A Proposal for a Ubiquitous Privacy Notice Standard

Roland Burton & Corinna Sherman
May 16, 2002

Table of Contents

Introduction

The growing popularity of the Internet, the proliferation of e-commerce web sites, and the emergence of marketing companies like DoubleClick have raised public awareness of the extent to which online businesses collect, use, and share customers' personally identifiable information (PII). Consumer profiling and the problems which arise from it, including sale of consumer data, fraud, and identity theft, have triggered a spate of discussion to determine what, if any, legislation is needed to protect consumer privacy online. Lawmakers' latest answer to this challenge is the Online Personal Privacy Act, S. 2201, a 42-page bill sponsored by Senator Ernest Hollings (D-SC), that seeks to apply different standards of protection for sensitive and non-sensitive personal online information.

Though well-intentioned, this and other narrowly tailored approaches to privacy legislation are not the most effective way to stop privacy invasions or handle consumers' concerns and often impose enormous legal and financial burdens on affected businesses. Rather than legislation specifically directed at protecting online privacy, the American public is better served by both online and offline implementations of a ubiquitous "Privacy Notice" template, backed by federal legislation and similar in spirit to the Nutrition Facts panels found on food product packages, that outlines clearly and concisely what information is being collected from them by a company and how it is used. Such a measure would require companies to explicitly state and adhere to their information practices, enable consumers to make educated choices about which businesses they patronize, and create greater market incentive for industry to develop strong privacy policies that cater to consumers.

Arguments for Federal Privacy Legislation

The motivations behind efforts to federally legislate privacy online are compelling. While technology has greatly enhanced companies' abilities to collect, analyze, and share huge amounts of personal data, consumers have been left to fend for themselves in an untamed online frontier with little knowledge or means to protect their personal information. Although the most popular Web sites represent companies with model privacy policies and equally commendable adherence to those policies, including Amazon, Hewlett Packard, and Microsoft, there are still "bad guys" who continue to make headlines for egregious disregard for consumer privacy and go unpunished. Some companies post policies, collect information from consumers, and then change their policies. Some start out with assurances of protection only to later declare bankruptcy and seek to sell their customers' data to the highest bidder. Eli Lilly made news last year after disclosing a list of hundreds of customers suffering from depression, bulimia, and obsessive compulsive disorder over the Internet and following up with nothing more than an apology and a promise that it would not happen again – not much comfort to the individuals whose medical records had been divulged. Just last March, Yahoo provoked customer outrage when it changed its customers' account preferences to indicate that they wanted to receive solicitations through spam, snail mail, and telephone and added users' home addresses and phone numbers to their "Yahoo ID" profiles without their permission. Privacy advocates have called these incidents failures of the market and hold

them up as reasons for government to step in and establish baseline privacy standards through legislation. As Senator Hollings stated during a Commerce Committee hearing on S. 2201 last April, "Businesses keep confounding consumers with unclear privacy policies that state, 'your privacy is important to us,' but subsequently outline exceptions crafted to allow almost any use of personal information. Other Web sites don't post privacy policies, safe in the knowledge that they face no legal jeopardy under current law for selling your information."[1]

Confused consumers face the difficult decision to either hand over their personal information to untrusted parties for the convenience of online services or refrain from participating in e-commerce altogether. According to recent surveys and polls, this has translated into decreased consumer participation in online commerce and lost sales. In 2000, a Pew Internet and American Life Project poll revealed that 84% of Internet users are concerned about businesses and strangers obtaining information about themselves or their families.[2] Such concerns came at a price of an estimated $12.4 billion in lost sales to U.S. companies in 2000 alone.[3]

An Ernst and Young report, *Privacy Promises Are Not Enough*, noted that "at the core of this trust issue is the fact that consumers do not trust businesses to protect their privacy or follow their stated privacy policies."[4] In response, individuals are turning to online deception tactics to defend themselves. About a quarter of American Internet users have provided a fake name or personal information in order to avoid giving a Web site real information about themselves, and a fifth have used a secondary email address to avoid giving a Web site real information.[5] On the other hand, few people are either willing or knowledgeable enough to jump through complicated technological hoops for the sake of protecting their privacy. Only one in ten Internet users have sent an encrypted email and only one in twenty have used software that hides their computer identity from Web sites.[6] In addition, Internet newcomers are less likely to employ self-defense tactics than are young people and experienced online users. Just 18% of users online for six months or less have provided fake personal information, compared to 31% of those with three or more years of online experience.[7] These statistics emphasize the need for a

---

[1] "Statement by Senator Ernest F. Hollings, Hearing on S. 2201, the Online Personal Privacy Act."
[2] The Pew Internet and American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* (Aug. 20, 2000), p. 4. Available online at http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf.
[3] Testimony of Frank Torress, Legislative Counsel for Consumers Union, before the Senate Committee on Commerce, Science, and Transportation, S. 2201, Online Personal Privacy Act, April 25, 2002, p.3. Available online at http://commerce.senate.gov/hearings/042502torres.pdf.pdf.
[4] Testimony of Frank Torress, Legislative Counsel for Consumers Union, before the Senate Committee on Commerce, Science, and Transportation, S. 2201, Online Personal Privacy Act, April 25, 2002, p.3. Available online at http://commerce.senate.gov/hearings/042502torres.pdf.pdf.
[5] The Pew Internet and American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* (Aug. 20, 2000), p.10 . Available online at http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf.
[6] The Pew Internet and American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* (Aug. 20, 2000), p.10 . Available online at http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf.
[7] The Pew Internet and American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* (Aug. 20, 2000), p.10 . Available online at http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf.

solution to privacy concerns that the average consumer, regardless of their amount of online experience, finds accessible and straightforward.

