ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

Legislative Hearing on "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act"

Before the

House Committee and Energy and Commerce
Subcommittee on Commerce, Trade,
and Consumer Protection

May 5, 2009
2123 Rayburn House Office Building
Washington, DC

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act. My name is Marc Rotenberg and I am the Executive Director of the Electronic Privacy Information Center (EPIC) and Adjunct Professor at Georgetown University Law Center.

EPIC is a non-partisan research organization, focused on emerging privacy and civil liberties issues. We have worked for many years to draw attention to new privacy and security risks, such as data breaches, pretexting, and the commercial sale of personal data, as well as to make recommendations for both technical solutions and legislation that can help mitigate these risks. While there is no single solution, either in technology or law, that can prevent security breaches, there are a number of steps that can be taken to reduce the risk.

I have several specific suggestions for the legislation that is currently before the Committee today. But I would also like to make a preliminary comment about the relationship between legislation and the efforts that are underway to safeguard security and privacy. I think it would be a mistake to assign to the FTC, or to any agency, the central responsibility for information security. This is an area where technology is changing rapidly, and both new problems and new solutions arise almost daily. The federal rulemaking process is ill suited to respond in this environment, and there is a real danger that well intended regulation may in some circumstances frustrate more effective solutions either because the process is too cumbersome, too secretive, or simply unresponsive.

At the same time, there is a need to make clear fundamental obligations on the companies and organizations that collect and use personal data on consumers and Internet users. It is simply too easy for firms today to capture the benefits of data collection and ignore the risks. In the absence of security obligations and breach notification requirements, it is too easy for firms to continue bad practices. In fact, not only are there few incentives to change practices, without legislation, companies are likely to conceal rather than to correct problems.

This is why legislation is appropriate – to ensure that companies carry the responsibility for their data practices. But it is critical to ensure the legislation is effective, flexible, and responds to the rapidly changing environment. Congress should be wary of setting security standards through a rulemaking process. The better approach, in my opinion, is to focus on the broad obligations, to make clear the incentives, and to encourage the development of the best solutions. This does not diminish in any respect the need for robust security standards – it simply leaves the law to do what it does best: make clear the rights and responsibilities of the

various participants in the information exchange – and leaves to the technical experts the obligation to develop the best solutions.

The other key point to make at the outset is that almost all of the states have responded over the last few years to develop robust security breach notification legislation. Many of these laws can be traced back to the California notification law that was famously triggered in a matter that EPIC brought attention to involving the sale of data on American citizens to a criminal ring engaged in identity theft. That notification and the investigation that followed led to dramatic changes in the information broker practices in the United States. While there is clearly a lot more that needs to be done to safeguard personal data, you should not underestimate the enormous value of these breach notification statutes as well as the unintended problems that could result if the federal law preempts the more responsive state law. For reasons I will discuss in more detail below, I would recommend that you not adopt legislation that would preempt the ability of the states to develop more effective means to respond to these new problems

H.R. 2221, the Data Accountability and Trust Act

Mr. Chairman, although I have not seen the text of H.R. 2221, I understand that this bill is identical to H.R. 958, The Data Accountability and Trust Act that was introduced in the 110th Congress. My comments therefore are directed to the text of that bill. The main legislative development that has occurred since the introduction of H.R. 948 is the adoption of American Recovery and Reinvestment Act of 2009 (ARRA), which includes new provision for medical record privacy and new authorities for the FTC, including a rulemaking for security breach notification. It may be worth looking at those provisions to determine whether the current bill should be revised. There are also significant developments in technology, such as the rapid rise of social network services and the increasing use of text messages, which may be worth considering as the Committee reviews this legislation. Significantly, the new communications tools may also provide new opportunities for breach notification, and new analytic tools could provide better understanding of security challenges if the FTC data is made available to the public.

