Statement of

IOANA RUSU
Regulatory Counsel
Consumers Union

Before the

U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Regarding

Privacy and Data Security: Protecting Consumers in the Modern World

June 29, 2011

Chairman Rockefeller, Ranking Member Hutchinson and esteemed Members of the Committee. Thank you for the opportunity to appear before you today to discuss privacy and data security issues. My name is Ioana Rusu, and I am Regulatory Counsel for Consumers Union, the non-profit publisher of *Consumer Reports*® magazine.

Privacy in a Rapidly Changing World

Few can deny just how much the world has changed over the past decade. We now research and shop for products without ever leaving our homes. Our phones have become mini-computers, allowing us to organize our finances, pay bills, and order services on the go, as well as to pinpoint our exact geographical location. Social networks and online blogs enable us to create virtual lives, to reconnect with long-lost friends, and even to organize against oppressive government regimes. By transmitting and accessing more information than ever before, we've created both a vibrant online community and an efficient and convenient Internet marketplace. These incredible tools have enriched and enhanced our lives.

At the same time, however, these same tools have planted some unnerving questions in our hearts. For example, will we continue to express ourselves freely on the Internet when we know that every click and keystroke is being recorded by unknown entities, to be used for unknown purposes? And once we've entrusted our personal data to a third party, can we be sure it will it be carefully safeguarded? It is time for us to answer these questions in a clear and straightforward manner. A privacy and data security policy composed of clear, predictable, and comprehensive rules will enhance consumer trust and encourage innovation.

The first step towards this goal is our recognition that privacy is still very much a relevant and important concept in our world today. Although we live in an age of extensive sharing, very few people would agree that every piece of information they transmit should be available to everyone, for any conceivable purpose. We share information because it facilitates transactions, gives us access to services we seek, and allows us to more easily communicate with others. But it is incorrect to assume that consumers don't care about how that information is used and disseminated. In fact, in a May 2011 *Consumer Reports*® poll, 82% of respondents were concerned that companies they did business with may be passing on their personal information to third parties without their permission. Such consumer distrust could represent a significant barrier to the adoption of new technologies, which in turn harms commerce and discourages innovation.

Legislative Solutions for Protecting Consumer Privacy

The Commercial Privacy Bill of Rights of 2011 introduced by Senators Kerry and McCain seeks to implement some reasonable standards that would give individuals more control over who gets access to their personal information and for what purpose.

The bill's framework is firmly rooted in a set of Fair Information Practice Principles (FIPPs) – "rules of the game" that spell out how covered entities should be collecting,

handling, and sharing consumer data. These principles include clear, concise, and timely notice about data collection practices; opt out requirements for certain uses of personal information; access and accuracy requirements; and the principle of "privacy by design," which requires entities to incorporate privacy protections directly into their day-to-day activities, as they develop new products and implement new technologies. Taken together, the FIPPs create a roadmap for the fair and responsible treatment of consumer data online.

We are pleased that the bill requires companies to offer consumers an opt out from unauthorized uses of their information, including the unauthorized transfer of information to third parties and the passive collection of information by third parties on first-party sites. Third-party sharing of information is extremely expansive in today's e-commerce, as tracking technologies allow advertisers to collect vast amounts of information about consumers and to aggregate them into personal profiles that are then used to target individuals much more effectively than ever before. While some consumers may not mind receiving advertising tailored to their interests, others prefer that their behaviors and preferences online remain private. The latter group should be able to choose not to have data shared with these unknown third parties.

The bill also recognizes that some types of information are more intimate and more easily used for harmful purposes than others. As a result, the bill creates a "sensitive information" category, which includes personally identifiable information (PII) that could result in physical or economic harm to an individual, or information about an individual's medical condition, medical records, or religious beliefs. If companies wish to collect, use, or share sensitive information, they must obtain the individual's affirmative opt in consent. We strongly agree with this provision. A young woman suffering from bulimia should never worry that when she joins an eating disorder support forum, her information will be passed along to companies who will market weight loss supplements to her at every step, constantly reminding her of her obsession with her weight. She also should never have to worry that information about her condition will be sold to her insurance company, who will then raise her rates. Such uses of sensitive information are unexpected and unfair, and should not be permitted without the consumer's informed consent.

In addition, we are pleased that the bill requires entities to engage in data minimization by not collecting more data than is needed, and by only retaining collected data for a limited amount of time. Consumers Union believes that the traditional notice-and-choice approach to privacy has not done enough to allay consumers' concerns. This approach has resulted in lengthy privacy policies, filled with legalese, that consumers must "agree to" in order to access a website or receive a service. As a result, Consumers Union supports the implementation of substantive privacy principles, such as data minimization and data retention limits, which do not rely solely on consumer participation to function. These principles require companies to carry out an honest assessment of their own data practices, and to collect and retain only information necessary to the operation of their business. It is also important to note that rich repositories of information within indefinite retention periods tend to be prime targets for hackers and can expose extensive amounts

of information in case of a data breach. Fewer privacy concerns will arise if only necessary data is collected and stored for a limited amount of time.

