12-7-2017

Cybersecurity and Tax Information: A Vicious Cycle?

Diane M. Ring
Boston College Law School, diane.ring@bc.edu

Cybersecurity and Tax Information: A Vicious Cycle?

Author : Diane Ring

Date : November 7, 2017

Michael Hatfield, *Cybersecurity and Tax Reform,* 93 **Ind. L.J.** (forthcoming Spring 2018) available at SSRN.

The international tax arena is awash with calls for tax transparency, and a variety of reforms are underway at the national, regional and global level to bring such transparency to fruition. See, e.g., Joshua Blank's recent article *The Timing of Tax Transparency*, reviewed by Omri Marian earlier this year. Of course, with great caches of information comes great potential for security breaches of all types. Michael Hatfield, in his forthcoming article, *Cybersecurity and Tax Reform*, draws attention to the immensely important cybersecurity risks and challenges of a tax system founded on government collection and use of significant quantities of information. Quoting a former FBI Assistant Director, Hatfield describes IRS taxpayer information as "the gold standard" for being a "treasure trove of information" from the perspective of cyber criminals—large quantities of very valuable data housed in one agency. Is the IRS ready? Maybe not.

Hatfield's solution to these cyber risks (given the operational demands of running a tax system and the constraints faced by the IRS) is substantive law reform and not merely more security. To be clear, security is a great idea, but at some point, reality must step in and when it does, Hatfield argues that it points to a remedy grounded in tax *design* and not just cybersecurity. His bold proposal—to have the tax system collect less data—relies on the marriage of substantive law changes and a rethinking of the sources of data security.

To make his case, Hatfield begins by painting a somewhat discouraging picture of technology at the IRS. The IRS was an early adopter of computer technology in the 1960s, but it did not stay on the cutting edge. Hatfield offers a nuanced and rich understanding of why the IRS has had difficulty keeping pace with new technology and increasing demands on computerization in the ensuing decades. He points to a mix of factors including: (1) inadequate funding for the scale of the task (given the complex nature of IRS work, the volume of data, and the need to interface with the public); (2) inability to recruit and retain cybersecurity experts (with competition from not only the private sector but also from other government agencies such as NSA, the Pentagon, and the White House, which as Hatfield suggests, may have more "mission" appeal than the IRS); (3) too many users (including both IRS employees as well as taxpayers, third party information reporters, and tax professionals); and (4) the inherent challenges of cybersecurity.

What is interesting in light of its less-than-stellar cybersecurity/technology is that the IRS has not suffered a catastrophic cyberattack or breach to date. In an odd twist, Hatfield contends that the outdated technology at the IRS has served as a partial barrier to cybersecurity attacks. However, the pressure for the IRS to modernize remains strong. Technological innovation is viewed as the path by which the IRS can improve collection of taxes owed. There is also pressure to turn the tax compliance process into the online experience demanded by members of Congress and the public. These constituents have come to expect full online access and service based on their private sector experiences with ordering goods and services, managing bank accounts, and paying and processing credit cards online. In the face of pressure to modernize, Hatfield remains less than sanguine about IRS success on the technical battleground of cybersecurity.

Instead, Hatfield suggests that Congress seriously embrace a goal of collecting less information. He draws on a number of contemporary tax reform proposals to demonstrate ways in which some of them could systematically reduce the quantity and variety of information required and the number of individuals interacting with the tax system. One example he highlights is Pay-As-You Earn (PAYE)—a system of withholding through the year that would adjust withholding to ensure that the net amount withheld matches the taxpayer's overall tax liability. The result would be no

refund and possibly no tax return—at least assuming certain other simplifying tax law changes accompany PAYE, such as a reduction in the number of credits and deductions, fewer tax rates, and a diminished role of family status in individual taxation.

Hatfield offers this and other examples to illustrate his broader argument that Congress can and should tackle the challenge of cybersecurity in the tax system through a new approach to tax legislation. Specifically, he urges Congress to add *cybersecurity impact* to the usual list of criteria according to which tax legislation is judged (revenue, efficiency, equity, administrability, and political viability). Thus, Congress would consider whether proposed tax legislation would reduce the quantity and types of data collected and would consider such a reduction a point in favor of a particular rule. Hatfield makes a compelling case for the need to minimize the collection problem by having less data in the first place, rather than relying on raw technology and security to protect tax information. But he appreciates the tradeoffs that such an approach would entail in terms of accuracy, precision, equity, and the tax system's ability to meet non-revenue goals (e.g., redistribution, business incentives, etc.).

There may be another reason that limited-information tax regimes may be difficult for the IRS to implement: cybersecurity risks from the *private sector* and from *foreign governments*. Across the globe, tax leaks (including leaks of data gathered in hacks of financial institution customer data) have highlighted notable gaps in tax laws, tax enforcement and tax compliance. The public and legislatures are now regularly confronted with information suggesting ways in which social, political and economic elites have engaged in tax evasion or tax avoidance. In response, international pressure has mounted for increased tax transparency and disclosures to governments. The goal is to have governments directly collect the useful information that tax leaks have been providing. It is possible that we may find ourselves trapped in a cycle in which cybersecurity risks emanating from the private sector and foreign governments create pressure on the IRS to obtain more information, which then generates cybersecurity risks associated with growing government data repositories. It is unclear whether Congress would be willing to affirmatively reduce information collection to break the cycle. But, as Hatfield argues effectively, it is an option Congress needs to take seriously.

Cite as: Diane Ring, *Cybersecurity and Tax Information: A Vicious Cycle?*, JOTWELL (November 7, 2017) (reviewing Michael Hatfield, *Cybersecurity and Tax Reform,* 93 **Ind. L.J.** (forthcoming Spring 2018) available at SSRN), https://tax.jotwell.com/cybersecurity-and-tax-information-a-vicious-cycle/.