The Online Personal Privacy Act of 2002, S. 2201

S. 2201 attempts to protect consumer privacy through five core principles of privacy protection laid out by the Federal Trade Commission (FTC) in its 1995 report to Congress on online privacy: notice, consent, access, security, and enforcement. It takes a two-tiered approach to privacy protection, allowing companies to collect nonsensitive PII with an opt-out policy but applying more stringent opt-in consent rules for sensitive PII (SPII). PII, as defined by S. 2201, includes first and last names; home or other physical address; e-mail address; telephone number; birth certificate number; any other identifier for which the FTC finds there is a substantial likelihood that the identifier would permit the physical or online contacting of an individual; or information that an Internet service provider, online service provider, or operator of a commercial website collects and combines with one of the identifiers described above. SPII includes specific financial data, health data, ethnicity, religious affiliation, sexual orientation, political affiliation, and social security number.

Title I of the bill requires Internet service providers, online service providers, and commercial web site operators (collectively referred to as "Internet companies") to

- post clear and conspicuous notice of their information practices, including what information will be collected and how it may be collected, used, and/or disclosed to others.
- obtain affirmative consent from consumers ("opt-in") before collecting and using or disclosing SPII.
- provide "robust notice" for individuals to opt-out prior to PII collection.
- maintain permanence of consent: a user's consent or denial of consent must follow his information until he changes his preferences, regardless of whether the collecting company changes ownership or declares bankruptcy.
- provide notice of a material change in privacy policy and refrain from collecting, sharing, or using PII unless a user has had an opportunity to consent or withhold consent.
- provide notice of a privacy breach relating to PII, such as a hacker breaking into a consumer database.
- provide reasonable access to a user to PII that the company has collected from the user online for a reasonable fee not to exceed $3.
- establish and maintain reasonable procedures to protect the security, confidentiality, and integrity of PII they maintain.

The first four bullet points do not apply to collection, disclosure, or use of PII for the purposes of protecting the security and integrity of the service or Web site; conducting a transaction, delivering a product or service, completing an arrangement for which the user provided the information; or providing other products or services integrally related to the transaction, service, product, or arrangement for which the user provided the information. A company is also not to be held liable for disclosing PII in response to a request made under the Children's Online Privacy Protection Act (COPPA);

a request for access to, or correction or deletion of, a user's PII by that user; or a request by a law enforcement, investigatory, national security, or regulatory agency or department of the U.S., backed by a warrant, court order, or equivalent administrative compulsory process.

Title II of the bill outlines rules for enforcement of the requirements listed in Title I. It specifies that the legislation is to be enforced by the Federal Trade Commission. It grants consumers rights of redress by allowing the FTC to award up to $200 of collected civil penalties to each injured party; and allowing private actions by users in cases involving SPII, with a minimum of $5000 in damages to be awarded by a federal district court upon showing of actual harm. The bill also allows class action suits to be brought by state attorneys general.

S. 2201 addresses many of the privacy concerns that have been voiced over the past several years, but its effectiveness is questionable at best. The bill attempts to solve the emerging problem of inconsistent state regulation of privacy that has been worrying online businesses by establishing a uniform federal standard and preempting state Internet laws. E-commerce representatives, however, have voiced serious concerns that "the passage of the bill would mean expensive overhauls of e-commerce systems and databases, and create security nightmares by letting customers into the system to check, and change, their personal information."[8] Paul Misener of Amazon.com warned,

> It has provoked grave concern, particularly in our engineering department. These can-do engineers and programmers, who have built up our computer system all the way from our CEO's garage to the Fortune 500 in just seven years, seriously question whether we possibly could comply with the technical requirements of this bill.[9]

Industry representatives have also voiced worries that S. 2201 may hamper businesses' efforts to stop fraud and identity theft if customers opt-out of providing information that is used to verify accounts and credit. Besides posing a substantial and expensive engineering challenge, S. 2201 also threatens to make privacy policies even less comprehensible to consumers by allowing private and class action lawsuits to be brought against companies in violation of the Act. In an effort to better protect themselves in a lawsuit, companies will pack their privacy policies with legalistic fine print, rendering them much less readable to the average layman. An alternative suggested by Misener is to make a regulatory body such as the FTC responsible for balancing the "competing interests of legal precision and simplicity."

