Testimony of David Sohn
Senior Policy Counsel
Center for Democracy & Technology

before the

Subcommittee on Commerce, Trade, and Consumer Protection,
U.S. House of Representatives Committee on Energy and Commerce

Legislative Hearing on

H.R. 2221, the Data Accountability and Trust Act
and
H.R. 1319, the Informed P2P User Act

May 5, 2009

On behalf of the Center for Democracy and Technology, thank you for the opportunity to participate in this hearing on the Data Accountability and Trust Act and the Informed P2P User Act.

CDT is a nonprofit, public interest organization dedicated to promoting privacy, civil liberties, and democratic values on the open and decentralized Internet. CDT has been a leader in the policy debates over privacy issues raised by the Internet and other new technologies, from spyware to data mining to electronic surveillance. In particular, CDT has argued that Congress should take a more comprehensive approach to privacy in order to promote trust and consumer confidence in the digital environment.

CDT applauds the Subcommittee for focusing on the privacy-related legislation that is the subject of this hearing. This testimony will start with some observations about privacy challenges in the modern technological environment and the need for general privacy legislation. It will then offer CDT's analyses of the specific provisions of the Data Accountability and Trust Act and the Informed P2P User Act.

Modern Privacy Challenges and the Need for General Privacy Legislation

The bills that are the subject of today's hearing both address risks that consumers' personal data could be improperly disclosed. Each imposes responsibilities on certain companies for mitigating some of those risks. In addition, each contains provisions aimed at empowering consumers – in one case by ensuring consumers' ability to see and potentially correct their data broker files, and in the other by requiring clear disclosure about file sharing software.

The common background to these bills is that technology has created powerful new ways to gather, store, sort, analyze, locate, correlate, and disseminate data. This has enabled increasingly intensive use of personal data, which can deliver significant benefits. For example, businesses obtain and share personal information in order to facilitate valuable economic transactions and provide more customized services. Large databases of personal information are used to help detect and prevent fraud. The government uses personal information to determine eligibility for government benefits, for tax collection, and to support law enforcement and anti-terrorism efforts.

But the growing use of personal data raises a host of privacy challenges as well. Most consumers have only a limited understanding of the multiple ways that their data is used and shared in today's data economy. Since the widely publicized security breach at ChoicePoint in 2005, there has been a nearly continuous stream of announcements of data security breaches at companies, government agencies, and universities. Consumers are concerned that they lack control over their personal information, and identity theft has become all too frequent.

Despite the unprecedented challenges to privacy in the modern environment, there is still no comprehensive law that spells out consumers' privacy rights in the commercial marketplace. Instead, a confusing patchwork of distinct standards has developed over the years, with highly uneven results and many gaps in coverage.

CDT commends the Subcommittee for taking a careful look at the specific bills that are the focus of today's hearing. We also believe, however, that it is important to recognize that the bills address individual corners of a broader puzzle. Having sound practices to protect against and respond to data breaches, as the Data Accountability and Trust Act would require, is only one aspect of the custodial obligations that should apply to those who collect, use, and store personally identifiable information. Similarly, peer-to-peer file sharing software is only one avenue by which consumers may share files and perhaps inadvertently disclose personal information.

CDT would urge this Subcommittee to give high priority to developing a single, consistent regime of baseline privacy standards. Such legislation would be based on the "Fair Information Practices," a set of principles that date back several decades and have been widely acknowledged as the cornerstone for privacy protection. For consumers, baseline privacy legislation would seek to ensure greater control over how personal data is shared and used, and to provide redress for consequences that result from mistaken or inappropriate use or disclosure of that data. For entities collecting, using, or sharing consumers' personal data, legislation would establish accountability for being a responsible custodian of the data.

CDT has testified previously on the need for baseline privacy legislation and would welcome the opportunity to work with the Subcommittee on such a bill.

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

The Data Accountability and Trust Act features three principal elements. It would create a nationwide data breach notification standard; require entities that electronically store personal information to implement security safeguards, similar to the safeguards currently required for financial data under FTC rules implementing the Gramm-Leach-

Bliley Act (GLB); and require information brokers to submit to security audits in the event of a data breach and, importantly, to allow consumers to review what is in their individual data files.

CDT supports the concept of a nationwide data breach notification standard, so long as that standard is at least as effective as the laws already in place at the state level. All but a few states have enacted data breach notification laws, so as a practical matter companies today do notify affected individuals in the event of a data breach. If a federal law were to preempt state laws and replace them with a weak notification regime, the result would be a significant step backwards for consumers and data security. Moreover, the Subcommittee should recognize that, from a consumer perspective, even a good federal breach notification requirement does not by itself offer much tangible progress over the status quo, since notification is already effectively the law of the land. To be of real benefit to consumers, data security legislation must include some additional protections.

