Maurer School of Law: Indiana University
Digital Repository @ Maurer Law

Indiana Law Journal

Volume 93 | Issue 4 Article 6

Winter 2018

Cybersecurity and Tax Reform

Michael Hatfield
University of Washington - Seattle Campus, mhat@uw.edu

Follow this and additional works at: https://www.repository.law.indiana.edu/ilj

 Part of the Internet Law Commons, and the Tax Law Commons

Recommended Citation

Hatfield, Michael (2018) "Cybersecurity and Tax Reform," *Indiana Law Journal*: Vol. 93 : Iss. 4 , Article 6.
Available at: https://www.repository.law.indiana.edu/ilj/vol93/iss4/6

This Article is brought to you for free and open access by the Law School Journals at Digital Repository @ Maurer Law. It has been accepted for inclusion in Indiana Law Journal by an authorized editor of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.

JEROME HALL LAW LIBRARY
INDIANA UNIVERSITY
Maurer School of Law
Bloomington

Cybersecurity and Tax Reform

MICHAEL HATFIELD*

INTRODUCTION

Sometimes the most practical solutions to digital technology problems are not digital. Some Russian security officials have returned to using manual typewriters for sensitive communications because every "form of electronic communication is vulnerable," which means, as one official explained, sometimes "the most primitive method is preferred: a human hand with a pen or a typewriter."[1] In Germany, too,

---

* Professor of Law, University of Washington. I would like to thank Scott Schumacher, Shannon McCormack, Adam Thimmesch, Leandra Lederman, Steve Johnson, and Nina Olson. I would like to thank the participants in the 2016 University of Washington Graduate Program in Taxation Symposium, those in the 35th Cambridge International Symposium on Economic Crime at Jesus College, Cambridge, England, and those in 27th Annual Tax Research Network Conference at University of Birmingham, England. For their excellent research assistance, I would like to thank Mary Whisner, Sam Hampton, and Logan Weaver.

1. Miriam Elder, *Russian Guard Service Reverts to Typewriters After NSA Leaks*, GUARDIAN (July 11, 2013, 11:42 AM), https://www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks [https://perma.cc/ZRZ3-J7FU].

some government employees are being discouraged from using digital technology for communication, instead encouraged to talk over coffee, lunch, and walks.[2]

As evidenced by the 2016 presidential election related hacking of campaign e-mails, the United States faces serious cybersecurity problems too. Unfortunately, cybersecurity is very difficult to achieve.[3] There are millions of lines of code in each computer program, each line potentially vulnerable to attack.[4] Attacks are easy, fluid, and constant.[5] Defense requires constant success; attackers need only rare success in order to do great damage.[6]

But it is the human factor that is the greatest difficulty for cybersecurity.[7] Motivated by financial gain, personal grudges, or political ideals, human users are unavoidable risks, even when those users have limited technical skills.[8] The greatest loss of top secrets in U.S. history involved an inside user with just a thumb drive and a security clearance.[9] Indeed, it was Edward Snowden's thumb drive that pushed Russians to manual typewriters and Germans to long walks.[10] But the risks are greater than those raised by dissident insiders, as indifference and negligence, such as the failure to use good passwords or resist curious links, are the more common and more difficult risks to manage.[11]

A great deal is risked by inadequate cybersecurity. Identity theft and other cybercrimes cost victims financially and psychologically.[12] There are also cyberwar and cyberterrorism.[13] Physical infrastructures, like utilities and nuclear reactors, have been hit through cyberattacks.[14] But in this newest age of war and terrorism, information is increasingly becoming the target. In recent "vacuum cleaner" attacks, the Chinese government vacuumed up personal information on tens of millions of Americans whose health was insured by Anthem and another four million government employees whose security clearance files were held by the federal Office of

---

2. Philip Oltermann, *Germany 'May Revert to Typewriters' To Counter Hi-Tech Espionage*, GUARDIAN (July 15, 2014, 2:04 PM), https://www.theguardian.com/world/2014/jul/15/germany-typewriters-espionage-nsa-spying-surveillance [https://perma.cc/WB2R-P93Z] (discussing the strategy considered by the German government).

