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

Chairman Hollings, Senator McCain, and members of the Committee, my name is Paul Misener. I am Amazon.com's Vice President for Global Public Policy. Thank you for inviting me to testify today on S. 2201, The Online Personal Privacy Act.

Although, as I will describe throughout this testimony, Amazon.com has serious concerns about several aspects of this bill, we greatly appreciate the time and energy you and your staff have committed to consumer information privacy issues, as well as your continuing willingness to hear Amazon.com's perspectives.

Amazon.com also gratefully acknowledges that S. 2201 contains two important provisions that we could support. First, this bill would confirm our belief that the privacy

promises a company makes to consumers must still apply to the private information consumers provide to that company, even after ownership of the company or information changes. Second, S. 2201 intends to preempt inconsistent or additional state laws. It would be difficult or impossible for nationwide websites to comply with as many as fifty conflicting laws, and it would be unfair (if not also unconstitutional) to permit the citizens of one state to make the privacy decisions for the citizens of another. Both of these provisions in S. 2201 are welcome and would be good for our customers, company, and industry.

As for our concerns, Mr. Chairman, Amazon.com is the Internet's number one retailer and, therefore, has as much experience (and as much at stake) as any other entity on these issues. On behalf of our customers and company, we look forward to working with you and your Committee to address the concerns we raise in this testimony. I hope that you will welcome our perspectives in the constructive and cooperative spirit in which they are offered.

Privacy at Amazon.com

Mr. Chairman, Amazon.com is pro-privacy. The privacy of personal information is important to our customers and, thus, is important to us. Indeed, as Amazon.com strives to be Earth's most customer-centric company, we must provide our customers the very best shopping experience, which is a combination of convenience, personalization, privacy, selection, savings, and other features.

Therefore, Mr. Chairman, Amazon.com shares your goal of providing consumers the personal privacy protections they want, and we already provide most of the substantive protections that a reasonable interpretation of your bill would require. At Amazon.com, we manifest our commitment to privacy by providing our customers notice, choice, access, and security. Before I describe these four facets of privacy protection at Amazon.com, please allow me to explain how we use customer information.

Personalization at Amazon.com

In general, Amazon.com uses personally identifiable customer information to personalize the shopping experience at our store. Rather than present an identical storefront to all visitors, our longstanding objective is to provide a unique store to every one of our customers, now totaling well over 35 million people. In this way, our customers may readily find items they seek, and discover other items of interest. If, for example, you buy a Stephen King novel from us, we likely will recommend other thrillers the next time you visit the site.

Amazon.com now inserts, among the now-familiar "tabs" atop our Web pages, a special tab with the customer's name on it. When I visited Amazon.com's site last week, for example, the tabs included Books, Electronics, DVDs, and "Paul's Store." By clicking on the "Paul's Store" tab, Amazon.com introduced me to six smaller stores, including one named, "Your Kitchen and Housewares Store," which featured a Calphalon Commercial Nonstick Collector's Edition 10-Inch International Griddle/Crepe Pan, which I promptly bought.

It was no coincidence, of course, that Amazon.com recommended this crepe pan to me, and that I liked it: using so-called "collaborative filtering" techniques, which compare my past purchases (many of which are cookware items) to anonymous statistics on thousands of other Amazon.com purchases, Amazon.com computers automatically – and correctly – predicted that I would want that crepe pan.

Similar personalization is provided in the traditional Amazon.com recommendations on the home page, in purchase follow-up recommendations, in the "New for You" feature, and in some varieties of email communications. Customers can improve the quality of these recommendations in several ways, including by deleting individual Amazon.com purchases from consideration, and by rating the products they buy at Amazon.com or elsewhere. For example, last year I bought my niece a few CDs from the singer Britney Spears but, because I do not want similar music recommended to me, I have deleted these CDs from the list of items Amazon.com uses to produce my recommendations. In addition, on Amazon.com's site, I can rate a CD that I might have purchased at Wal-Mart, in order to improve the quality of Amazon.com's music recommendations to me.

Obviously, Amazon.com's personalization features directly benefit our customers. And, just as obviously, these features require the collection and use of personally identifiable customer information. The question, then, is how do we protect the privacy of this information?

Privacy Practices at Amazon.com

As I indicated earlier, Amazon.com manifests its privacy commitment by providing notice, choice, access, and security.