As a final cautionary note on S. 2201, it must be pointed out that the bill conflicts with existing privacy law, the Gramm-Leach-Bliley Act of 1999, which regulates information practices for financial institutions. Specifically, pieces of information that are treated as "opt-out" by the GLB are designated as "opt-in" by S. 2201. Imposing conflicting privacy standards for companies that collect data both online and offline will needlessly complicate business operations. Privacy protection designed by industry, in

---

[8] Gaudin, Sharon, "Online Privacy Bill Raising 'Grave' E-Commerce Concerns," E-Commerce News, April 26, 2002. Available online at http://www.internetnews.com/ec-news/article/0,,4_1016831,00.html.
[9] Gaudin, Sharon, "Online Privacy Bill Raising 'Grave' E-Commerce Concerns," E-Commerce News, April 26, 2002. Available online at http://www.internetnews.com/ec-news/article/0,,4_1016831,00.html.

contrast, has the advantage of being tailor-made to the circumstances of a particular industry sector, "applying sector-specific protections that suit the particular regulatory environment in which the industry must operate."[10] Not only does industry self-regulation avoid creating conflicting privacy standards, it also allows a company to craft its own policy with special consumer needs in mind. A health company's privacy policy, for example, has very different motivations and rules governing it than that of a baseball card trading web site. Not restricting the specific content of a privacy policy gives businesses the valuable flexibility they need to serve their customers best.

The Online/Offline Disparity

The point to make about privacy is that concerns over it are the same both online and offline. Consumers want control over who has access to their personal information; whether a company selling their sensitive information has a web site or not makes no difference. As Paul Misener of Amazon.com observed in his testimony before the Senate Commerce Committee, 99% of consumer transactions occur offline, and information collection practices are even more widespread in regular brick-and-mortar institutions than they are on the Internet.[11] The Wall Street Journal reports that Time Warner, for example, has the names, addresses, and information on the reading and listening habits of 65 million households. USA Today says Time Warner has access to information about its 13 million cable subscribers and from its other businesses, like Time and People magazines.[12] Misener points out, "The huge, searchable, and transferable computer databases kept by offline companies are just as much at risk as the information collections of online entities."[13] Why, then, is the push for regulation being limited to the online world? Most of the information being collected online and offline is the same anyway, and it makes little sense to legislate one and not the other, especially when the offline form of collection is so much more prevalent. Such a move is unfair and misleading to consumers. Some might argue that an important distinction between the online and offline worlds is that the Internet allows for the collection of "click-stream" data, by which a web site operator can track and analyze what an individual views on a website. Even if such a phenomenon warrants regulation, however, it should be in the form of legislation specifically tailored to address that form of data collection, not blanket legislation that discriminates against online businesses in general. Former chairman of the Senate Committee on Commerce, Science, and Technology Robert Pitofsky testified on May 25, 2000,

---

[10] *Privacy and Online Politics: Is Online Profiling Doing More Harm Than Good for Citizens in our Political System?*, The Center for Democracy & Technology.

[11] Statement of Paul Misener, Vice President, Global Public Policy, Amazon.com, Testimony Before the Senate Committee on Commerce, Science, and Transportation, Hearing on S. 2201, The Online Personal Privacy Act, April 25, 2002, p. 16. Available online at http://commerce.senate.gov/hearings/042502misener.pdf.pdf.

[12] Testimony of Frank Torress, Legislative Counsel for Consumers Union, before the Senate Committee on Commerce, Science, and Transportation, S. 2201, Online Personal Privacy Act, April 25, 2002, p.7.

[13] Statement of Paul Misener, Vice President, Global Public Policy, Amazon.com, Testimony Before the Senate Committee on Commerce, Science, and Transportation, Hearing on S. 2201, The Online Personal Privacy Act, April 25, 2002, p. 17. Available online at http://commerce.senate.gov/hearings/042502misener.pdf.pdf.

> [I] have increasingly come to the view that the theory of distinguishing online from offline is really rather weak. I was recently influenced by one of our advisory panel people who said, "What is the point of treating warranty information from when a consumer files a warranty card, that is just going to be read into an electronic format by some clerk—Why would you treat that information differently from another?" I found that a very powerful argument. I am also influenced by the fact that we hear through mergers, joint ventures, and otherwise, that online and offline companies are merging their databases. And that's another reason we should think about both.[14]

One example to which Pitofsky may have been referring is DoubleClick's 1999 announcement, after having purchased the consumer transaction database Abacus, that it intended to attach surfing habits and online searches to personal identity. This move generated great public disapproval and was abandoned in February 2000, but it illustrates quite well the increasingly blurry line separating online and offline data collection. When giving his views about S. 2201, Senator Thomas B. Leary of the FTC claimed that it was "…illogical to regulate one medium and not the other."[15] We agree.

For the reasons expressed above, we believe that S. 2201 is not the best way of tackling consumer privacy concerns. After examining all the ways in which regulation may be achieved, we will propose a partially technological, partially legislative solution that provides clear and concise notice to consumers about their privacy risks, both online and offline, while remaining open and flexible for businesses.

