Your Tax Returns Are Hacker Bait

J.D. Tuccille

Apr. 10, 2014

Right about now, millions of Americans are staring at tax forms, silently or loudly cursing the ordeal according to their personal preferences. Maybe they'll answer a few nosy questions about their lives and finances and either receive a bit of their money back or make a payment to Uncle Sam. Maybe they'll answer a *lot* of nosy questions, with a similar outcome at the end. Either way few, if any, are happy about the cash slipping from their possession into Uncle Sam's coffers. It's possible, though, that they should be more concerned about just how well the Internal Revenue Service (IRS) safeguards the answers to those nosy questions.

As it turns out, the federal government is a remarkably terrible guardian of information, and the tax man keeps a treasure trove of personal data about almost every American.

"People often focus on whether government agency employees will abuse the citizens (as they did in the recent IRS scandal)," Chris Edwards, director of tax policy studies at the Cato Institute told me. "But probably a bigger threat is that the vast databases held by the IRS, HHS, security agencies, etc, will be leaked on purpose, leaked because of bureaucrat sloppiness, or be hacked. The more they collect, the more that will eventually leak."

Sometimes the threat is intentional, and from the inside. Last year, IRS employee Demetria Brown was indicted for wire fraud and aggravated identity theft after she fished information from the tax databases. Just months earlier, Tax Compliance Officer Ceil Love pled guilty after stealing her own niece's tax information for the same purpose. Also in 2013, IRS employee Joy Fox was indicted for stealing the identities of eight people from the tax agency's computer systems.

In 2012, former IRS employee Thomas W. Richardson received 105 months in prison for stealing the Social Security numbers of 58 people in order to file for $8 million in fraudulent refunds.

IRS agents also trawl through the databases out of what appears on some occasions to be sheer curiosity. Tax man John Snyder received three years probation in 2008 for scrolling through the records of 202 people for, he claimed, no particular reason. Similar nosiness is found in the records of the Treasury Inspector General for Tax Administration with mind-numbing frequency.

Whatever other benefits IRS employment may offer, an ability to satisfy snoopiness seems among the most appreciated.

But that sort of internal, deliberate abuse of personal information, common though it is, pales in comparison to the threat posed by sheer bungling and disregard for security.

"While of course the government needs at least some of this data to determine and levy taxes and to prosecute those who don't pay their fair share, if they're going to store so much information, they need to make sure they are taking steps to safeguard privacy and keep this data secure," notes Hanni Fakhoury, staff attorney for the Electronic Frontier Foundation, in answer to my questions. "The government's IT efforts with the healthcare exchange websites don't instill a lot of confidence about their technical acumen however."

Nor does the IRS's own history. Last year, in the midst of the brewing scandal over politicized scrutiny of conservative non-profit groups, the IRS posted the filings of Section 527 political organizations online, as it's suppose to do. Except that the filings contained the Social Security Numbers of tens of thousands of people. It's not supposed to do that.

Public.Resource.org, an organization devoted to making government (but not private) information accessible, discovered the error and asked the IRS to please stop. "While the public posting of this database serves a vital public purpose (and this database must be restored as quickly as possible), the failure to remove individual Social Security Numbers is an extraordinarily reckless act," the group noted.

Then again, the IRS *has* become more efficient about giving away Americans' personal details. In 2007, the Treasury Inspector General for Tax Administration (who seems to be very busy) reported (PDF) "the loss or theft of at least 490 computers between January 2, 2003, and June 13, 2006." Since data stored on IRS computers is typically not encrypted or otherwise secured, the report concluded, "it is likely that sensitive data for a significant number of taxpayers have been unnecessarily exposed to potential identity theft and/or other fraudulent schemes." How much simpler to post hacker bait to the Web rather than putting identity thieves through the trouble of snatching physical devices.

Criminal hackers may not be the only unintended recipients of the personal data Americans hand to the tax collectors. "We've already seen that the IRS may be privy to sensitive national security information, as well as information obtained from the DEA," the EFF's Fakhoury says, referring to Reuters reports that the Drug Enforcement Administration funnels surveillance data to federal agencies, including the IRS. "I would imagine the reverse happens too: the IRS providing tax information to DEA, NSA and other law enforcement agencies. That just amplifies the potential privacy violations."

The IRS already pushes constitutional boundaries in its efforts to gather information. Chris Calabrese, legislative counsel for privacy-related issues at the American Civil Liberties Union, points to the tax agency's since-abandoned claim that it has the authority to read emails without bothering to obtain a warrant. He cautions that the IRS (and many other government agencies) will gain similarly broad power if the Securities and Exchange Commission is successful in its

efforts to assert the power to compel data disclosures by third parties on the authority of nothing more than a subpoena issued by bureaucrats.

Any data gathered by such means will likely enjoy the same quality of privacy protection so well documented by the Treasury Inspector General for Tax Administration.

Americans sufficiently concerned enough about privacy to actually step beyond the IRS's jurisdiction find that escape isn't so easy. Worried that Americans were trying to flee U.S. taxes by fleeing the country, Congress passed the Foreign Account Tax Compliance Act to extend the IRS's jurisdiction—to the world.

"FATCA is a nightmare," says Cato's Edwards. "Even if an American renounces his citizenship and moves permanently to Britain, for example, he still has to file U.S. tax returns for 10 years."

Under FATCA, foreign financial institutions are required to surrender to the IRS information on "U.S. persons" who have accounts with them. The U.S. leans heavily on foreign governments to enforce FATCA on their own banks with payments to financial institutions in resistant countries subject to 30 percent withholding.

Not surprisingly, foreign banks and account holders find the law intrusive and burdensome. "FATCA will demand that Canadian banks hand over to the IRS personal information found in Canadian bank accounts linked to U.S. citizenship. Should a Canadian citizen's information be found there as well, it too will be turned over," warns the Canadian Federation of Independent Business.

Rather than be data-mined by American tax collectors proven unreliable in protecting their own citizens' information, many foreign banks now just refuse Americans' business. That, in turn, convinced many U.S. citizens living abroad to surrender their passports before the law fully kicked in.

The rest of us... well, we're still stuck coughing up information to the tax man, to be incompetently stored until some hacker can't resist the temptation.