Notice. Amazon.com was one of the first online retailers to post a clear and conspicuous privacy *notice*. And in the summer of 2000, we proudly unveiled our updated and enhanced privacy policy by taking the unusual step of sending email notices to all of our customers, then totaling over 20 million people.

Choice. We also provide our customers meaningful privacy *choices*. In some instances, we provide opt-*out* choice, and in other instances, we provide opt-*in* choice. For example, Amazon.com will share a customer's information with a wireless service provider only after that customer makes an opt-*in* choice. We simply are not in the business of selling customer information and, thus, beyond the very narrow circumstances enumerated in our privacy notice, there is no information disclosure without consent.

Access. We are an industry leader in providing our customers *access* to the information we have about them. They may easily view and correct as appropriate their contact information, payment methods, and purchase history. And, with a feature called "The Page You Made," customers even can see part of the "click-stream" record of products they view while browsing Amazon.com's online store.

Security. Finally, Amazon.com vigilantly protects the *security* of our customers' information. Not only have we spent tens of millions of dollars on security

infrastructure, we continually work with law enforcement agencies and industry to share security techniques and develop best practices.

It is very important to note that, other than an obligation to live up to pledges made in our privacy notice, there is no legal requirement for Amazon.com to provide our customers the privacy protections that we do.

Market Forces at Work

So why do we provide notice, choice, access, and security? The reason is simple: privacy is important to our customers, and thus it is important to Amazon.com. We simply are responding to market forces.

Indeed, if we don't make our customers comfortable shopping online, they will shop at established brick and mortar retailers, who are our biggest competition. Moreover, online – where it is virtually effortless for consumers to choose among thousands of competitors – the market provides all the discipline necessary. Our customers will shop at other online stores if we fail to provide the privacy protections they demand.

These market realities lead Amazon.com to eschew the term "industry self-regulation." We believe this concept – which often is touted as a substitute for legislation and government regulation – suggests that companies must act altruistically in order to provide consumers the protections they deserve. But this suggestion simply is not true.

Companies must provide the privacy protections consumers demand or be forced out of business. Nowhere is this more true than among website-based retailers: a consumer can easily choose among hundreds of retailers without leaving her home. Contrast that with brick and mortar retail, which presents consumers with only a very small number of store choices within a reasonable driving distance.

Moreover, as Amazon.com has consistently stated, and last year testified before this Committee, these market realities also lead us to conclude that there is no inherent need for privacy legislation, at least for typical website-based business-to-consumer commerce. The Federal Trade Commission's annual privacy sweeps (this year conducted by the Progress and Freedom Foundation at the behest of the Commission) confirm that those companies with high levels of privacy protections are the ones that succeed in this robust market. There simply is no market failure for legislators to address; indeed, as just noted, the "online" retail market is inherently more competitive than that of traditional "offline" retail. Put another way, if there is a market failure, it is with *off*line, not online consumer transactions.

Notwithstanding these points on the inherent need for legislation, Mr. Chairman, Amazon.com wants to work cooperatively and constructively with you and your Committee on this issue. For S. 2201, we have one general concern, and several specific concerns, which I will describe momentarily. Let me again say, however, that we greatly appreciate the work you and your staff have put into this bill.

Fairness Among Transactions and Consumers

Before addressing specific provisions of S. 2201, please allow me to comment on what Amazon.com believes to be the bill's most serious shortcoming: As drafted, S. 2201 would require companies to provide various privacy protections, but only for a tiny fraction of consumer transactions. And, S. 2201 would not require companies to provide any protections for tens of millions of American consumers with relatively low incomes and limited educational backgrounds.

As I previously have testified before this Committee, Amazon.com believes that privacy legislation must apply equally to online and offline activities, including the activities of our offline retail competitors. It makes little sense to treat consumer information collected online differently from the same (or often far more sensitive) consumer information collected through other media, such as offline credit card transactions, mail-in warranty registration cards, point-of-sale purchase tracking, and magazine subscriptions.