Our Proposed Solution

Lawrence Lessig spoke of four modalities of regulation in real space and cyberspace: law, social norms, markets, and architecture.[16] So far, all of the current efforts at improving American consumers' privacy rights have been aimed at looking for a solution entirely in the law. The most recent of these is Senator Hollings' Online Privacy Protection Act, S. 2201, as discussed in a previous section. No recent bills on online privacy have come close to passing, though, through a combination of low priority within Congress and strong objections from within industry. There have been no attempts to introduce such sweeping legislation offline as is being suggested for the online world. The only exceptions to this are in the financial sector with the GLB and in the medical sector with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is interesting to note that before the existence of large corporate databases, the largest information stores were held by the government and various federal agencies. In the 1970s, it was felt that legislation was needed to protect American citizens from the misuse of these data banks. In 1974, the Privacy Act was passed, which greatly restricted the flow of data to and from these government databases. This Act helped to ensure that federal databases would be used solely for their original purposes, such as law

---

[14] Statement of Paul Misener, Vice President, Global Public Policy, Amazon.com, Testimony Before the Senate Committee on Commerce, Science, and Transportation, Hearing on S. 2201, The Online Personal Privacy Act, April 25, 2002, p. 11. Available online at http://commerce.senate.gov/hearings/042502misener.pdf.pdf.

[15] Senator Thomas B. Leary, Letter to Senator John McCain RE: S. 2201, April 24, 2002. Available online at http://www.ftc.gov/os/2002/04/sb2201leary.htm.

[16] Lessig, Lawrence, "Commentaries, The Law of the Horse: What Cyberlaw Might Teach," *Harvard Law Review*, Vol.113:501, 1999, pp. 506-507.

enforcement and taxation. Databases as large as these, however, now exist in the private sector, with few limits on the kinds of data exchanges allowed.

Architecture at the moment is predominantly making the privacy situation worse. The nature of the Internet, while allowing for anonymity at one level, also allows for data to be harvested quickly, easily and in huge quantities. The use of vast information databases is not just an online occurrence, either. The technology that powers the product databases on Amazon.com can also store data that may have originally been collected offline. A prime example of this is the supermarket reward card. Purchase information collected from the computerized cash registers can be quickly transferred into national company databases without the consumer's awareness. Attempts have been made in the online world to use architecture to improve privacy, an example of which is the Platform for Privacy Preferences Project (P3P). P3P is yet to be widely adopted, though the latest version of Microsoft's Internet Explorer 6 includes one implementation. The version in Explorer 6 is limited to allowing the user to customize how his browser deals with cookies, but the use of cookies on the Internet is only a small part of the privacy problems facing online users. P3P has been adopted by an increasing number of websites, although the adoption is predominantly among the "good guys" sector of the online world. Many sites with poor privacy policies do not use P3P. As implemented in Explorer 6, P3P does not protect against misuse of customer-volunteered data, such as a typed-in email address. In the offline world, architectural solutions have included the mass-mailing of over a billion incomprehensible privacy policies to consumers, which has generally been regarded as an extraordinarily expensive failure.

Whether or not the market is effectively protecting privacy depends on who you talk to. Many of the large banks and online retailers claim that the market is already creating the right balance between data sharing and privacy protection, though these companies obviously have a vested interest in avoiding the level of costs that bills such as S. 2201 would incur. According to Senator Hollings, EPIC, and the Consumers Union, the market is losing the privacy battle. Still, only 1% of all transactions are carried out online. Surveys have shown that concerns about privacy rank as the number one reason why people who have Internet access do not shop online. The balance in the market at the moment appears to be between those who are willing to "risk" online shopping and those who are not, rather than consumers deciding which of the online companies offer good privacy policies and which do not.

Tackling privacy through the norms poses similar problems to trying to tackle the problem using the market. Unfortunately there is a lack of knowledge on the consumer end about both what data companies collect in the first place and, once collected, what they can do with the data. The trend at the moment is that most consumers who feel that online commerce invades their privacy avoid it altogether, even though there may be online companies who offer better privacy protection than some of the offline companies that the consumers already use. The norms at the moment are creating a divide between those consumers who are happy to shop online and those who are not. This lack of information needs to be addressed in any new privacy legislation.

In order to improve privacy protection in America, this paper proposes a new standard, to be backed by federal legislation, that tackles the privacy issues by using a

combination of law and architecture. The hope is that the new standard will make consumers significantly better informed of their choices, and so help to establish the market and the norms as privacy regulators as well. The architecture is to be changed by creating a universal format that all privacy notices must obey. This makes the reading, understanding and comparison of privacy policies easy. The law is to be used by making it a requirement that all companies who collect data must post this universal privacy notice, and to require that all information in the notice is accurate. The idea behind the standard is that rather than restricting how a company can collect and use data, it requires the company to clearly and concisely tell its customers: what data it collects; how that data is collected and what is done with the data once collected. This new standard is called the PNS – Privacy Notice Standard.

Basic Aims of the PNS

The PNS has to be able to convey the most important parts of a company's privacy policy, and do so in a concise way that is simple for people to understand. The PNS is designed to get away from situations where:

> Companies post privacy policies that require the help of both an English major and a commercial lawyer to understand, and even then the policies are misleading and contradictory.[17]

The PNS must also convey the information in a way that neither trivializes the policy nor misses crucial points. A company should also not feel that it its policies are misrepresented by the PNS in any way.

The policy must be cross-platform and cross-medium. It is crucial that not only is this standard accessible through all the many methods of online access available today, but it must also be equally accessible in the offline world. This requirement separates the PNS from recent attempts to improve privacy in America. The PNS identifies the need for improved privacy offline as well as online and seeks to avoid creating a disparity between online and offline data handling procedures.