As currently drafted, H.R. 2221 attempts to address growing concerns about privacy protection and security breaches by granting the FTC new authority to regulate companies that collect and use personal data. The bill attempts to crack down on the information broker industry, limit pretexting, and sets out new notice obligations in the event of a security breach. Overall, this is an important and timely legislation that seeks to address several of the key concerns of American consumers and internet users – the failure to ensure that personal information is adequately protected, the unregulated market for personal data, and the inability of users to know when their data has been improperly disclosed.

EPIC would like to express its support for the legislation and the sponsors of this measure. We appreciate the willingness of the Committee to examine this issue and to develop a legislative response. My comments on the bill are intended to show areas where it may be possible to strengthen the legislation.

Method of Notification

The bill currently proposes the use of either written notification or email notification when an obligation to provide notification arises. Sect. 3(d)(1)(A). I would suggest that you include an additional obligation to provide a text message where possible. A text message would not be an effective substitute for written notification or email, because it is essentially ephemeral. But is a very effective technique for notification and it could help make people aware that they should look for a notice that might arrive in the mail or show up in the email box.

In a similar spirit, where the bill speaks of providing notification by means of a web site, it may be appropriate to add "or social network presence." Many organizations today are interacting with users though popular social network services such as Facebook. In many configurations, the data remains with Facebook, so there is no direct data collection by third parties. But in other circumstances, for application developers and advertisers for example, third party companies obtain information from users through Facebook. If security breaches arise in these circumstances, notification by means of the social network service may be the most effective way to reach the target population.

Public Record Defense

There is an odd provision, Section 4(c) of the Act, that would create an affirmative defense where all of the personal information disclosed as a result of a security breach in violation of the Act is "public record information" available from federal, state, or local government systems and was acquired by the company that suffered the breach for such purposes. The theory underlying this provision, I imagine, is that there could be no additional harm to the individual of the breach of this information if it is already available to the public. But this is the wrong way to understand the problem and the affirmative defense will undercut the purpose of the Act.

If an organization suffers a security breach of confidential information or of "public information" it has a problem that needs to be corrected. If no action is taken to correct the problem, it is quite likely the breach will occur again. That is why the security obligation should apply even when there is no immediate harm to the individual: The problem remains. Also, I would not assume the fact that personal

information may be found through public data sources that the information disclosed in a data breach is equivalent. It is quite likely, particularly in the information broker industry, that the "public" information contained in a particular data record is far more detailed than any record that would be available in a singe government record system.

Treatment of Personally Identifiable Information

One of the key provision of the Act is the definition of "Personal Information" set out in sect. 5(7). This definition is critical because, as with most privacy bills, this definition will determine when the obligations of the Act should be applied and when they can be pretty much ignored.

As currently drafted, the bill sets out a narrow definition for Personal Information, as compared with other privacy statutes. For example, the bill seems to suggest that a social security number would not be personally identifiable if it is possessed without the associated person's name. The bill also ignores other popular identifiers, such as a user ID for Facebook, which points as readily to a unique individual as would a driver's license or a social security number.

The definition is also narrow in light of the FTC report released earlier this year on Internet advertising that noted that there are many ways to track Internet users, including the use of "IP address" that can uniquely identify a user's computer, much as phone number will uniquely identify a cell phone. In many cases, this is also a form of personal information that should be subject to the bill's requirements.

The bill does provide for a rulemaking that could modify the definition of "personal information" but even this rulemaking seems unnecessarily narrow as it is limited to changes that are "necessary to accommodate changes in technology or practices."

I would suggest a construction that would define Personal Information as information that "identifies or could identify a particular person," followed by the examples cited in the bill as illustrations, with the qualifying phrase "including, but not limited to." This approach is technology neutral, less dependent on the rulemaking process, and more likely to adapt over time.

Preemption

Section 6 addresses preemption and the circumstances under which the federal law would overwrite possibly more effective state information security legislation. As currently drafted, H.R. 2221 preempts state laws that either have similar security obligations as well as state laws that provide for security breach

notification. The Act does leave in place state trespass, contract and tort law, as well as claims involving fraud.