3. Peter J. Denning & Dorothy E. Denning, *Cybersecurity Is Harder than Building Bridges*, 104 AM. SCIENTIST 154, 154 (2016).

4. *Id.* at 156.

5. *Id.* at 155–56.

6. *See id.*

7. *See infra* Part II.D.

8. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-758T, INFORMATION SECURITY: CYBER THREATS AND DATA BREACHES ILLUSTRATE NEED FOR STRONGER CONTROLS ACROSS FEDERAL AGENCIES 4 (2015).

9. Chris Strohm & Del Quentin Wilber, *Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers*, BLOOMBERG: TECH. (Jan. 10, 2014, 12:01 PM), http://www.bloomberg.com/news/articles/2014-01-10/pentagon-says-snowden-took-most-u-s-secrets-ever-rogers [https://perma.cc/DWE3-3E9A].

10. *See infra* notes 285–289 and accompanying text.

11. *See infra* notes 77–82 and accompanying text.

12. *See infra* Parts I.B, III.

13. *See infra* notes 136–50 and accompanying text.

14. *See infra* notes 136–142 and accompanying text.

Personnel Management (OPM).[15] Building a database on individuals in potentially hostile nations has become a war aim in the digital age.[16] But even more worrisome for national security experts is the opportunity for hostile actors quietly to take control of U.S. information systems by quietly manipulating the data in those systems.[17]

According to FBI experts, the IRS information system is the "gold standard" for cyberattacks in the United States.[18] The IRS collects personal information, and, in some cases, extraordinarily detailed and sensitive information, on about 290 million individuals each year.[19] With a U.S. population of 328 million, that is not information on everyone, but it is information on closer to everyone than any other single agency collects.[20] The IRS also handles more money than any other agency: $3.3 trillion in total collections and $403 billion in individual income tax payments.[21] Taking advantage of online refund processing, each year cybercriminals steal about $3 billion from the IRS.[22] Last year they also stole detailed personal information on about 724,000 individual taxpayers.[23]

But there are greater risks. Even more would have been lost if the IRS database were the target of a vacuum cleaner attack like Anthem and the OPM. Or if IRS information were quietly manipulated to push payments into criminals' accounts or push taxpayers and tax administrators into confusion. Or if the information were simply deleted, destroying all record of payments and filings and dropping the government, taxpayers, and the economy into costly chaos.

Unfortunately, there is no reason to believe the IRS will develop adequate cybersecurity. While history is not determinative, it is revealing. And while the IRS has achieved some significant information technology successes, its history is marked more by significant failures.[24] The IRS computing system remains largely dependent on the magnetic tape drives housed in the Martinsburg, West Virginia,

---

15. Ellen Nakashima, *With a Series of Major Hacks, China Builds a Database on Americans*, WASH. POST (June 5, 2015), https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html [https://perma.cc/V8XP-68LK].

16. *See id.*

17. Spencer Ackerman, *Newest Cyber Threat Will Be Data Manipulation, U.S. Intelligence Chief Says*, GUARDIAN (Sept. 10, 2015), https://www.theguardian.com/technology/2015/sep/10/cyber-threat-data-manipulation-us-intelligence-chief [https://perma.cc/YTG8-YVXV].

18. Krysia Lenzo, *Ex-FBI Official: IRS Is a Favorite Target*, CNBC (Feb. 10, 2016), http://www.cnbc.com/2016/02/10/ex-fbi-official-irs-is-a-favorite-hacking-target.html [https://perma.cc/92L8-G3SP].

19. JUSTIN BRYAN, INDIVIDUAL INCOME TAX RETURNS, 2011 (2013) http://www.irs.gov/pub/irs-soi/13inreturnsfallbul.pdf [https://perma.cc/6KT8-NCCG].