The bill grants enforcement power to both the Federal Trade Commission and state attorneys general (AGs) – a crucial provision that will increase the likelihood that bad actors are caught and punished. The enforcement provisions of the bill are crucial elements of this privacy framework, and emphasize the fact that any comprehensive privacy standards must be backed up by the force of law. The reason why industry self-regulation initiatives have largely failed to address this problem so far is that companies choose to voluntarily participate, and are held accountable insofar as they violate the stated terms in their own privacy policies. Under the proposed framework, all covered entities would be required to comply or risk enforcement action by either FTC or state AGs.

As discussed above, the Commercial Privacy Bill of Rights of 2011 lays out an important foundation for better privacy practices which Consumers Union supports. At the same time, we look forward to working towards strengthening the measure so that it provides consumers with even more transparency and control.

First of all, we support providing consumers with an opt-out not only for the unauthorized use of covered information, but also for its collection. Companies should not be permitted to amass vast quantities of information about individuals' behaviors and interests, without at least giving those individuals some notice and opportunity to opt out.

Secondly, we believe the bill could be strengthened by extending the definition of "sensitive information" to also include information directly tied to unique identifiers, not just to PII. As the FTC noted in its recent staff report, the distinctions between PII and non-PII are becoming increasingly irrelevant. A consumer's behavioral profile is not "anonymous" simply because it is not tied to his name or address; it is sufficient that it is tied to his particular device. Companies could use that information to treat consumers unfairly, even without access to their PII. For example, if a website does not know my name, but knows that, based on my browsing habits, I am a user with a taste for luxury goods, it could presumably show me different offers, at different prices, than it would for another user. This may result in economic harm to me.

In addition, re-identification methods today allow companies to aggregate many pieces of "anonymous" consumer information into profiles that can then be linked to actual persons. While the bill does include a provision prohibiting re-identification by third parties – a provision that we support – we believe this same prohibition should also apply to first parties who claim to collect only anonymous information from consumers. Such first parties should also be prohibited from re-identifying the consumers to whom the data applies. We are pleased to see heightened protections for sensitive information, but would like to see the definition of "sensitive information" expanded to address the ways in which online behavioral tracking is currently being carried out: though unique identifiers tied to individual devices.

Third, we wish to see more authority granted to the Federal Trade Commission to modify and update the definitions in the bill. As industry never fails to point out, this is a rapidly changing and emerging field, with new developments springing up almost on a daily basis. The FTC should have flexibility to address these new issues as they arise.

Also, the expansive language of the pre-emption provision could forestall any state laws that "relate to" covered entities' collection, use or disclosure of covered information. Although some pre-emption may be necessary to ensure uniformity in privacy practices across state lines, states should be given leeway to come up with innovative ways of protecting consumers while also supporting technological innovation. We would recommend that the pre-emption provision in the bill, at most, cover any state laws that "expressly" require covered entities to implement requirements with respect to the collection, use or disclosure of covered information. Although still pre-emptive, this language would be more narrowly tailored and may still allow state action in areas not covered by the bill.

While we believe the Commercial Privacy Bill of Rights Act will provide consumers with meaningful choice over how their personal information is collected, transferred, and used, our organization has long supported giving consumers the possibility to opt out of online tracking. That is why Consumers Union also strongly supports Chairman Rockefeller's Do-Not-Track Online Act of 2011 as an important and necessary component of consumer online privacy policy.

The bill would lend the force of law to industry's self-regulatory efforts by requiring that when a consumer using a Do-Not-Track (DNT) tool expresses a preference to not be tracked online, companies must respect that choice. The Federal Trade Commission would have authority to establish standards for the implementation of such DNT tools, taking into consideration the appropriate scope of such mechanisms, technical feasibility, and cost. In addition, the bill gives both FTC and state AGs authority to enforce the statute and ensuing regulations, and to seek civil penalties and damages from bad actors.

Public support for a DNT option is particularly high at the moment. According to the same *Consumer Reports*® poll mentioned above, 81% of respondents agreed that they should be able to permanently opt out of Internet tracking. In addition, the FTC endorsed this idea in its most recent report, and we are pleased that some industry actors have already developed and incorporated DNT tools directly into browsers. Despite the emergence of such consumer-friendly tools, however, marketers currently can and do ignore consumers' DNT choices. This is precisely why Chairman Rockefeller's bill is a much-needed component in today's privacy discussion.

Consumers Union believes that the Do-Not-Track Online Act and the Commercial Privacy Bill of Rights Act, taken together, would give consumers strong privacy protections and meaningful choice in the way their information is collected and used online.