The breach notification provisions in the Data Accountability and Trust Act could be improved, as discussed below, but are much better than some that have been proposed in other federal legislation in the past. The provisions requiring entities with personal data to have data security policies and procedures in place would be helpful and CDT supports them. CDT also supports the idea of requiring information brokers to allow individuals to access their files. While CDT would prefer to address access requirements in general privacy legislation, the ability of consumers to access their files and point out errors would be an important safeguard. The bill's specific language on access may need some modification to ensure its effectiveness, but these provisions could turn out to be the most significant gain for consumers in the bill.

In short, CDT supports the principal elements of the Data Accountability and Trust Act. We hope that the bill can continue to be improved and that the Subcommittee will resist suggestions that would weaken it. CDT's detailed comments and suggestions for improvements with respect to the bills specific provisions are as follows.

Breach notification trigger

The bill's trigger for breach notification, set forth in Section 3(a) and 3(f), requires notification to affected individuals and the FTC in the event of a security breach involving personal data unless it can be determined that there is "no reasonable risk of identity theft, fraud, or other unlawful conduct." CDT supports this formulation, because if a particular security breach truly poses no significant risk to the individuals whose data is involved, it should not be necessary to notify them. Indeed, such over-notification could be counterproductive.

Crucially, the bill's notification trigger permits notification to be avoided only when there is an affirmative determination that no serious risk exists. This creates strong incentives for a company suffering a breach to get to the bottom of what happened – because if it can determine there is no real risk, it will not have to notify its customers. A trigger that required notification only in the event of an affirmative finding of risk would create the opposite incentive – a company might not want to investigate too closely, because finding evidence of risk would trigger the obligation to notify. The current bill's "notify unless" formulation is the right one and should not be changed.

In the absence of any outside scrutiny of risk determinations, however, a company could have an incentive to err consistently on the side of finding little or no risk, in order to avoid the cost or embarrassment associated with notifying customers. Even if the affected individuals were eventually to become victims of identity theft, it would be difficult ever to trace those crimes back to the specific breach, since nobody other than the company and the identity thieves would be aware that the breach even occurred. In short, with nobody in a position to question dubious risk assessments, there could be a temptation to under-notify.

CDT believes this problem could be greatly mitigated by requiring a company, when it determines a breach poses insufficient risk to warrant notification, to notify the FTC or other appropriate regulator and provide some explanation as to why the company believes there is no significant risk. No formal process for FTC review or approval of a company's determination would necessarily be required. Simply knowing that a brief explanation would need to be filed with the FTC, and that the FTC might respond if it spotted a pattern of behavior or otherwise became suspicious, may be all it would take to ensure that companies remain diligent in their risk determinations and weigh the inevitable "judgment calls" in an even-handed manner.

CDT therefore recommends modifying the notification trigger so that breaches judged to be non-risky still require a submission of a brief written explanation to a regulatory body such as the FTC.

Requirement for security policies and procedures

Because notice only kicks in after a breach has occurred, CDT supports the provisions of Section 2(a) requiring entities that electronically store personal information to implement security safeguards similar to those contained in FTC rules under the Gramm-Leach-Bliley Act (GLB). CDT believes, however, that the provisions of Section 2(a) should not be limited to "personal information" as that term in defined in the bill.

The bill's current definition of "personal information" is quite narrow, probably because it was drafted with breach notification in mind. For purposes of breach notification, it makes sense to use a relatively narrow definition, to avoid over-notification. But the security practices and procedures required under Section 2(a) should apply broadly to whatever information a company holds about individuals. Making security policies apply to a broader range of personal information is consistent with the FTC's implementation of the security safeguards requirements in GLB: The FTC requires safeguards for essentially "any record containing nonpublic personal information . . . about a customer. (See 16 CFR 314.2 and 313(n)-(o)).

Of course, where data is relatively non-sensitive, companies should not be required to implement excessive security processes; security safeguards should be appropriate to the data's sensitivity. The FTC's GLB rules say this explicitly, and CDT would recommend adding data sensitivity to the list of factors for consideration enumerated under Section 2(a)(1) of the bill.