To meet these aims, the standard is based on a simple template that all companies who collect PII must display above their privacy policy. The template involves a table, which the company is responsible for filling in, and several explanatory footnotes. The idea behind this standard comes from the "Nutrition Facts" panel. Consumers know that on all food packaging, they will find a panel containing certain required bits of nutritional information. We want similar expectations for privacy notices. The following page outlines the exact structure of the PNS template.

[17] Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, Hearing on S. 2201 before the Senate Committee on Commerce, Science, and Transportation, April 25, 2002, p.2. Available online at http://www.epic.org/privacy/internet/s2201_testimony.htm.

Privacy Notice

Company Names *Date of last revision*
Company Address *[Proposed date of next revision]*

Data Item (1)	Collection method (2)	Anonymity (3)	Shared with third parties (4)	Use within company (5)	Use by third parties (6)

(1) This is a description of the actual data item that is collected.

(2) The means by which the data item or data items are collected. Can take two values:
Explicit: requires the customer to explicitly submit the data.
Automatic: Information that is collected automatically, without the customers explicit consent.

(3) Indicates whether the data item, or any part of the data item will be linked to you personally in any way. If 'Anon', then the data can never be linked to you without your consent to a change in this privacy policy. If 'PII', then the data is Personally Identifiable Information.

(4) Indicates whether the data item, or any part of the data item, will be shared with third parties
YES: Your data item will be shared with third parties.
YES, OPT-OUT: You have the option of telling the company not to share your data.
YES, OPT-IN: You have to tell the company that you want your data to be shared
NO: No, none of your data will be shared with third parties

An exception is made regarding third party companies who are directly connected with a business transaction to which the customer has consented to, such as credit card companies and delivery companies. These companies do not need to be declared in columns (4) or (6).

(5) This field tells you what the company uses this data for.

(6) If the data is shared with a third party, what is the data used for within this third party.

Company Privacy Policy starts here.

The standard would also require legislative backing, as does the Nutrition Facts panel. The key to the success of the legislation is the palatability of the PNS to those who are least likely to want to accept it. In this respect, the PNS needs to be fully explained and the relationship of the PNS to the company fully defined. The rules proposed below are intended to be clarifications of the ways in which the PNS template should be filled out.

Rules and Regulations for the Completion of the PNS Template

The first requirement is that any commercial company, organization or website ("company") that collects data from consumers must have a privacy notice that complies with the PNS. There is one exception to this: if all the data collected by a company would be classed as "Anonymous" in column (3), then the Privacy Notice is not required. The Privacy Notice is intended to inform consumers and, as such, is not required for companies who only collect data from other companies, e.g. B2B companies.

If data is collected online, the Privacy Notice must be displayed online, in a format that can be viewed on any platform. The Privacy Notice must look the same onscreen as it does offline, as shown above. It must be linked to on the home page of the website, and on any page where any data item is collected. This link must be available as a text link, marked "Privacy Notice." The site can, at its own discretion, use an image link as well. If the data is collected offline, then a Privacy Notice must be able to be provided upon request. If data is collected on a premises, then a notice must be stored on those premises. If the data is collected off premises, then the company must be able to provide access to a notice upon request.

The company must maintain the order of information as outlined in the PNS template. This requirement ensures that the most important part, the table, remains at the top of the page so that consumers can quickly and easily see the core of the company's privacy policy. The company can still include additional information, such as its original privacy policy, if the company feels that this information is useful to the consumer.

Columns (2), (3) and (4) must only contain the options listed in the key beneath the template table. Column (1) must contain a concise description of the data item or data items being collected from the consumer. Examples might be "email address" or "records of goods bought." The company does not need to declare data collected from other companies.

The company must try to fill in (5) as concisely as possible, without omitting any uses of the data item(s). Examples include "mailing lists", and "identification". If column (5) is filled in as "NO", then column (6) must be filled in as "---". Otherwise the company must try to fill in (6) as concisely as possible, without omitting any third party uses of the data item(s). Examples include "third party mailing list" or "market research data sharing". Separately incorporated affiliates and subsidiaries of the company that receive data collected under the PNS must be counted as third parties, unless they are directly involved in a transaction to which a customer has consented.

The company is responsible for correctly filling in the template and ensuring that the information within the table remains accurate. If the information in the table changes in any way, then the date at the top right must reflect this change. If a change needs to be made to the content of the table due to a change in the company's privacy policy, the company must give 28 days notice before the change is implemented. This notice must be given at the top of the table, below the active revision date. This may be omitted if no revision is planned within the next 28 days.

Any data collected under this Privacy Notice must always be treated according to this version of the notice. If the company decides to make a change in its policies requiring a change in the information in the Privacy Notice table, then any data that was collected before this change in policy must still be used according to the original PNS that was in effect when the data was collected. The company may, at its own discretion, provide the customer with an opt-in notice if the company wants to use data in a way other than as listed in the original PNS.

Enforcement

As well as rules for the completion and posting of the standard, the legislation backing the PNS will also need to include information about penalties for non-display, incomplete display or incorrect display.