20. *U.S. and World Population Clock*, U.S. CENSUS BUREAU, http://www.census.gov/popclock.

21. INTERNAL REVENUE SERV., DATA BOOK 3 tbl.1 (2015), https://www.irs.gov/pub/irs-soi/15databk.pdf [https://perma.cc/3NUD-BH63].

22. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-508, IDENTITY THEFT AND TAX FRAUD 1–2 (2016).

23. *Id.* at 6.

24. *See infra* Part II.A.

computer center established in 1961.[25] After decades of work and billions of dollars, the IRS has failed to establish a state-of-the-art computer system, or even a searchable database of all taxpayer information.[26] Indeed, after four years of work and $139 million dollars, the IRS has failed even to upgrade from Windows 2003 to Windows XP.[27]

The IRS now spends $2.4 billion each year on computer technology, but that is spread among nineteen different projects, of which updating its system is only one.[28] Given the billions spent already, there is no reason to believe adequate technology at the IRS is merely a matter of funding. All the same, Congress has been reducing funding at the IRS for years, and probably will continue to do so.[29] It would require a substantial increase in IRS funding to return it to past levels, which makes it even less likely the IRS will achieve adequate cybersecurity.[30]

But cybersecurity is difficult for even well-funded organizations to achieve.[31] There is a shortage of cybersecurity experts, and the IRS has to compete with Google and the Pentagon for them.[32] Making the problem worse, the complexity of the IRS computing system exceeds that of most outside organizations.[33] The IRS computing system involves hundreds of millions of users, billions in payments to hundreds of millions of taxpayers, trillions in collections from hundreds of millions of taxpayers, and notoriously complex laws, regulations, and processes.[34] Doubting the IRS's ability to secure its system does not mean doubting the effort or intelligence of IRS employees. It only means taking seriously the difficulties faced by these employees and taking seriously the history of technology failures that have occurred despite the decades of hard work by those employees and the billions of dollars spent by their managers.

Given that the IRS is the gold standard for cyberattack but yet cannot manage to upgrade its Windows systems, one may wonder why the worst sorts of attacks have yet to hit the IRS. Ironically, it may be the decades of failures that have protected the IRS from cutting-edge technological attacks.[35] While not like manual typewriters, the antiquated system of the IRS, which until very recently depended entirely on weekly uploads to magnetic tapes, is not at all like the updated systems at Anthem

---

25. *See infra* notes 183–187 and accompanying text.

26. *See infra* notes 192–209 and accompanying text.

27. TREASURY INSPECTOR GEN. FOR TAX ADMIN., NO. 2015-20-073, INADEQUATE EARLY OVERSIGHT LED TO WINDOWS UPGRADE PROJECT DELAYS 2 (2015), https://www.treasury.gov/tigta/auditreports/2015reports/201520073fr.pdf [https://perma.cc/Z3DB-GC92].

28. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-297, INFORMATION TECHNOLOGY: MANAGEMENT NEEDS TO ADDRESS REPORTING OF IRS INVESTMENTS COST, SCHEDULE, AND SCOPE INFORMATION 1–4 (2015).

29. *See infra* Part II.B.

30. *See infra* Part II.B.

31. *See infra* Part II.E.

32. *See infra* Part II.C.

33. *See* James R. Thompson, *Fixing the IRS*, GOV'T EXECUTIVE (Apr. 1, 2012), http://www.govexec.com/magazine/features/2012/04/fixing-irs/41637 [https://perma.cc/MW2N-MGK5].

34. *See infra* notes 280–283 and accompanying text.

