

Treasury Proposes Forcing Credit Card Companies to Act as IRS Agents

May 19, 2008

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

In an effort to track down unreported small business income, the U.S. Treasury is calling on Congress to create a sweeping new program that would require all credit card companies to report the income of all merchants to the Internal Revenue Service.

[\(1\) Treasury Proposes Forcing Credit Card Companies to Act as IRS Agents](#)

[\(2\) Treasury Proposal Mirrors Problems with Other Data Collection and Data Retention Schemes](#)

[\(3\) Request for SSNs Runs Contrary to Anti-ID Theft Initiative](#)

(1) Treasury Proposes Forcing Credit Card Companies to Act as IRS Agents

In an effort to track down unreported small business income, the U.S. Treasury is calling on Congress to create a sweeping new program that would require all credit card companies to report the income of all merchants to the Internal Revenue Service.

The proposal, raised in President Bush's FY2009 budget, would require credit card companies to report the aggregate transactions of all of their merchants (that is, all the businesses that have merchant accounts with the card companies and to whom credit card payments are made). The reports to the IRS would have to be tied to the Taxpayer Identification Number (TIN) of the merchant. Many small businesses use their owners' Social Security Numbers as their TIN. A similar program aimed at Internet "brokers," including eBay and Amazon, which raised privacy concerns last year, seems to have been dropped from this year's budget proposal.

The credit card reporting proposal is disturbing on many levels. For starters, it would require credit card companies to turn over to the IRS large amounts of information about their merchants without any reason to believe that they have broken any laws. Also of concern is that such a law would require the collection, storage and transmission of large amounts of sensitive personal information at a time when Internet users are increasingly concerned about identity theft and when public and private sector data breaches have become routine.

To make matters worse, the proposal will create yet another private sector database tied to the Social Security Number at the very time that experts in privacy and ID theft are urging companies to wean themselves from use of the SSN. The proposal calls for credit card companies to submit the name, address, and TIN of each participating merchant that sells anything during the year and the net amount of that transaction. In order to comply, credit card companies would need to keep track of ID numbers and other information on all merchants. Credit card companies collect TINs and SSNs today from merchants at the time of approval, but the standard industry practice is to delete this information in favor of an internal merchant identifier. This security and privacy protection measure have to be abandoned if the IRS proposal moves forward.

Finally, the Administration request is just the latest manifestation of a broader effort by the government to force businesses to collect and retain large amounts of customer data. These "data retention" proposals would force the creation of massive, privately maintained databases of personally identifiable data that government investigators could tap at their leisure. What's particularly troubling about this trend is that it occurs against the backdrop of measures like the

PATRIOT Act that weaken the legal standards that protect ordinary Americans against undue government snooping.

The government is effectively seeking to increase the amount of information collected and stored about ordinary Americans even as it relaxes the standards by which it can obtain that information.

The Treasury Department has done little to justify why Congress should impose this substantial new burden on sole proprietors and other small businesses.

While the IRS needs TINs and SSNs for tax purposes, and private sector tax reporting is partly what the number was created for, this proposal essentially deputizes credit card companies and requires them to maintain this information for extended periods. The Treasury Department is seeking to dramatically increase the amount of sensitive personal data collected from individuals, even as other agencies are being urged to limit such collection as a means of combating ID theft.

[President's Budget FY2009 - Department of Treasury](#) [1]

[Policy Post 13.7, May 04, 2007 IRS Proposal Could Impact Millions of Internet Users](#) [2]

[Testimony before House Small Business Committee on credit card reporting proposal, June 12, 2008](#) [3]

(2) Treasury Proposal Mirrors Problems with Other Data Collection and Data Retention Schemes

The credit card reporting proposal is another example of efforts to require businesses to retain records of their customers for government purposes. Last year, the Treasury Department suggested data retention rules for Internet "brokers" such as Amazon and eBay, and the Justice Department has been calling for federal legislation that would require Internet service providers to retain information about their customers for months or even years at a time.

These proposals are all objectionable in the following ways:

- Data retention requirements threaten personal privacy and pose a security risk at the very time the public is justifiably concerned about security and privacy online. One of the best ways to safeguard privacy is to minimize the amount of personally identifiable data that is collected and stored. Data retention flies in the face of that wisdom by mandating the creation of large new databases of personally identifiable information that would become ripe targets for identity thieves. The credit card companies do not want to store this information for fear of a security breach. The government should not be forcing them to take risks with innocent taxpayer's information.
- Data retention laws are susceptible to "mission creep." Although the Treasury proposal calls only for reporting of bulk data on merchants, there is nothing in the proposal to limit the further use of the information that the sites must collect to generate those reports. Either the government or the brokers themselves could use the information for currently unanticipated purposes.
- Data retention laws undermine public trust. The new data disclosure demands that credit card companies would be required to make in order to meet their new IRS obligations would alienate small businesses and self-employed workers who are already rightly skittish about how much of their sensitive personal information they must surrender to do business. Right now, the main practice of credit card companies is to delete TINs and SSNs quickly when they receive them. This practice should be encouraged.
- Data retention laws are burdensome and costly. Particularly for smaller operators, the Treasury proposal represents a huge increase in record keeping, storage and paperwork.

Adoption of any data retention law should be preceded by a full-scale reexamination of existing data privacy laws. The US has a shaky privacy framework to deal with the kind of information that would be collected under this proposal. CDT has long maintained that Congress must enact comprehensive consumer privacy legislation and update the laws that protect our personal information from government intrusion. Until such rules are adopted, data retention requirements like the Treasury proposal would exacerbate the already serious weaknesses in our national privacy framework.

[CDT Data Retention Memo](#) [4] (June 2006)

(3) Request for Storage of SSNs Runs Contrary to Other Government Initiatives

In May 2007, the Office of Management and Budget called on government agencies to report on and cut down on the use of Social Security Numbers and to look into using alternatives to the numbers for internal identification. The reason for this policy is that widespread collection and storage of SSNs and TINs creates a risk of identity theft and fraud.

The OMB action followed the April 2007 Justice Department and FTC plan to combat identity theft, which called on government agencies to reduce unnecessary use of SSNs. The logic of reducing use of SSN use is obvious. SSNs are an essential element of many types of ID theft and often one of the main targets of serious data breaches. Until we can limit the frequency of data breaches, we can at least limit the negative exposure caused by breaches by limiting the number of places we store SSNs.

The underlying finding of the DOJ-FTC report - that SSNs are a prime target for identity thieves and that their use should be limited - is difficult to reconcile with a plan that calls for massive new collection and storage of TINs.

Although the DOJ-FTC report implies that the IRS is an appropriate agency to collect TINs, forcing credit card companies to maintain the data on all merchants creates a major new risk for those taxpayers who have done nothing wrong.

[OMB Memo 07-16](#) [5]

[DOJ-FTC ID Theft Release \(April 2007\)](#) [6]

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL:

<https://www.cdt.org/policy/treasury-proposes-forcing-credit-card-companies-act-irs-agents>

Links:

[1] <http://www.whitehouse.gov/omb/budget/fy2009/treasury.html>

[2] <http://www.cdt.org/publications/policyposts/2007/7>

[3] <http://cdt.org/testimony/20080612sohn.pdf>

[4] <http://www.cdt.org/privacy/20060602retention.pdf>

[5] <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>

[6] <http://www.ftc.gov/opa/2007/04/idtheft.shtm>