My own view is that it would be a mistake to adopt a preemption provision of this type. Businesses understandably will prefer a single national standard. That is the argument for preemption. However privacy laws have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish. This approach to consumer protection is based upon our federalism form of government that allows the states to experiment with new legislative approaches to emerging issues. President Obama made this point very directly in his recent remarks to the National Governors Association when he described the states as the "laboratories of democracy." This was a reference to a famous opinion by Justice Brandeis about the specific authority of the states to legislate in response to new problems. This view reflects the belief that there should be experimentation in regulatory approaches.

There is an additional reason that I believe weighs against preemption in the information security field: these problems are rapidly changing and the states need the ability to respond as new challenges emerge. California, which is widely credited for adopting the first breach notification statute, also found itself needing to update its own law to address the specific problems of medical information breach. It is very likely that the states will face new challenges in this field. Placing all of the authority to respond here in Washington in one agency would be, as some in the security field are likely to say, a "critical failure point."

While there is a clear need to strengthen security safeguards, I remain concerned about the ability of the FTC to develop a regulatory framework for information security in the United States, particularly when it is the only agency with authority to do so.

Private Right of Action

As the bill is currently drafted, a person whose personal data is improperly leaked by a company in possession of the data is signed up for two years for a credit card notification service. While this remedy may provide a nice revenue stream for those in the credit card monitoring service, it may not be very satisfying for consumers. Where a security breach has led to cases of identity theft, which was clearly the case in the Choicepoint incident, consumers are entitled to a real remedy.

I would strongly urge the Committee to add a private right of action to the bill with a stipulated damage award, as is found in many other privacy laws. Not only would this provide the opportunity for individuals who have been harmed by security breaches to have their day in court, it would also provide a necessary backstop to the current enforcement scheme which relies almost entirely on the

Federal Trade Commission, acting on its own discretion and without any form of judicial review, to enforce private rights.

If the law is passed without a private right of action, and the Commission fails to act, is reluctant to act, or simply doesn't understand a problem where it should act, individuals who are harmed by a security breach will be in a worse position then they6 were before the law was adopted because any rights that were previously available under state law, less those explicitly carved out, will no longer be available.

Safe Harbor

There are two different types of safe harbor provisions in the Act. Section 3(f)(1) essentially suspends the law if, following a breach of security, "such person determines that "there is no *reasonable risk* of identity theft, fraud, or other unlawful conduct." (Emphasis added). In other circumstances, a reasonableness standard might be appropriate. The problem here is that the company will decide itself, having suffered the breach, *whether there is reasonable risk of harm to others* and there will be no effective way to review this decision if the company guesses wrong. That is an approach that will invite greater secrecy and less accountability. The simple solution may be to remove the word "reasonable." If a company determines that there is "no risk of identity theft, fraud, or other unlawful conduct" then it would be reasonable to suspend the notification requirement.

The presumption in Section 3(f)(2) of the Act creates an important incentive to use strong security safeguards, including encryption and data minimization techniques, but also has the effect of preventing notification when security breaches occur. It is unclear, for example, how this presumption will be challenged if there is no notification to the party or to the FTC when a breach occurs. A partial solution would be to require the (a)(2) notification to the FTC with an explicit designation that the specified security standards were in place. This would fulfill several goals: provide some form of notification, create the appropriate presumption for the use of good security techniques, and enable the FTC to further investigate if necessary.

Transparency

On a related point, there is an unnecessary amount of secrecy surrounding the obligation to notify the Commission in Section 3(a)(2). As the bill is drafted, the companies will notify the Commission but the Commission will only make the information available to the public when it "would be in the public interest or for the protection of consumers." This leaves too much discretion with the agency, and will also make it difficult to evaluate long terms trends and key problems by preventing access to routine reporting about security breaches.

The better approach is to simply make information about security breaches available to the pubic. Section (a)(1) will still have the intended effect of ensuring the target population is affirmatively notified. Section (a)(2) will now ensure that the information about security breaches is generally available to the public.