35. *See infra* notes 290–294.

and the OPM that the Chinese government vacuumed.[36] While this technological arrest has been unintentional, unlike the intentional Russian and German government strategies, it appears to have been effective. What has been successfully attacked at the IRS are not these older systems, which are open only to IRS users, but the newer, public-facing systems that provide outside users greater convenience in getting refunds or information.[37]

However, like all other institutions, the IRS is interested in increasing user convenience and institutional efficiency through greater use of information technology, not less.[38] There is long-standing pressure on the IRS to reduce the gap between taxes owed and taxes paid and to reduce the burden of those filing returns and paying taxes.[39] President Barack Obama said that IRS technology should make filing returns and paying taxes as easy as ordering pizza online.[40] And the IRS itself has articulated a Future State initiative in which almost all taxpayer experiences are mediated through information technology.[41]

The political appeal of making taxpaying more like pizza ordering, the political necessity of more effective and more efficient tax collection, and popular delight with all things new and digital means that the IRS will not regress technologically. The IRS is not about to order typewriters. This is obviously true. But so is the IRS's inability to achieve cybersecurity. At risk are cash payments to be stolen, in large part by international crime syndicates. At risk are personal identities and information to be stolen, in large part by the same criminal actors. And at risk are the revenue, economic, and political consequences of information being vacuumed, changed, or destroyed by political activists, terrorists, or government actors.

This Article takes seriously the cybersecurity challenges faced by the IRS as well as the agency's limitations in solving those challenges through its technological advances. The Article argues that we ought not to depend wholly on changes in technology but must change the way we think about cybersecurity. This Article argues the government ought not to leave cybersecurity as an information technology problem for the IRS to solve but ought to come to it as a legal problem for Congress to solve.[42] Congress has designed a tax system that requires the IRS to collect information on hundreds of millions of individuals and to routinely issue hundreds of billions in refunds.[43] If the tax law did not require so much information on so many, nor involve refunds to so many, the IRS would be a less appealing and more defensible cyberattack target.[44] In short, if the tax law were simpler in specific ways, the

36. *See* Nakashima, *supra* note 15.

37. *See infra* notes 292–293 and accompanying text.

38. Michael Hatfield, *Taxation and Surveillance: An Agenda*, 17 YALE J.L. & TECH. 319, 322–23, 339–40 (2015).

39. *See infra* notes 77–82 and accompanying text.

40. Issie Lapowsky, *Filing Taxes Should Be as Easy as Ordering Pizza, Obama Says*, WIRED (Oct. 12, 2016), https://www.wired.com/2016/10/obama-filing-taxes-easy-ordering-pizza [https://perma.cc/7UD6-HYM4].

41. *See infra* notes 66–71.

42. *See infra* Part III.B.

43. *See infra* Part III.B.

44. *See infra* conclusion of Part III.B.

information technology needs at the IRS would be simpler, and adequate cybersecurity for the IRS would be easier.[45]

There are many ways to define and collect tax liabilities.[46] Tax law is a matter of politics, not science. Perhaps much to the sadness of those who wish it were a science, tax law is determined by political compromises and best guesses. The tax law need not demand so much information on so many individuals, nor must its administration turn on a system that generates refunds as a rule rather than an exception.[47] Within the limits of the political and financial realities that determine legislation, there is ample flexibility for Congress to reform tax law so that it demands less of both taxpayers and tax administrators and, thereby, provides more information security.[48] There are a great number of long-familiar tax reform proposals each with a unique balance of advantages and disadvantages. This Article argues that when considering these reforms, Congress should begin to weigh the impact of cybersecurity on the scales along with other traditional concerns.[49] Of course, cybersecurity should not be the heaviest of considerations—but it should be a thumb on the scale. Tax reforms can decrease the treasure trove held by the IRS and increase the likelihood the IRS can defend it.[50]

Part I describes cyberattacks at the IRS and elsewhere, predicting future cyberattacks at the IRS will be similar to previous cyberattacks. Part II begins with a history of computer use at the IRS, arguing that this history—as well as a variety of other factors, like inadequate funding and expertise and the technical and human difficulties of cybersecurity—reveals little reason to be hopeful that the IRS will fail to achieve appropriate cybersecurity. Part III argues that Congress should consider how potential tax reforms might make the IRS database a less appealing and a more defensible cyberattack target. This Article concludes with reflections on the relationship between law reform and the digital revolution.