As the FTC has been heavily involved in the development of privacy legislation both online and offline, it is a logical step to make the FTC the governing body for the PNS. In S. 2201, Senator Hollings takes the same viewpoint and has proposed that the FTC set the standards within S. 2201 and be responsible for its enforcement. The FTC will be responsible for investigating complaints based on an incorrect or missing PNS. If a customer believes that a PNS contains a material inaccuracy, then it is his responsibility to report this to the FTC. The FTC will investigate the complaint. If the claim proves valid, the FTC will require the company to correct the errors in its PNS within seven days. Failure to comply with the request will result in a fine. If the company fails to comply within the seven day period on more than three occasions in any five-year period, the company will be subject to further punishment. The FTC will have the right to impose further fines, and in extreme cases the FTC will have the option of starting a move of de-incorporation of the company. In all cases, the company has the right to appeal.

The FTC will be responsible for regular privacy sweeps, similar to the annual privacy policy checks the FTC already conducts, to check that businesses are adhering to their stated Privacy Notices. It will also mediate and render judgment in disputes between consumers and companies when there is disagreement over the clarity of the language used to convey the information provided in the Privacy Notice. In the case of a ruling against a company, the FTC will allow seven days for the amendment of the Privacy Notice, with the same enforcement provisions as detailed above. The FTC may, in addition, penalize the company further if it believes that the company deliberately used misleading language to deceive consumers. The FTC already has the power to act on false statements made by a company:

> Section 5 of the Federal Trade Commission Act grants the FTC jurisdiction over unfair and deceptive trade practices. A company that makes false statements to consumers about its information practices is subject to investigation by the FTC.[18]

The PNS is to be implemented nationwide. It does not interfere with any state-based content rules; it must merely be prefixed to any state-mandated privacy notice. If an individual has had his data used in a way not compliant with the PNS notice under which his data was submitted, then he has the right to private action only under existing state or federal law.

Additional Recommendations

The FTC should set up a web page listing companies and sites with one or more privacy policy violations in the past 5 years, intended to be a "bad guy" list. This page should also be available in hard copy format on request via a toll-free telephone number. Although less important, it may also be a good idea for the FTC to set up a second web page listing companies and sites with the best privacy policies and adherence, grouped by industry, creating a complimentary "good guy" list. This would provide companies with a public relations incentive to strengthen and adhere to their own privacy policies.

The Benefits of Approaching Privacy Issues with the PNS

The PNS has been designed to reflect both the needs of the consumers and the needs of the companies who expressed their views at the hearing for S. 2201 last month. It tries to achieve a balance between those who want legislation that is as far reaching and encompassing as S. 2201 and those who feel that the costs in implementing such legislation would far outweigh the limited gains they perceive.

The first issue that the PNS tackles is the lack of clarity offered by privacy policies. We believe that the PNS is very clear. For each data item collected, the PNS explicitly allows the consumer to see what is done with that data. Columns (2) to (6) were chosen to convey the minimum amount of information about the collection and use of data that still allows for informed choices to be made.

The PNS is designed to avoid overly burdening companies. Companies will have to carefully decide how best to fill out the form, but following that, it will be a simple issue of printing out a copy on paper or posting a copy on their servers. Companies are not required to actively inform all of their existing customers of the new implementation, or any subsequent changes that they make to their Privacy Notices. Extending the Nutrition Facts panel analogy, there are no rules requiring Kraft to give explicit notice to its customers whenever the nutritional content of Easy Mac® changes. Instead, the onus is on the customer to check for themselves. Implementing the PNS in this way will appease large businesses, who feel that requirements to actively inform customers about privacy policies incur great expense. This is especially the sentiment in the financial

[18] *Privacy and Online Politics: Is Online Profiling Doing More Harm Than Good for Citizens in our Political System?,* The Center for Democracy & Technology. Available at http://democracyonline.org/taskforce/conferences/CDTpaper.pdf.

world, where the GLB required the sending of over 1 billion letters to customers informing them of privacy policies.

It can be claimed that the PNS does not serve to regulate what information companies collect or how they collect such information. We argue, however, that this is a virtue of PNS, not a shortcoming. First, it is useful to return to the Nutrition Facts analogy. There are no rules or laws regarding the nutritional content of the food that food manufacturers produce, merely a requirement to declare the content. However the Nutrition Facts panel has provided consumers with a quick, easy way to compare food based on nutritional value as well as on price. This ease of comparison has created a market for such foods as General Mills Total® range of breakfast cereals. These cereals contain 100% of the RDA of many vitamins and minerals, which consumers can verify from the Nutrition Facts panel on the side of the carton. General Mills is competing with other cereal manufacturers, not just on price but on nutritional content. It is hoped that the PNS will foster the same kind of competition, introducing a situation where companies like Amazon.com and Outpost.com will compete both in price and privacy offered. Instead of consumers having to look at questionably hollow claims in vague privacy policies, they can quickly check using the PNS. Such comparisons will push companies towards having good privacy policies and thus use the market to solve the problem. Second, trying to restrict data collection is extremely difficult to do effectively without causing a lot of new problems. S.2201's categorizations of Sensitive and Non-Sensitive data has been criticized as arbitrary, with former Commerce Committee Chairman Muris once pointing out that S. 2201 treats the fact that he is a Republican as more sensitive data than a list of books that he reads. Additionally, if the baseline for regulation is set too low, then the new legislation is rendered useless. If the baseline is set too high, then the costs to business may indirectly harm consumers by severely reducing the services available to them. Passing new legislation has always been a balance between the goals of the legislation and the economic impact of the legislation's passage. By not restricting collection or use of data, PNS affords the maximum benefit of notice to consumers while minimizing the cost of implementation to business. PNS can be thought of as a first step to fixing privacy problems, but we think it is better to return to the first argument above and claim that the PNS will actually negate the need for further policies.