In addition, CDT would suggest modifying Section 2(a) to include a de minimis exception for persons that own or possess data in connection with purely personal, family, or noncommercial activities. Arguably, if an individual uses his or her computer for online shopping and also keeps personal data on it concerning, say, his or her elderly parents, the person could qualify as a person engaged in interstate commerce who

possesses personal data, and thus would be covered under this part of the bill. Given the small quantity of data such a person has, however, it would make little sense to require a formal written security plan that would satisfy the requirements of Section 2(a)(2).

Consumer access to information broker data

When information brokers collect, maintain, and sell personal data to third parties, enabling individual consumers to access their personal data files and point out possible errors can provide an important safeguard against inaccuracy and misuse. For example, if an innocent person finds his or her transactions are wrongly getting flagged as posing fraud risks, he or she could try to investigate and challenge the mistaken data that is causing the problem. An access and correction regime is well established under the Fair Credit Reporting Act (FCRA). CDT strongly supports the effort in Section 2(c)(3) of the Data Accountability and Trust Act to establish similar consumer access rights with respect to companies that aggregate and sell personal data.

Certain details of the current bill language, however, could undermine the provision's effectiveness. First, as discussed above with respect to Section 2(a), the scope of Section 2(c) is sharply limited by its reliance on the term "personal information." Given the bill's narrow definition of that term, the access requirements would apply only where the information broker has such details as a Social Security Number or a financial account number plus password. This narrow conception of personal information may be appropriate for breach notification purposes, but consumer access should not be so limited.

Where access rights apply, Section 2(a) does extend them beyond "personal information" to "any other information . . . that specifically identifies such individual." But the meaning of this phrase is unclear. Taken literally, the language could be read to cover only information that, by itself, would enable somebody to identify the individual. Lots of information that would be important for access purposes would not fall into that category. For example, suppose my information broker file says (wrongly) that I was convicted of a misdemeanor in 2002. This information alone would not allow anyone to identify me – but it is precisely the type of information to which consumer access is important. CDT believes the right of access should extend generally to information that is linked specifically to an identified individual and that the information broker makes available to third parties in the ordinary course of business.

CDT also notes that Section 2(c)(3)(B)(i) and (ii) refer to personal information that the information broker "maintains." Some companies compile information from various databases upon request, however, so it could be argued that they do not "maintain" a full set of information about an individual. The policy behind Section 2(c)(3), however, should be that a consumer can demand to see the data an information broker would provide in the ordinary course of business to a third party who asked for data about that consumer. One way to clarify this would be to track the language from Section 3(c)(A), which uses "collects, assembles, or maintains" instead of just "maintains."

Enforcement provisions

CDT generally supports the bill's enforcement regime. In particular, the bill wisely allows for enforcement by state Attorneys General as well as the FTC.

CDT would caution against, however, the affirmative defense contained in section 4(c) for violations involving data that is available from public records sources. There is a great deal of information that is practically obscure (i.e., publicly available in theory but difficult to access in practice) – because, for example, it exists only in dusty paper files in the basement of a small county courthouse. When companies gather this data and compile it in convenient electronic form, they effectively transform scattered bits of difficult-to-access information into highly usable, searchable, large-scale databases. If those databases later are subject to security breaches, individuals are put at risk – much greater risk than if the information had remained in scattered public records. Therefore, CDT believes that companies compiling personal data from public records should have some responsibilities to be good stewards of that data, and to notify individuals in the event of a security breach. There mere fact that an identity thief in theory could have obtained a person's data from another source would be of little comfort to a victim in a scenario where the thief took advantage of conveniently compiled electronic data and the holder of that data failed to provide notice of the breach.

Preemption

Given the large number of state data breach notification laws, preemption is a serious matter. Nonetheless, CDT believes that a federal data breach notification regime should preempt state breach notification requirements, so long as the federal regime is sufficiently robust. Having multiple and inconsistent rules on when and how to notify would be confusing and burdensome. CDT therefore believes the preemption set forth in Section 6(a)(2) is appropriate.

CDT has reservations, however, about preempting state data security laws covering topics other than notification, as Section 6(a)(1) would do. The information security provisions of the Gramm-Leach-Bliley Act (GLB) preempted inconsistent state laws, but otherwise allowed for state-level experimentation on the difficult question of how to ensure sufficient attention and precautions with respect to data security. CDT would recommend following the model set forth in Section 507 of GLB. Failing that, Congress at a minimum should be sure to preserve the language in 6(a)(1) limiting preemption to provisions that are "similar to any of those required under section 2." This language should preserve a state's ability to come up with an idea that is truly a fresh approach. California's breach notification law, the first in the nation, was a classic example of this. Had GLB broadly preempted state data security laws, it would not have been possible. Preemption should leave room for experimentation at the state level, because data security is likely to be an ongoing problem and nobody should pretend to have all the answers today.