I. THE PAST AND FUTURE OF THE IRS AS A CYBERATTACK TARGET

The IRS has been the target of cyberattacks, and it will be again. As described in Part I.A, billions of dollars are stolen each year through the online filing process, and personal information on 724,000 taxpayers was stolen in 2015 through online access to taxpayer account information. Part I.B looks to three factors to predict the types of cyberattacks the future likely holds for the IRS. The first factor is the increasing use of information technology (IT) at the IRS to collect more personal information. The second factor is that no other agency will be collecting more information on as many individuals as the IRS, making the IRS the greatest treasure trove of personal information in the country. The third factor is the range of cyberattacks and threats more broadly, which suggests the risks for the IRS include cybercriminals holding

45. *See infra* conclusion of Part III.B.
46. *See infra* notes 297–300.
47. *See infra* conclusion of Part III.B.
48. *See infra* conclusion of Part III.B.
49. *See infra* notes 307, 312, 340, 359, 376, 384–387 and accompanying text.
50. *See infra* conclusion of Part III.B.

IRS information for ransom, and terrorists and hostile governments aiming to damage the U.S. revenue collection system, political stability, and economy by stealing, changing, or destroying IRS information.

A. IRS as a Cyberattack Target

The IRS was an early adopter of computers, having computerized much of its operations by the mid-1960s, but it has struggled over the past decades to keep its systems current with new technology and security.[51] Among its struggles has been providing a secure system by which the hundreds of millions of individual taxpayers are able to provide and receive payments and information online.[52] In a limited sense, electronic return filing has been successful, insofar as most individual returns are now filed electronically.[53] However, the IRS is unable to ensure the identity of the person filing a refund-claiming return.[54] To appreciate the scope of this inability, one has to realize that, while casually one may think of the IRS primarily as receiving payments, in practice, one of its primary functions is refunding to individuals the amount by which their withheld tax payments exceeded the amount eventually shown due on their returns. Each year, the IRS makes refunds to about 119 million individual taxpayers.[55] These refunds total about $403 billion a year.[56] Predictably, this volume of payments lures criminals who file refund-claiming returns online with stolen personal information. About $26 billion is claimed fraudulently each year this way.[57] The IRS prevents or recovers about $23 billion.[58] But the IRS pays out and is unable to recover over $3 billion in fraudulent refunds each year.[59] Of course, the IRS has focused on improving the security of the process. For example, it provides special identification numbers to improve security.[60] But the IRS has been unable to secure even these numbers from criminal hackers: in 2016, hackers stole over 100,000 of these special filing numbers.[61]

Though the process has tremendous security problems, the IRS has offered online filing for decades. However, until 2015, the IRS did not offer individual taxpayers online access to their historic tax information. In January 2015, the IRS launched the Get Transcript service, enabling taxpayers to view this information (known as a

---

51. *See infra* Part II.A.
52. *See infra* Part II.D.
53. *See infra* notes 210–220.
54. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 22, at 8–9.
55. INTERNAL REVENUE SERV., *supra* note 21.
56. *Id.*
57. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 22, at 14.
58. *Id.*
59. *Id.*; *see also* NAT'L TAXPAYER ADVOCATE, 2009 ANNUAL REPORT TO CONGRESS 338–41 (2009); Matt Hunter, *Tax-Refund Fraud To Hit $21 Billion, and There's Little the IRS Can Do*, CNBC (Feb. 11, 2015), http://www.cnbc.com/2015/02/11/tax-refund-fraud-to-hit-21-billion-and-theres-little-the-irs-can-do.html [https://perma.cc/DTQ9-VS4A].
60. Jen Wieczner, *Why the IRS's Technology Nightmare Is Far from Over*, FORTUNE (Mar. 25, 2016), http://fortune.com/2016/03/25/irs-technology-taxes [https://perma.cc/T9PC-3DHJ].
61. *Id.*

