

**Testimony of
David Sohn
Senior Policy Counsel
Center for Democracy and Technology**

Before

The House Committee on Small Business

June 12, 2008

**Hearing on
“Electronic Payments Tax Reporting:
Another Tax Burden for Small Businesses”**

Chairwoman Velázquez, Ranking Member Chabot, members of the committee, thank you for holding this hearing on newly proposed reporting requirements concerning electronic payments. CDT appreciates the opportunity to participate.

CDT is a non-profit, public interest organization dedicated to preserving and promoting privacy, civil liberties, and other democratic values in the digital age. CDT has been a leader in addressing emerging threats to consumer privacy and the related issues of data security and data retention. CDT advocates a reasonable balance between privacy concerns regarding sensitive personal information and the legitimate needs of law enforcement and business. We believe that the proposal under discussion raises serious privacy and data security concerns that are especially significant in the small business context.

The proposed legislation would force banks that enable merchants to receive credit card payments to abandon the sound privacy and security practice whereby they currently do not track those merchants using Taxpayer Identification Numbers (TINs). For many of the smallest businesses, the TIN is the proprietor's Social Security Number (SSN). Thus, the proposal carries particularly acute privacy implications for many small business owners and runs contrary to the federal government's established goal of reducing the collection and use of SSNs in order to combat identity theft. In addition, the proposal would likely lead to the collection and retention of further personal and financial information relating to small business accounts; could create serious problems for small businesses in the event that credit card companies or other payment facilitators make

errors in recording or reporting data; and would establish a dangerous precedent in enlisting private sector intermediaries to track the behavior of customers for purely governmental purposes.

1. Background – Data Minimization Is an Important and Long-Recognized Privacy Principle

A set of commonly accepted “Fair Information Practices” (FIPs) has been the cornerstone of privacy protection for many years. The FIPs were initially articulated in the 1970s and embodied to various degrees in the Privacy Act of 1974, the Fair Credit Reporting Act, and other federal privacy laws. While the FIPs have been enumerated in various ways, they generally include the concept of data minimization.

The principle of “data minimization” means that companies and government agencies should limit their collection of information about individuals to what is directly relevant and necessary to accomplish a specified purpose, and should retain the data only for as long as is necessary to fulfill that purpose.¹ In other words, entities should collect only the personal data they really need, and should keep it only for as long as they really need it.

Data minimization provides an important safeguard against privacy and security risks. First, it reduces the likelihood of unauthorized or accidental disclosure of personal data.

¹ See, e.g., "Privacy Technology Implementation Guide," United States Department of Homeland Security, August 16, 2007 (http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_ptig.pdf).

The more data is collected and the longer it is electronically stored, the greater the risk that it will be leaked, stolen, sold, or otherwise disclosed. The ongoing parade of high-profile data security breaches in recent years makes it clear that once data is stored electronically, it is extremely difficult to guarantee its protection. Bad actors will work to gain access, and simple oversights such as an unattended laptop can result in unauthorized access to data. At least nine major data breach incidents were reported in just the last two weeks, each affecting thousands of Americans.² The Office of Management and Budget has rightly noted that an important step in preventing costly data breaches is “reducing the volume of collected and retained information to the minimum necessary.”³

Data minimization also helps protect against “mission creep.” This is the risk that personal data collected for one purpose will prove an attractive target for other parties with other purposes, resulting in disclosures and uses of the data that are significantly broader than the original parties to the collection of data (both the entity doing the collecting and the person from whom the information is collected) could have anticipated or expected. Collecting and retaining data that is not strictly necessary for a particular purpose opens the door to unanticipated uses and abuses.

² For an unofficial list of data breaches announced pursuant to breach disclosure laws, see The Breach Blog: <http://breachblog.com/>.

³ See Memorandum from the Deputy Director for Management, May 22, 2007 (<http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>).

2. Forcing Payment Facilitators To Keep TINs for Extended Periods Would Undermine Privacy and Security Protections Regarding the SSN of Many Small Business Owners

Consistent with the data minimization principle discussed above, the standard practice of banks providing merchant accounts for credit card payments is to collect a merchant's TIN when establishing an account, but then to delete the TIN once the account is approved. Instead of using a TIN (which may be a Social Security number) to identify and distinguish different merchants, the bank assigns an internal merchant identifier. Thus, the bank's databases do not link merchants with TINs and a security breach would not expose merchants' TINs. The Treasury Department's proposal to require reporting on each merchant's credit card receipts would force banks to abandon this sound security practice. Payment facilitators such as banks effectively would be required to retain and keep track of each merchant's TIN for an extended period.

This would raise particular privacy and security concerns for sole proprietorships. For owners of such small businesses or individuals engaged in small-scale business activity, the TIN may be the individual's Social Security number. Banks therefore would need to include many SSNs in their databases, and to tie those SSNs to individual merchant data for reporting purposes.