Making data publicly accessible will have the additional benefit of providing information in ways that are compatible with the President's goals of making government information more accessible and useful to the public. It is conceivable, for example, that better tracking of security breach incidents, combined with other data sources, will make it easier for security researchers to detect problems and find solutions. "Mash-ups" could help identify related problems. Further, longitudinal data is always useful to determine long-term trends, such as the FTC's own findings about the growing problem of identity theft. But none of this will be possible if the data provided to the FTC in the event of a security breach is not made available to the public.

H.R. 1319, The Informed P2P User Act

Mr. Chairman, I would like to make a few remarks about H.R 1319, the Informed P2P User Act. The purpose of the bill is to make people aware, who might not otherwise be aware, of some of the risks of P2P file sharing. The bill as drafted would require a person who seeks to make another computer available for file sharing to inform that person and also to make known, before activation of the file sharing function, the files that will be made available for file sharing, The Act further prevents a person from trying to prevent the owner of the target computer from taking reasonable efforts to disable file sharing functionality.

P2P networks also have certain functionalities that are not found in the traditional client-server architecture of the Internet. For example, P2P networks make it possible to make more efficient use of bandwidth, as well as providing some protection against failure, as there is no single point of failure that would exist in a hierarchical network or one that relies on a central directory.

At the same time, recent vulnerabilities in P2P networks have raised understandable concerns about the reliability of some of the applications. The vulnerability of a poorly installed network is substantial as a user essentially leaves the files on his or her computer vulnerable to access by anyone on the file-sharing network. This matter was brought to the attention of the Committee in the recent exchange concerning Lime Wire.

In the consideration of this bill, it is important to understand that P2P programs are used for a wide variety of function from the sharing of music to Internet-based telephony as well as scientific research. Even the military makes use of P2P networks. The technique is also important in countries where Internet censorship is a threat,

In the most generic sense, a P2P network is a technical description, much like saying a telephone network or the Internet. It is no intrinsic application, other than architecture that allows nodes to exchange information equally with other nodes in the network. Some Internet scholars have observed that this architecture reflects the collaboration among individuals that has helped spur the growth of the Internet. Professor Yochai Benkler refers to this as "Commons Based Peer Production."

No doubt part of the bill aims to discourage the use of file sharing techniques that may infringe copyright as well as making users vulnerable to certain types of inadvertent file sharing. But there is some risk that the bill would also discourage the use of file sharing techniques that do not raise such concerns. More generally, it appears to be posting a warning sign on a very wide variety of applications that most likely have little to do with the sponsor's concern.

I do think that if legislation is adopted of this type for file sharing in P2P networks, it may also be appropriate to adopt legislation for the use of persistent cookies by advertising networks. These techniques also raise privacy concerns for individual users and at present there is no notice provision comparable to that proposed in H.R. 1319 for these particular tracking techniques. Moreover, the decision to place a persistent cookie on another user's computer without that user understanding the consequences or making an informed decision to accept the cookie raises several troubling privacy concerns, including the possibility of tracking the user's online activity. While there are many circumstances under which persistent cookies enable useful functionality, users should be given notice and full opportunity to consent, or to disable the tracking features if they so choose.

We would be pleased to work with the committee both to ensure that the key concern in the P2P file notification is addressed as well as to expand the bill's coverage to address the related problem of persistent cookies.

Conclusion

Data breaches remain one of the greatest concerns for Internet users in the United States. Many companies have poor security practices and collect far more information than they need or can safeguard. But since there are few consequences

for poor security practices, they can obtain all the value from the user data and leave it to others to deal with the consequences. This clearly needs to change.

Companies need to know that they will be expected to protect the data they collect and that, when they fail to do so, there will be consequences. Legislation for information security and breach notification is needed, but it should not preempt stronger state measures and it should not rely solely on FTC rulemaking authority. My comments today suggest several steps that might ensure that the legislation is effective, takes advantage of new Internet-based services, and has the flexibility to evolve as new challenges arise.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.