Offline Privacy Practices. For example, the offline consumer information collection practices of brick and mortar retailers are described on the website (http://www.epic.org/privacy/profiling/) of the Electronic Privacy Information Center (EPIC):

> "Many supermarkets are offering membership cards that grant discounts to consumers. What often goes unmentioned is that these club cards enable the store to create detailed profiles of individuals' consumption habits. These profiles are linked to individually-identifiable information, often with the requirement at enrollment that the consumer show state-issued

> identification. Since many supermarkets sell more than just food (alcohol, cigarettes, pharmaceuticals, etc.), the companies can collect volumes of information about individuals' habits.
>
> "The danger in this profiling is increased by the fact that supermarkets are not limited by law in sharing the information they collect. A supermarket can sell the information to a health insurance company or to other aggregators in order to make a more complete profile on an individual.
>
> "The risks of profiling based on consumption are often derided by supermarket profilers. They may say that "no one cares if you like asparagus more than broccoli." But, that's not the issue. Individuals have different definitions of sensitive information. And the profilers aren't interested in whether you're buying one vegetable over another. They are more likely to want to know whether an individual is buying baby diapers or adult diapers."

My wife and I know about these offline privacy practices firsthand. Our son is nearly five months old. Last month, after buying many packages of baby diapers from Giant Food, where we have a "loyalty card," we received a Giant Food "baby brochure," which essentially is an advertising packet. Clearly, this baby brochure solicitation from Giant came merely as a result of purchasing baby products from Giant stores: Giant's computers compiled information about our buying habits and decided to start sending us baby literature.

To be clear, I don't mind receiving such solicitations nor, I believe, do most Americans. It makes more sense for me to receive baby product ads than the brochures I often receive on lawn care services in spite of the fact that I live in a townhouse. I just mind that S. 2201 would ignore such offline practices, yet regulate the exact same personalization services provided by online entities such as Amazon.com.

Warranty registration cards, as EPIC also points out on its website, are yet another way offline entities collect, enter into electronic databases, and sell personally identifiable information that often is entirely unrelated to the subject of the warranty. Several weeks ago, my wife and I needed to buy a new clothes washer and dryer. The warranty registration cards for these large and potentially dangerous appliances had labels telling us to complete and return the cards in the interest of safety. But, for some reason, they also needed to know our household income and our reading habits! Consumers are essentially asked to either provide private information or be unsafe. Similarly, an earlier purchase of a small, but potentially dangerous, space heater included a warranty registration card (again emphasizing the safety aspects of registration) that asked for my household income, where my family took our last vacation, whether we read the Bible, and whether anyone in the household has prostate problems. Because the private information sought from consumers is clearly unrelated to the product subject to the warranty, and probably unrelated to other products sold by the manufacturers of my washer/dryer and space heater, it is obvious that, under the guise of safety, highly private consumer information is being collected and sold.

Obviously, these offline privacy practices are no less deserving – and often far more deserving – of Congress' attention than online practices. Amazon.com firmly believes that, in fairness to consumers (if not also companies), online and offline privacy practices must be treated equally.

The former and current chairs of the Federal Trade Commission have supported this view. In testimony before this Committee nearly two years ago, on May 25, 2000, then-Chairman Robert Pitofsky, in a colloquy with Senator Kerry, testified that,

> "[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."

Current FTC Chairman Timothy Muris, in testimony before the Senate Appropriations Committee on March 19, 2002, said that,

> "Consumers are deeply concerned about the privacy of their personal information, both online and offline. Although privacy concerns have been heightened by the rapid development of the Internet, they are by no means limited to the cyberworld. Consumers can be harmed as much by the thief who steals credit card information from a mailbox or dumpster as by the one who steals that information from a Web site."

And, last October, in a speech to the Privacy 2001 Conference, Chairman Muris specifically addressed the scope of privacy legislation, saying,

> "I am concerned about limiting legislation to online practices. Whatever the potential of the Internet, most observers recognize that information collection today is more widespread offline than online. Legislation limited to online practices perhaps seemed attractive when Internet commerce was expanding almost limitlessly. Today, however, it is increasingly difficult to see why one avenue of commerce should be subject to different rules than another, simply based on the medium in which it is delivered."

Mr. Chairman, parity is necessary in fairness to online companies. It simply would not be equitable to saddle online retailers with requirements that our brick and mortar (or mail or telephone order) competitors do not face, nor would it be fair to mislead consumers by telling them their privacy would be substantially protected by an online-only bill when, in fact, only a tiny fraction of their transactions would be addressed.

Online-Offline Differences. Some people contend, however, that online activities deserve discriminatory treatment under the law because of some inherent differences between online and offline business-to-consumer relations. As described above, there are many obvious similarities. I acknowledge, however, that there are three relevant differences between online and offline. Although one of these differences could lead to online consumers having relatively less privacy, the other two differences actually give online consumers more privacy protection than offline consumers.