The PNS also avoids the security concerns raised by Amazon.com, in response to S. 2201's requirement that customers be able to access, correct and delete their data, by not imposing any right of access on the companies. Implementation of PNS, unlike S. 2201, does not impose a large engineering burden on companies.

Another feature of the PNS designed to coax the market into improving privacy policies is the allowance of grouped data items. This is designed to encourage companies to do less with the data that they collect. To be able to lump data items, then all the data items within the group need to have the same anonymity, use with third parties and method of collection. The ways a company can lump data is explained and illustrated in the examples later on.

During the S. 2201 hearing in April, businesses asked for better nationwide privacy guidelines, as privacy regulations currently vary from state to state. Businesses

trading in many states, especially online companies who may have a base in one state but trade in multiple states, are finding compliance with all the different state privacy regulations difficult. The PNS does not address these complaints, but for a very good reason. The PNS applies to all companies, regardless of their online or offline status. This was done to avoid creating an unfair disparity between online and offline regulation. However, it makes the PNS so encompassing that if the PNS were to also preempt state laws, individual states would essentially lose control over all state commerce, a notion to which they would most certainly object.

Finally, a major criticism of S. 2201 is the extent to which it leaves online companies liable to class action and private action suits. In his testimony, Paul Misener of Amazon.com expressed fears that even with a limit of $200 on the damages payable, with a customer base of 35 million, a class action lawsuit would be devastating to the company. The PNS, on the other hand, offers no specific right of action to the consumer over incorrect privacy policies. The FTC has power to pursue complaints, but any further private or class action is reliant only upon existing laws.

Examples of Privacy Notices

To illustrate the idea behind the PNS template, four example are presented below of how some online and offline companies would fill in the table in the PNS. The examples are that of an online store (such as Outpost.com), an online service provider, a supermarket, and a hospital. For simplicity, the headers and footnotes associated with the table are omitted in the presentation below. In a real implementation of the PNS, these would have to be included.

Example of an Online Store's Privacy Notice

Data Item (1)	Collection method (2)	Anonymity (3)	Shared with third parties (4)	Use within company (5)	Use by third parties (6)
Email address	Explicit	PII	YES, OPT-IN	Login ID, optional mailing lists,	third party mailing lists
Password	Explicit	PII	NO	Login ID	---
Name	Explicit	PII	NO	ID, billing, delivery	---
Address	Explicit	PII	NO	ID, billing, Delivery, optional mailing lists	---
Tel. No	Explicit	PII	NO	ID, billing, delivery, customer service	---
Credit card information	Explicit	PII	NO	ID, billing	---
URLs visited (click stream)	Automatic	PII	NO	Tailoring of service (optional)	---
Operating System	Automatic	PII	NO	Tailoring of service (optional)	---
Browser type	Automatic	Anon	NO	Anonymous usage statistics	---
IP Address	Automatic	Anon	YES, OPT-OUT	Anonymous usage statistics;	web banner advertising

This single table shows clearly what data the online store collects, and how it uses that data. Consumers can immediately see that this online store does care about their privacy. The majority of the data that is collected is not passed on to third parties. The two data items that may be given to third parties are only passed on if, in the case of the email address, the customer explicitly give his consent (opt-in), or, in the case of the IP address, the customer doesn't decide to remove his consent (opt-out).

The store customer can also quickly see from column (5) that all the uses for the data are "good" uses. The service tailoring is optional, and being added to any mailing lists within the online store is optional. As stated in the regulations, this online store can fill in (5) as they see fit. This online store has chosen to include the word "optional" to further reassure customers without making the table overly complicated. Under the PNS, it would have been sufficient for the online store to omit the word "optional."

Again to reiterate, the online store can still include its own privacy policy beneath this table.

Example of an Online Service Provider's Privacy Notice

Data Item (1)	Collection method (2)	Anonymity (3)	Shared with third parties (4)	Use within company (5)	Use by third parties (6)
Email address	Explicit	PII	YES	Login ID, mailing lists,	mailing lists
Name	Explicit	PII	YES	ID, billing, delivery	mailing lists
Password	Explicit	PII	NO	Login ID	---
Nickname	Explicit	PII	NO	ID	---
IP Address	Automatic	PII	YES	Demographic and geographic usage statistics	advertising companies

This example is used to show that online privacy is not limited to companies who partake in online commerce. The online service provider could be the online support arm of a company, such as Apple Computer's AppleCare, or a subscription service, such as the online magazine MacUser UK. The user of this service can quickly see that not much data is taken. However, the user can also quickly see that this service does not seem to care much about the user's privacy. Most of the data is passed on to third parties, and all of the data is linked to a personal profile. The service does not give the user any way to prevent data from being passed on third parties.

Again this service has complied with the PNS. It was the company's decision to only declare the third party use as "mailing lists". They could have voluntarily been more explicit and declared who those third parties actually are.