"transcript") online.[62] Unfortunately, the security of the service was so low that, within the first few months of the service, hackers stole personal information from about 724,000 taxpayer accounts, and the service had to be cancelled.[63] These taxpayer accounts "have so much information that not only can [the cyber criminals] file false tax returns and get refunds, they can also sell that data on the black market and make an additional profit," according to former FBI Assistant Director Chris Swecker.[64] He described taxpayer account information as "the gold standard" and "the treasure trove of information" cyber criminals are seeking.[65]

B. The Future of the IRS as a Cyberattack Target

What types of future cyberattacks on the IRS should be anticipated? In the past, its failure to secure its online refund-claiming process has cost the government about $3 billion a year. Its failure to secure taxpayer information online has cost hundreds of thousands of individuals their personal information—within the first few months of making that information available online. To get a sense of the future cybersecurity problems at the IRS, we have first to note the ambitious plans the IRS has for updating its use of IT. Next, and perhaps most revealing, we need to consider what types of cybersecurity attacks other agencies have faced.

1. Information Technology

In 2015, the IRS announced its "Future State initiative." This is the agency's plan to "take advantage of the latest technology to enhance the entire taxpayer experience."[66] This plan involves a "web-first" strategy, aiming to provide to taxpayers an online opportunity for providing and receiving all of their tax relevant information.[67] This would not just be for filing returns and accessing prior returns, but for all communications with the IRS.[68] The IRS intends to become more interactive with the taxpayers through this strategy.[69] It expects to increase the speed at which information is gathered, from the taxpayer and third parties, and analyzed to reveal a taxpayer's potential compliance issues.[70] In short, the "future state" the IRS is pursuing

---

62. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 22, at 6; Jada F. Smith, *Cyberattack Exposes I.R.S. Tax Returns*, N.Y. TIMES (May 26, 2015), https://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html [https://perma.cc/W8RY-S53D]; *Written Testimony of Commissioner Koskinen on Unauthorized Attempts To Access Taxpayer Data Before Senate Finance Committee*, IRS (June 2, 2015), https://www.irs.gov/newsroom/written-testimony-of-commissioner-koskinen-on-unauthorized-attempts-to-access-taxpayer-data-before-senate-finance-committee [https://perma.cc/WJ8X-AJE6].

63. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 22, at 6; Smith, *supra* note 62.

64. Lenzo, *supra* note 18.

65. *Id.*

66. *Future State Initiative*, IRS, https://www.irs.gov/uac/newsroom/future-state-initiative [https://perma.cc/32JN-CPDJ] (last updated Nov. 9, 2018).

67. *Id.*

68. *Id.*

69. *See id.*

70. *Id.*

is one in which more digital information is collected and then analyzed and used more successfully by the agency.[71]

This initiative needs to be put into its context. As discussed below, the IRS's earliest successes at computerization have been followed by decades of high-profile, expensive failures to update its system. IRS announcements of new high-tech initiatives have become routine, and so have the announcements of newer initiatives to replace the formerly new initiatives. While this gives good reason to doubt the IRS will succeed in digitizing all of its operations and interactions with taxpayers, there is no reason to doubt the IRS will try.

It is obvious why the IRS will try. After all, every other organization in the twenty-first century is focused on leveraging off the IT revolution.[72] To appreciate the potential usefulness of emerging IT to the IRS, consider the importance of information to the tax administration. Former IRS Commissioner Doug Shulman described the IRS as "an information intensive enterprise," saying that what "really matters" to the IRS is "the organization of data and ultimately the knowledge and intelligence we extract from the information."[73] The fact that rapidly emerging information technologies are creating "minutely detailed records" of our lives,[74] increasingly facilitating the "persistent, continuous and indiscriminate monitoring of our daily lives,"[75] the usefulness of IT is much too great for the IRS to ignore. In our emerging information age, every "day, rivulets of information [are] sifted, sorted, rearranged, and combined in hundreds of different ways," and can be "stream[ed] into electric brains" at the IRS.[76]