The one difference that potentially gives online consumers less privacy protection is the availability of so-called "click-stream" information, by which a website operator can observe, for example, what individual visitors see while visiting a website. In the retail context, this means web-based retailers can tell what a customer looks at, not just what he buys.

Amazon.com has turned this technical capability into customer-friendly features by which we better personalize our customers' shopping experience. We do this in two

principal ways: First, we automatically display items that take into account a customer's recent shopping. If a customer has been looking at cameras, for example, the site may automatically display for her a camera tripod. Second, in our "The Page You Made" feature, we display, on the side of the screen, links back to some of the items the customer has looked at. Thus, instead of scrolling back through the site (the online equivalent of walking back to the other side of the store), we provide a simple way for a customer to get back to the items she earlier examined. Again, these features rely on the use of "click-stream" information.

But even this ability to see what is shopped but not bought is not entirely unique to online entities. Professor Clarke L. Caywood, in his top-selling marketing and PR textbook, *The Handbook of Strategic Public Relations & Integrated Communications* (McGraw-Hill, 1997), describes the same practice in the brick and mortar world:

> "Marketers at Wal-Mart, a large discount retail chain, for example, spend several days each week in their own stores (and those of the competition) watching consumers shop, questioning them about their purchases, and asking them for feedback. At the end of each week, they return to their headquarters office and, in conjunction with their colleagues who have also spent time in stores in other locales, they discuss what's on the consumer's mind, what trends they need to watch, and what problems they need to correct. Armed with that information, they can tailor all manner of programs to the immediate needs of customers in a very specific local area."

Importantly, even if Congress considers the "click-stream" difference between online and offline to be crucial enough to warrant discriminatory treatment under the law, no federal bill introduced to date, not even S. 2201, is based upon this particular

difference. Rather, S. 2201 and previous online-only bills would apply discriminatory legal treatment to activities that, for all practical purposes, are identical online and offline.

And, if differences between online and offline activities are the key, online transactions, in two important respects, actually protect consumer privacy better than offline transactions. One respect is physical characteristics. Those Wal-Mart employees said to follow consumers around stores – and, indeed, any employee of a brick and mortar store, watching from the floor or hidden cameras overhead – can see physical personal characteristics unknown to online retailers. Wal-Mart knows your sex and race; if you are pregnant; how well you dress; and if you have acne.

They also know where you are. Indeed, when one of Amazon.com's customers visits our store, we cannot know their location. They may be at home, at the office, with their laptop computer at the airport, on the beach with their wireless PDA, or at an "Internet Café" in Paris. We simply don't know. But, when I use my Mobil credit card, Exxon-Mobil knows exactly where I am, and can track my movements. My physical location at any given time is, I would think, highly sensitive information. And, yet, by my reading of Mobil's privacy policy, Exxon-Mobil would not even allow me to opt-out of Mobil using that information internally or sharing it with Mobil's "joint marketing partners." S. 2201 would do nothing to change such offline situations, but would require online retailers to obtain (as Amazon.com already does) opt-in approval before

transferring sensitive information. Again, if there's a privacy problem somewhere, it's offline.

And, for those who point out that offline consumers can always wear dark sunglasses or pay cash in order to remain anonymous, I note that online consumers have many, much easier ways to remain anonymous. They may easily set their web browser to block cookies or may use anonymizing software tools provided by companies such as Zero-Knowledge Systems. Amazon.com's privacy notice describes how to block cookies and provides link to Zero-Knowledge and other anonymizer companies.

Amazon.com Compliance with a Privacy Bill. At last summer's House Commerce Committee hearing on privacy, one Committee member kindly noted that the companies represented, including Amazon.com, are "the good guys." The implication was that the "bad guys" should be the target of privacy legislation, and that we "good guys" need not fear a reasonable law.

In one sense, this Representative was exactly right. Amazon.com does not fear the direct effects of reasonable privacy legislation because, unlike the vast majority of our competition in the brick and mortar world, we already provide notice, meaningful choice, access, and security. Indeed, if truly reasonably interpreted, almost all of the substantive requirements of S. 2201 likely would have little direct effect on Amazon.com and its customers. (The most notable exception would be the bill's extraordinarily burdensome access/deletion requirement.) We already are providing the privacy protections at the

heart of this bill, including excellent access by customers to their own private information, simply because that is what our customers want.

