of preference templates by seal programs and consumer advocacy groups, and to educate consumers on the effective use of the technology. After a time, if P3P looks like a failure, stricter notice mandates may be in order, but it is important to give P3P a chance.

- **The software companies will set the preference defaults so low that the technology is useless.** This is a serious concern; not only do we have to worry about whether the P3P filters will be set at a low or high level, but also about what "low" privacy and "high" privacy mean. The key will be for developers to make their user-side software as powerful and customizable as possible and to persuade users to make an informed choice about their preferences rather than accept the defaults. (Ideally, a P3P browser would require the user to make a privacy choice upon installation, before it could be used to surf the Internet.)

Endnotes

1. A *Wall Street Journal* and Harris Interactive poll of 2,365 adult Internet users, taken March 14-16, 2001. In response to the question, "How often, if ever, have concerns about privacy caused you to stop using a Web site or forgo an online purchase?" 5 percent responded "all the time," 9 percent responded "frequently" and 39 percent responded "occasionally." (Twenty-eight percent responded "rarely" and 19 percent responded "never.")

2. Legislation to limit spam has been championed by Rep. Heather Wilson (R-NM). The provisions of Wilson's bill (H.R. 718) track closely with the recommendations in PPI's paper *How To Can Spam* (it can be found at www.ppionline.org).

3. The Clinton Web site is currently archived on the National Archives and Records Administration Web site (http://www.nara.gov). It can be read at http://clinton4.nara.gov/WH/New/Commerce.

4. The June 1998 Federal Trade Commission report, "Privacy Online:: A Report to Congress," can be found at http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

5. The follow-up FTC report "Privacy Online: Fair Information Practices in the Electronic Marketplace," can be found at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.

6. In his February 2000 testimony before the Senate Commerce Committee, Vermont Attorney General William H. Sorrell stated, "[A]ny federal law enforcement approach to protecting consumers who travel the World Wide Web must include the states. We ask you to take such steps to ensure that the states can play a full and constructive role in the effort to police the Internet."

7. The American Enterprise Institute's Federalism Project sponsored a paper by George Mason University law professors Bruce Kobayashi and Larry Ribstein arguing that a federal solution to online privacy would "straightjacket [sic] emerging technologies and business practices" and advocated "[a] process of state experimentation." The paper can be found at http://www.federalismproject.org/conlaw/ecommerce/cookies.pdf.

8. "States seek uniform way to tax Internet purchases," *The Washington Times*, February 1, 2001, B8.

9. For a detailed explanation of the EU Directive, see the PPI paper *Online Privacy Standards: The Case for a Limited Federal Role in a Self-Regulatory Regime* (http://www.ppionline.org) . For more on the safe harbor agreement, see http://www.ita.doc.gov/td/ecom/menu.html.

10. Complete information about the history of P3P can be found at the official Web site (http://www.w3c.org/p3p).

11. The Network Advertising Initiative (NAI) represents DoubleClick and other advertising companies to ensure compliance with the settlement. As part of the settlement, NAI launched an easy-to-use web site that allows users to opt-out of all of the participating companies from a single form (http://www.networkadvertising.org). A third party enforcement site for independent investigation of complaints will be launched in the near future.

12. Further evidence of a potential industry rift is the recent trend of Internet Service Providers (ISPs) launching advertising campaigns that tout their ability to protect users from privacy-violating Web sites.

13. For details of such enforcement actions to date, see http://www.ftc.gov/privacy/index.html (News Releases section).

14. Privacy advocacy groups formed the Privacy Coalition in February 2000 to set forth their principles for online privacy legislation. The principles and a list of Coalition members can be found at http://www.epic.org/privacycoalition/coalition_press_release.html.

15. There are ample resources, such as anonymizers and free pseudonymous e-mail accounts, to protect those who are especially concerned about their privacy.

16. Privacy advocates propose additional privacy principles: correction, use limitations, and redress if information is used improperly. We consider the right to correct inaccurate information as "access" the reasons for excluding use limitations and redress are discussed in the Policy Recommendations section.

17. Cookies are text files placed on a user's hard drive by a Web site that can only be viewed by that site. Persistent cookies (those that remain on the hard drive after the user has left the site) can be very useful; for instance, they are used to store information such as address and frequent flyer number so the user does not have to retype them for every transaction. But some cookies, particularly those placed by banner advertising companies, can be used to track a user's online behavior and build a profile as the user visits sites that are seemingly unrelated but use the same advertising company.

18. Senator Torricelli's legislation in the 106th Congress (S. 2063) stated that Web site operators "may not terminate the provision of such service or access to or use of such Internet Web site to an individual who refuses to consent to the disclosure of records or other information . . . as a result of such refusal."

19. Data that fall into both categories is already covered by the FCRA's access provisions.

20. For an excellent description of the problems related to access, see the report of the FTC Advisory Committee on Online Access and Security at http://www.ftc.gov/acoas/papers/finalreport.htm.

21. Security for health-related data is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPPA), P.L. 104-191. Security for financial data is covered under the Gramm-Leach-Bliley Act (GLBA), P.L. 106-102.

22. The FTC Advisory Committee also stressed the need for flexibility to account for changes over time in a Web site's security risks and needs. See the report *op cit*.

23. Under any kind of opt-out standard, users would not be able to opt-out of providing information necessary to complete the transaction, such as a mailing address to which purchases can be delivered.

24. For most savvy Internet users that are concerned about sharing their personal information, this is a non-issue. Web browser software allows users to log on to the Internet under assumed names with fake personal profiles, and many services allow users to obtain e-mail addresses under assumed names. By using these tools, a user can visit sites that require personal information in exchange for access (such as the New York Times site) without ever revealing their true identity.

25. Some privacy advocates would argue that anonymous information linked to a specific browser number -- even if not linked to the user's name, address, e-mail address, or any other identifiable information -- is intrinsically harmful. As long as no effort is made to link anonymous data to an individual (or if such an effort is made, the individual has clear notice and choice), the intrinsic harm of anonymous data collection is a value judgement. PPI believes that no such harm exists and therefore that use limitations are not

justified. For those who believe otherwise, privacy-enhancing technologies are a better solution than legislation.

26. The preemption provision states that "if a State law provides for a private right-of-action under a statute enacted to provide consumer protection, nothing in this Act precludes a person from bringing such an action under that statute, *even if the statute is otherwise preempted in whole or in part*" by the federal privacy law (emphasis added). This loophole allows states effective control over online privacy by subjecting Web site operators to massive monetary judgements for violating laws that are supposedly preempted.