If the bill moves forward with a higher level of preemption than GLB, Congress should keep in mind that the price for strong preemption must be strong substantive protections. If the bill were to be weakened as it moves through the legislative process, preemption would need to be reduced as well.

The Informed P2P User Act, H.R. 1319

Peer-to-peer (P2P) file sharing software is fundamentally a consumer-friendly and empowering technology. Millions of people use it today to share text, software, image, audio, and video files stored on their computers. It has opened new ways for people to

communicate with minimal central coordination and to spread storage and bandwidth costs across a broad user base. It has been a major driver of innovation in the software industry. Unfortunately, it also frequently is used to engage in copyright infringement. Of greatest direct relevance to H.R. 1319, file sharing software can raise privacy concerns, because there is evidence that some users of file sharing software have inadvertently shared sensitive documents like tax returns or electronic check registers.

CDT strongly agrees with the authors of H.R. 1319 that file sharing software should clearly disclose to users whether and how files will be made available for sharing with third parties. Inadvertent sharing of information like financial records, personal files, or correspondence is a serious matter.

It is difficult to measure how common it is today for consumers to share files accidentally. There is reason to believe some progress has been made; in the years since CDT testified on this issue in 2003, the Federal Trade Commission has engaged with major P2P companies to improve their disclosures regarding the risk of inadvertent file sharing. It is undeniable, however, that major file sharing networks have enormous user bases which are likely to include novice users with limited understanding of how the systems work. Distributors of file sharing software therefore have a serious responsibility to make sure that consumers are appropriately informed and that the software is designed to promote safe behavior and avoid confusion regarding the sharing of users' files. They have not always lived up to that responsibility.

CDT also strongly agrees that users should be able to uninstall or disable file sharing software at their own discretion. Indeed, this principle is not limited to file sharing software. The FTC in multiple spyware-related cases has effectively established that it is an unfair practice for downloadable software to prevent consumers from uninstalling it later.

At a minimum, then, the principles embodied in H.R. 1319 reflect basic and fair practices that every developer of file sharing software should follow.

Enacting specific legislation in this area is a more difficult question, for several reasons.

The first challenge relates to scope. It would be hard to limit the reach of this kind of bill to what is commonly understood as P2P file sharing software, as we believe the authors intend. That is because the main thing file sharing software does – namely, enabling the exchange of data files between Internet-connected computers – is common to many kinds of software. Indeed, CDT believes that the definition of "peer-to-peer file sharing program" in H.R. 1319 would apply to many other types of software, including Web browsers, Web servers, anti-malware software, and perhaps even operating systems. If legislation ends up sweeping in many kinds of software, there are likely to be a wider range of issues and complications to consider, as the bill's requirements might not prove appropriate in all contexts.

There also are challenges related to implementation and effectiveness. Some file sharing programs may prove difficult to regulate effectively, either because their authors and distributors are located overseas, or because they are open source programs developed on a decentralized basis and hence lack any corporate entity that could take responsibility for compliance. In addition, it is possible that a major proportion of today's inadvertent disclosure risk stems from older versions of software – with poor user interfaces or inappropriately configured default settings – that still reside on users'

computers. A bill enacted now may have limited ability to address this legacy software problem.

Finally, CDT generally believes Congress should not go down the path of imposing granular design requirements for specific technologies. Software development in particular is a highly innovative field in part because of its largely unregulated environment, enabling individual programmers and small start-ups to focus on drafting code rather than navigating regulatory requirements. Even for more established software companies, specific design requirements are likely to prove burdensome and inappropriate in individual instances. For example, H.R. 1319 requires disclosure and consent at the time of installation. This may be appropriate for most downloadable file sharing software, but what about software that comes pre-installed on a computer? A law that mandates the specific timing or nature of disclosures may prove unworkable with some products or in some technology environments. Moreover, personal data can be mistakenly disclosed in any number of ways, but legislation targeting P2P file sharing picks out a particular technology for regulation. That is why, as discussed above, CDT would prefer to address data privacy issues in the context of general privacy legislation.

CDT is not convinced there are fully satisfactory solutions to the challenges facing efforts to legislate on this topic. One way to try to reduce some of the concerns would be to avoid imposing granular mandates and instead simply require conspicuous disclosure and informed consent regarding file sharing functions before those functions are activated. If Congress believes greater detail is needed, it could direct the FTC to conduct a study or even a rulemaking on the matter. Rules adopted by the FTC would likely be better tailored to specific contexts and special cases than requirements established in statute.