Offline Compliance with a Privacy Bill. However, in addition to a grave fear of being unfairly exposed to a spate of highly unreasonable lawsuits (which I will discuss in a moment), we fear any law that implicitly allows our offline competitors free rein to continue to be privacy "bad guys," unbeknownst to consumers. Indeed, although we are confident that, if consumers really knew what was happening to their private information in the offline world, instead of being mislead to believe that their privacy is more at risk online, they actually would flock to do business with online "good guys" like Amazon.com. But, with the considerable media hype and misinformation surrounding online privacy issues, and the relative dearth of revelations about offline consumer information privacy practices, we believe it would be very unfair to let our competitors surreptitiously collect, use, or transfer consumers' private information.

Consumers Online and Offline. But most importantly, it would be fundamentally misleading to American consumers to enact a law that applies only to online entities because, for the foreseeable future, the putative protections of such a law would apply to just a tiny fraction of consumer transactions. Last year, online sales accounted for only one percent of all retail trade in the United States. Obviously, any law that addresses only online transactions could not benefit consumers much at all compared to one that equally addresses online and offline activities. Moreover, a law that addresses only online activities would have the perverse effect of failing to provide any benefits to those

on the less fortunate side of the digital divide. Indeed, consumers who, because of economic situation, education, or other factors, are not online would receive no benefits from an online-only law.

Prior Online-Only Approaches. This is not to suggest that an online-only approach never was credible. To the contrary, based on what little was known publicly about both online and offline privacy practices as recently as two years ago, one reasonably could have concluded at the time that online privacy issues deserve discriminatory treatment, especially in order to avoid a potential "privacy disaster."

No disaster has occurred, and we believe that facts gathered by this Committee and other bodies reveal that an online privacy disaster is no more likely than an offline privacy disaster. In addition, consumers now better understand that computers are used to record both online and offline transactions. The huge, searchable, and transferable computer databases kept by offline companies are just as much at risk as the information collections of online entities. In any case, the bills introduced to date would do little or nothing to forestall privacy disasters, either online or offline.

Moreover, as elaborated throughout this testimony, discussions over the past few years have shown that there are few meaningful differences between online and offline privacy practices, and that some of these differences actually serve to protect consumer privacy better online. And, finally, as documented in the annual online privacy sweeps conducted by the FTC, *et al*., starting in 1998, it is clear that online entities have made

extraordinary strides to enhance their privacy practices over the past four years. Offline privacy practices certainly have not improved at anywhere near this pace, if at all, over the same period.

In sum, Mr. Chairman, although currently-available facts demonstrate that online practices do not deserve discriminatory treatment, there were good reasons why many people believed only a few years ago that such discrimination was warranted.

Privacy Bill Benefits to Industry. Even if this law would do little or nothing to benefit the vast majority of consumer transactions, it has been suggested, such as in S. 2201's Findings, that an online privacy bill would be good for online companies because the consumer trust it would spawn would lead to additional sales. This belief implies that the online industry, which has not sought a bill, either does not know what is best for itself or has a hidden agenda. Speaking for Amazon.com, I can say unequivocally that our agenda since our founding in the mid-1990s, has been to provide our customers the very best shopping experience. We believe, with good reason, that if S. 2201 were enacted, it would dramatically interfere with our ability to serve our customers. Indeed, S. 2201 has been reviewed by key personnel throughout our company and has provoked expressions of grave concern, particularly in the 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. And, even if

somehow they could make our systems comply, our engineers fear that many of the bill's provisions would seriously jeopardize our systems' security and anti-fraud efforts.

Questionable Industry Support for an Online-only Bill. It is often said that, even if not a majority, at least some in "industry" support an online-only legislative approach. The relevant question is, which industry? The principal proponents of an online-only law do very little business online with consumers. One of the companies, a hardware manufacturer, does but a fraction of its business online, while its biggest competitor does 100% of its business online. It is not difficult to imagine why the first company might support a burdensome online-only approach. Moreover, this same hardware manufacturer sells business hardware and services to Internet-based companies and, potentially at least, would benefit from a law that would require substantial technical investments by online companies. Lastly, the other major technology firm that supports online-only legislation actually manufactures computer components and makes only a tiny percentage of its sales to consumers, whether online or offline. It is difficult to believe this company knows much more about serving web-based customers than Amazon.com knows about semiconductor dumping practices.