It is important to appreciate that the IRS is under significant pressure to improve its information collection and use. There is significant political pressure to close the significant gap between taxes legally owed and taxes timely collected.[77] This is $450

---

71. The National Taxpayer Advocate 2015 Annual Report has criticized the Future State initiative on several grounds, including concerns over information security. NAT'L TAXPAYER ADVOCATE, 2015 ANNUAL REPORT TO CONGRESS (2015), https://taxpayeradvocate.irs.gov/reports/2015-annual-report-to-congress/full-report [https://perma.cc/U7LE-MF2F].

72. Hatfield, *supra* note 38, at 340.

73. *Prepared Remarks of IRS Commissioner Doug Shulman to the Leaders & Legends Series, Johns Hopkins Carey Business School, Baltimore*, IRS (May 18, 2011), https://www.irs.gov/newsroom/prepared-remarks-of-irs-commissioner-doug-shulman-to-the-leaders-legends-series-johns-hopkins-carey-business-school-baltimore [https://perma.cc/EKU5-S8C7].

74. Hatfield, *supra* note 38, at 322, 339; Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934 (2013) (arguing increasing surveillance capacity undermines intellectual privacy and has a coercive element).

75. Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 274 (2013) (arguing that privacy harms should be understood in the lens of totalizing surveillance); *see also* Hatfield, *supra* note 38, at 322.

76. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1394 (2001) (arguing that the privacy harm of mass surveillance is best understood as a dehumanizing effect of bureaucratic information gathering); *see also* Hatfield, *supra* note 38, at 322, 339.

77. Hatfield, *supra* note 38, at 337–38; Michael Hatfield, *Privacy in Taxation*, 44 FLA. ST. U. L. REV. 579 (2017); Solove, *supra* note 76, at 1394; *see* OFFICE OF MGMT. & BUDGET,

billion shortfall is known as the "tax gap."[78] It is, in large part, an information gap: the difference between what the IRS knows about the taxpayer's activities and what the taxpayer and third parties know.[79] The pressure to close the tax gap is pressure to close this information gap, and the usefulness of IT for closing that gap is obvious.[80] Politicians, tax administrators, and scholars have focused on this technology,[81] and in a future in which both government agencies and private companies are pursuing the "growing gush of data" being generated by an ever-increasing number of internet-connected devices, the role of IT is certain to be expanded.[82]

A closely related pressure to increase the use of IT is the political pressure to reduce the compliance burden on taxpayers. This burden is the cost to taxpayers of attempting to determine and to report their tax liabilities in a timely manner.[83] The National Taxpayer Advocate estimates tax compliance takes over seven billion hours of time each year.[84] It is so daunting that over eighty percent of individuals pay either for a professional to prepare their returns or for computerized assistance.[85] The National Taxpayer Advocate, IRS Commissioners, and politicians have long been focused on reducing this burden.[86] Like the tax gap, the compliance burden is also

---

FISCAL YEAR 2013 BUDGET OF THE U.S. GOVERNMENT 84 (2012), https://www.gpo.gov/fdsys/pkg/BUDGET-2013-BUD/pdf/BUDGET-2013-BUD.pdf [https://perma.cc/ND7L-WYYZ].

78. Hatfield, *supra* note 77, at 3.

79. Hatfield, *supra* note 38, 332, 335–38. On the asymmetric nature of tax information in tax compliance, see Leandra Lederman, *Reducing Information Gaps To Reduce the Tax Gap: When Is Information Reporting Warranted?*, 78 FORDHAM L. REV. 1733, 1735–38 (2010). On the roles third parties play in tax compliance more generally, see Leandra Lederman, *Statutory Speed Bumps: The Roles Third Parties Play in Tax Compliance*, 60 STAN. L. REV. 695 (2007).