If the Subcommittee decides to proceed with the current legislation, however, CDT would recommend the following specific changes to H.R. 1319.

Narrow the definition of software to which the bill applies.

As discussed above, CDT believes the bill's definition of "peer-to-peer file sharing program" in Section 4(2) would include such software as Web browsers, Web servers, anti-malware software, and probably many others. CDT also believes that the term "peer-to-peer" does not make a useful contribution to defining the bill's reach; the key question from a consumer standpoint is whether software could permit the unintended transmission of personal files to unknown parties, not whether the technical architecture could fairly be described as "peer-to-peer." CDT would suggest using the term "file sharing software" and defining it to include software that features all of the following four elements:

- The software is intended for and marketed to individual consumers.
- The software allows files stored on a user's local computer, including files actively and intentionally created by the user, to be designated as available for sharing with remote computers upon request by remote users.
- At the request of remote computers, and without requiring any further interaction, input, or authorization with or from the local user, the software will transmit to the remote computer (i) information identifying files that have been designated for sharing; and (ii) copies of such files.

- The remote computers capable of receiving such information and files need not have been individually selected or designated as intended recipients by the local user.

Significantly, this definition arguably would still include Web servers. Operation of Web servers by individual consumers is relatively uncommon, however, and Web servers aimed at the enterprise market would be excluded by the first element of the definition above.

Clarify the scope of parties to whom the bill applies.

Section 2(a) imposes requirements on persons that "cause or induce" a computer user to make files available through a file sharing program. These terms are broad and vague enough to leave significant questions about when and whether various Internet intermediaries might be covered by the bill. This creates a risk that parties who are not in any way the creators of software, like companies hosting public software distribution hubs or performing transmission or linking functions, could be held responsible for software that fails to operate as the bill requires. CDT believes that this would be dangerous, and suggests that any bill on this subject should focus narrowly on entities that actually produce software. In addition, as noted above, there are challenges in applying this legislative framework to open source software. CDT would suggest clarifying that Section 2 applies specifically to persons that develop or produce file sharing software intended for large scale or mass market distribution. The reference to "mass market" or some similar term would be important to include, because otherwise the bill could apply to individual hobbyists and tinkerers who are not in any way writing software for the general consumer marketplace.

Clarify the disclosure obligations under Section 2(a)(2).

As discussed above, CDT would advise making the bill's obligations more general and less prescriptive with regard to timing. With regard to the substance of the disclosure obligations, CDT notes that the requirement in Section 2(a)(2)(A) to disclose "which files are to be made available" is not entirely clear. For example, would it require specific notification of individual files in a user's "shared" folder at the time of initial activation, or would informing the user about the existence of the "shared" folder be sufficient? In addition, the language on its face does not appear to require any explanation of how files may be added or removed from the "share" folder in the future. CDT would suggest modifying Section 2(a)(2)(A) and (B) to ensure user disclosure and consent regarding (i) how the user can determine which files are currently designated for sharing; and (ii) what the process is for both adding and removing files from the designated sharing list.

Clarify and narrow the software removal provision.

Section 2(b)(2) applies to any person that caused or induced the installation of certain software. As discussed above with respect to Section 2(a), CDT believes that those terms are open ended and that it would be better to make the provision apply to those who develop file sharing software intended for commercial scale distribution. CDT also believes that the bill should not mandate the affirmative provision of a removal tool, as Section 2(b)(2) arguably does. Allowing removal using the operating system's regular removal function should be sufficient, and CDT recommends modifying the bill to make this clear. For example, the bill could require reasonable and effective means for

consumers to uninstall the software, either through the computer's operating system or other uninstall tool or instructions that can be readily located.

In addition, Sections 2(b)(1) and (2) refer to blocking or removal of a file sharing program "or function thereof." CDT does not believe that legislation should mandate that software allow users to block or remove individual software functions on an a la carte basis. To the extent that this language could be interpreted to impose such a requirement, it would raise complicated technical and policy questions. CDT recommends simply focusing on ensuring the ability to block or remove entire programs.

Conclusion

CDT welcomes the Subcommittee's leadership on data privacy and security issues facing consumers and on the specific bills examined in this hearing today. In particular, CDT would urge the Subcommittee to make general baseline privacy legislation a core part of its agenda on these issues. We stand ready to work with the members of the Subcommittee to craft practical policies to address the privacy challenges that arise in the rapidly changing technological environment. Thank you again for the opportunity to testify.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact: David Sohn, (202) 637-9800, dsohn@cdt.org