Relative Expediency of an Online-only Bill. Finally, it also has been said that "online" and "Internet" transactions are being singled out because it would be too difficult to craft a law that protects the other 99% of consumer transactions. Although it is hard to believe that expediency is the reason for the "online-only" focus, it is important to note that other bills have been (or soon will be) introduced in Congress that address

both online and offline transactions. And, certainly this Committee has jurisdiction over all channels of commerce. Moreover, passing an online-only law at this point likely would delay passage of an offline bill for many years and, thus, actually would hurt the chances of providing privacy protections for consumers offline. In any case, it certainly would not be 99 times more difficult to craft a law that protects 99 times as many consumer transactions.

Conclusion. For all the foregoing reasons, we firmly believe that any privacy legislation that moves forward out of this Committee should apply to all consumer transactions, not merely the one percent conducted online.

Key Positive Provisions in S. 2201

Mr. Chairman, as noted earlier, we believe that there are at least two key provisions in S. 2201 that we could support. We appreciate the fact that you included these in your bill. They are the following:

- Continuing Promise (Section 102(e)(1)(b)): This explicit confirmation that "the promise runs with the information" is good. Although we believe existing common law and Section 5 of the FTC act already would prevent successor entities from treating information less restrictively than was promised at the time the information was collected, we appreciate and support the enactment of this clarifying language, particularly because it removes potential ambiguity in bankruptcy proceedings.

- Preemption (Preamble Section 4): As noted above, this is a necessary and good provision to ensure equal consumer privacy protections nationwide and to allow nationwide entities to comply (it would be virtually impossible for a nationwide website to comply with conflicting rules from multiple jurisdictions). Even though state laws most likely would fail a constitutional challenge, the expense and uncertainty of litigation could be avoided with this sort of Congressionally adopted ceiling. Given the agreement on the need to preempt inconsistent state

laws, we merely need to ensure that this language is adequately clear. (Reviewing courts look for clear congressional intent; ambiguous language favors non-preemption.)

Specific Areas of Concern about S. 2201

Mr. Chairman, we also have identified the following areas of serious concern in S. 2201. Amazon.com will focus its cooperative and constructive efforts on these issues, as well as on the online-offline parity point, in an effort to provide you and your Committee as much information as soon as possible. Our principal concerns are as follows:

Private Rights of Action (Section 203):

- As noted above, we fear giving overly aggressive litigants a new tool to extract rents from "good guy" companies with relatively deep pockets. It is clear from the FTC/PFF sweeps that the most popular and, thus, the most successful, websites already are providing outstanding privacy protections. Unfortunately, however, it will be these "good guys" that litigants attack, because these are the entities capable of paying big judgments. Indeed, under the current bill, it would be far more lucrative to bring a class action suit to catch a "good guy" on a technicality than catch a "bad guy" in an egregious act.
- A company could be hit with a judgment of $5,000 per user per violation (with up to a $100,000 kicker for repeated violations) with a showing of but minimal actual harm and showing no malfeasance. Because class actions are not precluded, there probably will be a class action alleged for every potential violation. And, if the alleged violation is a part of a company doing business, there will be gigantic cases.
- Allowing such private rights of action will cause the "good guys" to make their privacy notices much more legalistic – and much less readable to consumers – just so that they would fare better in a lawsuit. Unreadably long privacy statements and fine-print legalese would become the norm. A regulatory body such as the Federal Trade Commission, on the other hand, could balance the competing interests of legal precision and simplicity.
- In addition, the uniformity necessary to run nationwide websites would be destroyed by a host of litigants suing companies all across the country. A single authority, such as the FTC, could provide the nationwide approach that private litigation cannot.

State Actions (Section 204):

- In a highly unusual, if not entirely unprecedented, grant of power, this section would allow state attorneys general to bring class actions on behalf of all their residents, unfairly exposing online entities to politically motivated lawsuits.

Access and Deletion (Section 105):

- Several of the terms in this section, such as "reasonable access," "reasonable opportunity," and "suggest," are ambiguously defined and it is unclear how the ambiguity will be resolved. Is this a matter for the Courts or perhaps a broad FTC rulemaking?
- This section seems to require data deletion, which would dramatically hinder our efforts to limit fraud and thwart consumer identity theft. Indeed, this provision likely would end up making consumer identity theft easier, by making criminal activity much harder to trace. Further, just imagine asking a bank, or credit card company, or brick and mortar store, to simply "forget" a transaction conducted with them last month, or last year!
- Our information technology department tells us that the access/deletion requirements would require extraordinary costly technical measures. They also fear that, even if it would be possible to meet these requirements, our security and anti-fraud measures would be compromised.
- Finally, there are very narrow exceptions to law enforcement disclosure. One situation not addressed is where a website operator discovers fraud and wants federal help investigating it. Could we be liable if we report fraud to law enforcement or to the victim of the fraud? And what if the victim files a civil suit? Does the fraudster really have a right to contest that motion?