Example of a Supermarket's Privacy Notice

Data Item (1)	Collection method (2)	Anonymity (3)	Shared with third parties (4)	Use within company (5)	Use by third parties (6)
Name	Explicit	PII	YES, OPT-IN	Reward Card	Promotional materials
Street Address	Explicit	PII	YES, OPT-IN	Reward Card, promotional mailings	Promotional mailings
Zip Code	Explicit	PII	YES, OPT-OUT	Reward Card, promotional mailings, anonymous usage statistics	Promotional mailings, anonymous usage statistics
Tel no.	Explicit	PII	YES, OPT-IN	Reward Card, promotional information	Market research
Email	Explicit	PII	YES, OPT-IN	Reward Card, promotional information	Promotional mailing list
Details of goods bought using Reward Card	Automatic	PII	NO	Tailoring offers; Anonymous usage statistics	---
Details of goods bought not using Reward Card	Automatic	Anon	NO	Anonymous usage statistics	---
Time of day you shop	Automatic	Anon	YES	Anonymous usage statistics;	Anonymous usage statistics

This example demonstrates the implementation of the PNS in the offline world, specifically by a supermarket. Again, the supermarket's customers can quickly see the types of information collected and the uses of that information. This is another good policy, and this supermarket clearly has good privacy policies. The customer can see that PII is only collected as part of the store's Reward Card scheme. Any PII is only passed on to third parties with an opt-in decree. Only anonymous data is passed onto third parties without the customers explicit consent. Another interesting comment about this

policy is that it shows a flexibility within the structure of the table. Column (1) requires a listing of the data items that are collected. This list must be fully comprehensive, but does not prevent the lumping of data. The online store shown in the first example simply declared "Address". The supermarket, on the other hand, has to split this into a "street address" and a "zip code", so that it can declare that the zip code is classed as YES, OPT-OUT in Column (4) and is used by those third parties for anonymous usage statistics. This complicates the table somewhat but has to be done to ensure compliance with the PNS. It is hoped that rather than create complicated tables, the companies would prefer to group and apply uniform privacy standards to multiple data items. The supermarket above could group zip code and street address if either it made the street address YES, OPT-OUT or made the zip code YES, OPT-IN. Rather than tell customers that they have to act to prevent his street address being given away, we think that the supermarket would prefer to improve the privacy on the zip code. The same could happen with the two rows relating to the details of goods bought. The supermarket has to split them since the anonymity differs. If both were made anonymous, then the table would be made simpler and privacy would be strengthened.

Example of a Bank's Privacy Notice

Data Item (1)	Collection method (2)	Anonymity (3)	Shared with third parties (4)	Use within company (5)	Use by third parties (6)
Account details	Explicit	PII	NO	Transactions, account management	---

This example shows an extreme case of data item lumping. Here, all the data that the bank collects from its customers falls under the same categories in columns (2), (3) and (4). The bank therefore has the option to lump all the data items as "Account details". All these items are explicitly collected and are not used by any third parties. The customer can now tell very quickly how data is treated by this bank. The opposite situation would be a bank which listed every item with different entries in columns (2), (3) and (4). In such a situation, a consumer would be confused and would be more likely to bank with an institution that has a simple policy as shown above.

Conclusion

To conclude, we believe that legislation is needed in the U.S. to tackle the threats to privacy both online and offline. We believe that the best way to approach these problems is the implementation of the PNS, backed with the federal legislation suggested. As Senator Hollings said in the April 25 hearing on S. 2201, "Good privacy means good business." Rather than directly implementing legislation that forces businesses to treat customer data in specific ways, the PNS merely makes businesses' privacy practices much more explicit. We believe that the accessibility of privacy notices, and the ease with which policies can be compared, will drive businesses to strengthen their policies in

response to market forces. The March 2002 *Report on the Information Practices and Policies of Commercial Websites* from the Progress & Freedom Foundation states:

> Most striking to us is the fact that the most significant changes come in areas that seem to be of greatest concern to consumers, especially the sharing of information with third parties (more notice, more choice), and increased measures to protect the security of data. While poll results may be ambiguous on the importance of fair information practices to consumers, the results here suggest that such practices are meeting the test of the marketplace: they are becoming more common, not less.[19]

The PNS answers all of the complaints raised against S. 2201, and provides the "robust notice" that is sought within this act. Crucially, PNS will not require nearly the same amount of effort from companies, or anywhere near the same expense to implement. The PNS is also much closer to the business ideals at the heart of America. In the most capitalist economy in the world, the market should, when possible, be left to find a balance. When this does not happen because of deceptive business approaches, the deception should be attacked, not the businesses themselves.

Acknowledgements

We would like to thank Prof. Hal Abelson, Barbara Lawler, and Ted Wilson for their help in researching this paper.

[19] Adkinson Jr., William F., Eisenach, Jeffrey A., Lenard, Thomas M. , *Privacy Online: A Report on the Information Practices and Policies of Commercial Websites*, Special Report, The Progress & Freedom Foundation, March 2002, p. 28.

DECLARATION OF AUTHORSHIP:

EDITOR: Corinna Sherman

CONTENT:
pgs. 3-7 – Corinna Sherman
pgs. 8-20 – Roland Burton (commencing from "Our Proposed Solution")
pg. 21 (Conclusion) Jointly authored