Protecting Consumers' Data from Breaches

Protecting consumer privacy extends beyond giving consumers control over how their information is used and shared. Any comprehensive, standardized privacy policy must also address how collected information is stored and safeguarded, and what protections each consumer should enjoy in the unfortunate event of a data breach.

Last month, Sony's PlayStation network faced numerous attacks that resulted in the theft of over 100 million personal records, according to Privacy Rights Clearinghouse. And in April, the email data base of marketing company Epsilon was hacked and an unknown number of consumer names and email addresses were stolen. Because Epsilon sends out more than 40 billion marketing emails annually, the potential breadth of this breach could render it the biggest of its kind in U.S. history.

The ubiquity of security breach incidents today renders the Data Security and Breach Notification Act of 2011, introduced by Senator Pryor and Chairman Rockefeller, particularly timely and relevant. Consumers Union believes this bill will protect consumers by mandating strong data security practices for all covered entities, as well as notification in case of breach. The bill will also hopefully incentivize covered entities to engage in data minimization practices on the front end, before a breach occurs.

The Data Security and Breach Notification Act first directs the Federal Trade Commission to promulgate regulations that would lay out how covered entities must maintain and protect personal information. These regulations would encourage companies to assess vulnerabilities and anticipate reasonably foreseeable attacks, in order to address those issues and prevent a breach.

If a security breach nevertheless does occur, the bill would require covered entities to provide timely notice of security breach to affected consumers and at least two years of free credit reports or credit monitoring. Consumers Union supports these provisions. If consumers do not know their data has been compromised, they cannot take steps to protect themselves. We also do not believe that consumers should have to bear the costs when personal information that they entrusted to a company is lost.

Although Consumers Union would prefer that consumers receive notification whenever their personal information is compromised, if there is to be a standard for risk, then Consumers Union would prefer the approach taken by this bill, where the risk is considered as an exemption rather than as an affirmative trigger. Under an "exemption" approach, a company with a security breach has to qualify for the exemption by showing that there is no reasonable risk of harm. Insufficient information about the level of risk does not eliminate the obligation to tell consumers about the breach. We would like to note, however, that the strongest state notice of breach laws do not require a finding of risk before mandating consumer notification.

We are particularly pleased that the bill focuses on the activities of information brokers, defined as commercial entities whose business is to collect, assemble, or maintain

personal information concerning individuals with the purpose of selling such information to unaffiliated third parties. We strongly support the provisions instructing information brokers to maximize the accuracy and accessibility of their records, as well as to provide consumers with a process to dispute information. In addition, the provisions requiring information brokers to submit their security policies to the FTC, as well to undergo potential FTC post-breach audits, will foster accountability and enforcement of this bill.

This bill arms state officials with strong enforcement tools to ensure compliance with the law. Consumers Union agrees that state attorneys general and other officials or agencies of the State should have the authority to bring enforcement actions against any entity that engages in conduct violating the bill. State attorneys general have been at the forefront of notice of data breach issues and have played an invaluable role in addressing identity theft and data breach. Consumers' personal information will be better protected because of these enforcement tools.

Consumers Union believes that the Data Security and Breach Notification Act would encourage companies to act proactively to prevent against data breaches and to quickly address any breaches that may occur. At the same time, we look forward to working towards strengthening a couple of the provisions in the bill.

First, we are concerned that companies conducting risk assessments may not always evaluate the facts in a fair and truthful manner, in order to avoid costly notice requirements. As a result, we would suggest that companies be required to either submit the results of their self-assessments to the FTC and state AGs, or, alternatively, to maintain a copy of those results for a defined period of time and make them available to the authorities upon request. A faulty self-assessment that clearly ignores potential risks should be treated as a violation of the statute.

We also hope that the 60 day window for providing notification will be narrowed. The sooner consumers are made aware of a breach, the quicker they can take remedial action. In addition, we are concerned that some credit monitoring companies are automatically billing consumers after the mandatory two free years of monitoring have ended. Consumers should affirmatively consent to any additional monitoring beyond the two years provided by the company.

Closing

In closing, we urge you to continue the conversation on the important topics of data privacy and security. While these three bills put in place important protections for consumer data, both online and offline, we encourage you to also consider adding additional protections for kids and adolescents. Teens between the ages of 13 and 17, in particular, make up a large portion of Internet users today. At the same time, they are more vulnerable to inappropriate uses of their personal information online. We hope you will develop some heightened standards to address the privacy of these sensitive users.

Consumers Union looks forward to working with you as these three bills move forward. Consumers are looking to you to enact standardized, mandatory and enforceable rules of the road that companies must follow when handling user data. We firmly believe that implementing these baseline principles will enhance consumer trust in the marketplace and encourage businesses to grow and innovate with confidence. Thank you for your time, and I would be happy to answer any questions you may have.