Requiring banks to maintain databases containing and tied to SSNs would set back the effort to prevent identity theft and other forms of fraud. It runs contrary to the recommendations of experts in privacy and identity theft, who continue to urge companies to wean themselves from excessive use of SSNs. It also runs contrary to the

federal government's own strategy for reducing identity theft. When the President's Identity Theft Task Force issued its findings last year, its foremost recommendation was to reduce the use of SSNs.⁴ The Task Force observed that a Social Security number is "the most valuable commodity for an identity thief."⁵ In light of this, banks' current practice of not retaining TINs is a sensible and important data security practice, and forcing them to abandon it would increase the risk of identity theft in the event of a data breach.⁶ CDT believes Congress should not push banks to abandon a common data security safeguard and potentially create a new target for identity thieves at a time when Americans are deeply and justifiably concerned about the prospect of identity theft.⁷

3. Implementing the Proposal May Entail Additional Expansion in Data Collection from Small Business Owners

CDT urges Congress to be skeptical of administration claims that the reporting envisioned by the proposal would translate neatly into major revenue increases. CDT is particularly concerned that this proposal, if enacted, would lead to further requirements

⁴ *See, generally*, the Identity Theft Task Force's report, "Combating Identity Theft: A Strategic Plan," April 23, 2007 (<http://www.idtheft.gov/reports/StrategicPlan.pdf>).

⁵ *See* "The President's Identity Theft Task Force Releases Comprehensive Strategic Plan to Combat Identity Theft," Press Release, April 23, 2007 (<http://www.ftc.gov/opa/2007/04/idtheft.shtm>).

⁶ According to one analysis, 30 percent of known identity thefts in 2006 were caused by corporate data breaches. *See* Sasha Romanosky, et al., "Do Data Breach Disclosure Laws Reduce Identity Theft?" Seventh Workshop on the Economics of Information Security, June 25, 2008 (<http://weis2008.econinfosec.org/papers/Romanosky.pdf>).

⁷ An April 2008 survey found that 81% of Americans are concerned about having their identity stolen. *See* Sheyna Steiner, "Consumers take steps to thwart ID thieves," *Bankrate*, April 21, 2008 (http://www.bankrate.com/brm/news/Financial_Literacy/identity_theft/ID_theft_poll_national_a1.asp?caret=95a). There were roughly 8 million victims of identity theft in the U.S. in 2007, with damages totaling \$45 billion. *See* "2008 Identity Fraud Survey Report," Javelin Research, February 2008.

for data collection because it is quite likely that the government will need even more information in order to make use of the information that banks would be required to report initially. For example, sometimes more than one small business may share a single merchant account, as in the case of multiple vendors at a flea market. Aggregate receipts for such an account would not provide a meaningful picture of the income received by any individual vendor. To make the information useful to the Internal Revenue Service, the bank providing the merchant account would need to collect and track substantially more data about account holder activity than it does today. Similarly, many small businesses may rely on payment systems such as PayPal. These systems could be pressed to collect further data from users in order to ensure that information reported to the I.R.S. more accurately reflects individual activity.

Wherever data about aggregate credit card receipts might paint an incomplete or misleading picture, there likely will be pressure to provide more detailed breakdowns and hence to collect and store more data. Before moving to adopt any legislative proposal in this area, Congress should carefully inquire into the types of additional data collection that would be demanded, either as an express requirement of the regime or as a logical follow-on or supplement to it.

4. The Proposal Is Particularly Inappropriate at a Time When the Privacy Framework Governing Personal Data Is Lacking

More broadly, before Congress imposes new obligations that would expand the scope of personal data that companies collect and maintain, it should conduct a full-scale

reexamination of existing data privacy laws. The United States' current privacy framework relating to private-sector data is uneven, and in recent years government has moved to weaken the legal standards under which government can access such information. Congress should not enact new laws that would exacerbate the already serious weaknesses in the nation's privacy framework.

5. Forcing Banks To Collect, Store, and Report Additional Customer Data for Purely Governmental Purposes Sets a Bad Precedent

A major concern for CDT is that the proposal to require reporting on credit card payments could establish a dangerous precedent and could encourage additional government efforts to enlist private-sector intermediaries in tracking the behavior of their customers. For example, if Congress were to enact this proposal, state governments might well consider enacting obligations for payment facilitators to keep and report data for state tax collection purposes.

Outside the context of credit card payments and tax collection, the Justice Department has advocated federal legislation to require Internet service providers to retain information about their customers' online activities for months or even years at a time for the assistance of law enforcement. CDT believes such data collection and retention mandates are highly objectionable. They threaten personal privacy, through the creation of massive new databases with personal information that could be subject to security breaches or misuse. They are susceptible to "mission creep." They undermine public trust, especially given the inadequate current legal framework governing use of private-

sector data and the government's ability to access it. And they are burdensome and costly. Congress should not embrace a mandatory private-sector data collection and retention scheme that could pave the way for additional mandates that would greatly undermine consumer privacy.

6. Conclusion

As this Committee and Congress evaluate proposals to require payment processors to report merchant transaction data to the I.R.S., CDT urges careful consideration of the impact for data privacy and security. CDT believes that the potential impact is serious, particularly for the small businesses that are the focus of this Committee. At a minimum, this suggests that proponents of the proposal should bear a heavy burden proof concerning whether the proposal is necessary, effective, and better than possible alternatives. CDT appreciates the opportunity to participate in this hearing and to share our views on this important topic.