"Reasonable" Security (Section 106):

- Companies have every possible motivation, including tort law, to maintain effective security against hackers. There is no need for a new statute to require it.
- After a security breach, it may very be difficult to argue that "reasonable" precautions were taken. With little precedent for guidance, the fact of a breach would make any failed security precautions look unreasonable. In other words, without clarifying language, a security "reasonableness" standard likely would function as a strict liability standard. On the other hand, to the extent that security practices of other entities become well known, it also would be a concern if "reasonable" were defined as "what everybody else is doing." This interpretation could make it risky for companies to take innovative approaches to security.
- Any detailed, public investigation of whether a company took reasonable precautions might reveal too much to hackers about what a company does and does not do.

Information Collection (Section 101(a)):

- Even if S. 2201 were not modified to apply to offline entities, this provision could unfairly be read to impose requirements on online entities' use of offline information that is, and would remain, available to offline entities without restriction. Online entities should face no more restrictions on offline information than do offline entities.

Notice and Consent (Section 102):

- "Clear and conspicuous," "affirmative consent," and "robust" all are ambiguous terms, despite the definitions offered in Section 401, particularly with regard to the various technical means for delivering this information. For example, robust notice on a web-enabled telephone – with a very small display – might be very different from robust notice on a wide-screen monitor.
- We are concerned about the general prescriptions on "use" disclosures. How detailed must these disclosures be? If the requirement is for super-detailed specifications, then companies will have to anticipate too many small variations on the general theme of how information is used, instead of focusing on the most important general points. Importantly, if too much information is required, consumers will not be presented readable disclosures. Finally, as for "methods of using," we are concerned that this might require the revelation of potentially sensitive technical information not relevant to consumers, but very relevant and useful to hackers.
- For sensitive information, are "opt-in" (in the title) and "affirmative consent" (in the text) the same thing? There is considerable ambiguity in both of these terms. Would the "initial robust notice" requirement force website operators, every time they collect a little more PII, to go back and give robust notice? Yet if the visitor just returns, and the operator doesn't collect PII, then no robust notice is required. And, under the construct of this bill, every web page visit, which produces click-stream information, creates PII when it's combined with a user's identity. We fear that repetitive opt-out requirements would be burdensome and annoying to consumers.

Definitions (Section 401):

- This section, in addition to containing many ambiguities, incorrectly defines the term "cookie." Further, the definition of "robust notice" is not clear. What is "actual notice"? Is it subjective? Also, the definition itself contains a "use" ("to use or disclose that information for marketing or other purposes"). Does this mean you have to give Robust Notice, before the collection of PII, but Robust Notice is the same as actual notice that you intend to use for marketing or "other" purposes. Is a website's link to a privacy notice "robust" in this way? And what about "robust notice" on a wireless or other small screen device such as the remote terminal on the kitchen wall or the automobile dashboard?

We have identified these principal concerns with S. 2201, and plan to continue our analysis and dedicate our attention to providing the Committee information on each of these points.

Conclusion

In conclusion, Mr. Chairman, Amazon.com is pro-privacy in response to consumer demand and competition. We already provide our customers notice, choice (including opt-in choice where appropriate), access, and security. You have called for these same features in S. 2201 and, although we have many concerns with this bill, we appreciate that you recognize, as we do, the importance of consumer privacy.

Our foremost concern with S. 2201 is that it would apply only to some companies and only to one percent of consumer retail transactions. For the many reasons articulated in this testimony, Amazon.com respectfully requests that any privacy legislation approved by this Committee apply to all consumer transactions, not merely those conducted online.

In addition, Amazon.com has serious concerns with several specific provisions in the bill. Primary of these are the provisions for nearly unfettered class action litigation; access/deletion obligations that would jeopardize our security and anti-fraud efforts; and technically infeasible security requirements. We look forward to working with you and your Committee to address all of these issues.

Thank you again for inviting me to testify; I look forward to your questions.

* * * * * * * *