The IRS Wields **New Weapon** Against Taxpayers

BY JOHN EDWARDS

NEW DATA COLLECTION AND ANALYSIS technologies are giving the Internal Revenue Service a powerful new weapon to ensure that people and businesses pay all of the taxes they owe. The IRS has long relied on relatively crude analytical tools to match the Social Security numbers and addresses on filers' tax returns against information printed on W2, 1099, and other income-reporting documents supplied by employers, financial institutions, and other parties.

Typically, if a taxpayer reports less income than the reporting documents indicate, the IRS will send a letter reporting the discrepancy and demanding either an explanation or full payment.

But a recent technology overhaul has taken the tax agency's ability to scrutinize taxpayers' financial activities to an entirely new level. "Big data," a computer industry term for systems that allow organizations to accumulate and analyze unprecedented amounts of information from a vast array of sources, promises to give the IRS far deeper insights into taxpayer activities and behavior.

With the help of big data, the IRS will be able to look at data arriving in rigidly structured formats, such as phone bills and credit card statements, as well as unstructured content, like contracts, emails, and Facebook posts.

The agency is currently using its new big data capabilities primarily for macro research tasks.

"The IRS research organization uses big data techniques to enable advanced analytics on massively large data sets," said Jeff Butler, director of research databases in the IRS' Research, Analysis, and Statistics division, in an interview published on the MeriTalk website. "Examples include estimating the U.S. tax gap, and predicting identity theft and refund fraud."

Down the road, however, big data promises to help the IRS better detect taxpayer deceptions, uncover multiple identities, and identify unusual financial activities to determine more accurately who should be investigated for fraud or denied refunds. "The IRS will use the big data info it gets from phone companies, banks, and hotels to choose whom to audit," predicts Nathan MacPherson, a tax attorney based in Anchorage, Alaska. "Formerly we had red flags, such as the home office deduction, and now we face red flags based on this big data."

MacPherson says that one way the IRS might decide to use big data is for the detection of suspicious activities. "Cellphone records and regular phone records: Are you making phone calls to someone in Belize, for instance, a tax haven? Or the Bahamas? Do you have regular phone calls with people over there?" MacPherson asks. "With your credit card records and other bank records, they can see the [money] flow going through, and if that doesn't match up with what you're reporting, then they may want to know what's going on."

Joe Mastriano, a Houston-based certified public accountant whose firm specializes in tax matters, is concerned that the IRS is increasingly relying on external contractors — many of whom are acquiring their own big data capabilities — to find ways of obtaining money from taxpayers who already owe back taxes and penalties.

> **"The IRS will use the big data info it gets from phone companies, banks, and hotels to choose whom to audit."**
>
> **— Nathan MacPherson, tax attorney**

"They have these computers, and they're very, very sophisticated now," Mastriano says. "[The IRS] will give vendors your Social Security number, and they can get into your health records, all your credit card transactions, as well as eBay, Facebook, and Google Maps data."

The accumulation of massive amounts of taxpayer data also poses another important danger: data leaks.

"The risk of identity theft due to IRS leaks of private taxpayer information, as has recently happened, or hacking of IRS computers, just like has happened with computers of big companies," MacPherson observes.

Mastriano thinks that the IRS' use of external contractors also raises the risk of data leaks. "They're giving out our Social Security numbers to third party contractors," he says.

Is big data's potential payoff, better taxpayer compliance and improved revenue collection, worth the effort and risk? MacPherson doesn't think so. "The IRS' own statistic shows that 98 percent of IRS revenue comes from voluntary front-end compliance," he says. "Big data is not needed to curb the 2 percent of bad apples." ❑

ILLUSTRATION/MATTHEW BILLINGTON

GUARDING YOUR ONLINE PRIVACY

Avoid Placing Private Data in the Cloud

■ File-syncing and storage services like Dropbox and iCloud are useful and convenient, but they are hardly privacy bastions. That's because most of the data you send into the cloud ends up on corporate servers that lie beyond your personal control. Law enforcement officials who obtain the right paperwork, regardless of how little justification they may have for looking at your files, can then view your financial records with impunity and without your knowledge.

Sidestep Service-Based Software

■ Financial applications that are based on software running on remote servers, rather than your own computer, pose the same privacy risks as file-syncing and storage services. Use such software at your own risk.

Check Privacy Policies

■ Study the privacy policies of your bank, credit card, insurance, and other financial service providers. Does the organization you're entrusting your personal data to have the right to sell the data to third parties? Can you opt out of this activity? Under what conditions will the organization reveal your account information? Who will receive it? If you don't like what you see, take your business elsewhere.

Don't Respond to Emails Requesting Personal Information

■ Watch out for "phishing" emails or screen pop-ups requesting sensitive information, such as Social Security numbers or financial account numbers and passwords. Also don't believe a screen pop-up that leads you to a purported financial or government website, no matter how "legit" the page looks. Instead, log onto the organization's site directly or call the company or agency yourself. Never use a link embedded within the email.

Secure Your System

■ Use a firewall and spam-filtering and anti-virus software to block "Trojan horses" and other types of malware that can steal information from your computer or smartphone.

Don't Say Regrettable Things Online

■ Exaggerating your income or boasting about dubious deductions on a social media site where you can be identified could lead to dire — and expensive — consequences. ❑