80. Hatfield, *supra* note 38, at 332, 335–38.

81. NAT'L TAXPAYER ADVOCATE, *supra* note 59, at 34; BARACK OBAMA'S COMPREHENSIVE TAX PLAN (2008), http://web.archive.org/web/20170422040822/http://halebobb.com/Obama/Factsheet_Tax_Plan_FINAL.pdf [https://perma.cc/2KXX-RFD6]; Hatfield, *supra* note 72, at 338; Hatfield, *supra* note 77, at 27–28; Jay A. Soled, *Call for the Gradual Phase-Out of All Paper Tax Information Statements*, 10 FLA. TAX REV. 345, 363–64 (2010) (calling for third parties to provide information to IRS website that taxpayers could use prepare returns, reducing burdens on both IRS and taxpayers); *Prepared Remarks of IRS Commissioner Doug Shulman to the Leaders & Legends Series, Johns Hopkins Carey Business School, Baltimore*, *supra* note 73; Richard Clarke, *Richard Clarke on the Future of Privacy: Only the Rich Will Have It*, WALL ST. J. (July 7, 2014), https://www.wsj.com/articles/richard-clarke-on-the-future-of-privacy-only-the-rich-will-have-it-1404762349 [https://perma.cc/85YA-QUNY].

82. RICK SMOLAN & JENNIFER ERWITT, THE HUMAN FACE OF BIG DATA (2012); Hatfield, *supra* note 38, at 339–42; Hatfield, *supra* note 77, at 20; Solove, *supra* note 76, at 1394.

83. *See* NAT'L TAXPAYER ADVOCATE, 2008 ANNUAL REPORT TO CONGRESS 3, 5 (2008), https://www.irs.gov/advocate/national-taxpayer-advocates-2008-annual-report-to-congress [https://perma.cc/B7B6-HK5X].

84. *Id.*

85. *Id.*

86. *See Tax Complexity, Compliance, and Administration: The Merits of Simplification in Tax Reform: Hearing Before the S. Comm. on Fin.*, 114th Cong. 1–2 (2015) (statement of Sen. Orrin Hatch, Chairman, S. Comm. on Fin.) (describing the costs of tax compliance as larger than the economy of New Zealand); *id.* at 2–5 (2015) (statement of Sen. Wyden,

an information problem.[87] Taxpayers have the burden to collect the relevant information, and then to inform themselves how the law applies to it, and then report their conclusions to the government. So, like the tax gap, the compliance burden problem seems best solved by IT.[88]

2. Tax Information

While it should be clear to even a casual observer why the IRS would pursue better information technology, it is not likely clear how much information the IRS needs. The IRS needs information on a great many individuals. There are about 145 million individual income tax returns filed annually,[89] reporting information on about 290 million individuals each year.[90] There is no other government agency that needs to collect information on so many individuals each year. In a country with a population of 328 million,[91] that figure represents nearly every individual in the country.

It is not just a great many individuals, but a great amount of information on many individuals that the IRS needs. The tax law can touch on almost any detail of life, making those details become tax relevant. As greatly important as financial information is, the range of tax relevant information is greater. Consider the nonfinancial information reported on the face of the Form 1040.[92] The return reveals not only the taxpayer's job and current address but whether or not the taxpayer has lost a job, prematurely invaded a retirement account, or moved fifty or more miles away.[93] It not only identifies any dependent who is a college student but also the dependent's college, course of study, length of time studying, and felony drug convictions.[94] Not only does the return reveal if the taxpayer is married but whether or not the spouse is blind or disabled, or if the taxpayer's spouse has

---

Ranking Member, S. Comm. on Fin.) (describing the tax returning filing process as painful); *Complexity and the Tax Gap: Making Tax Compliance Easier and Collecting What Is Due: Hearing Before the S. Comm. on Fin.*, 112th Cong. 1–3 (2011) (statement of Sen. Baucus, Chairman, S. Comm. on Fin.); NAT'L TAXPAYER ADVOCATE, *supra* note 83; *see also* Hatfield, *supra* note 38, at 337–38.

87. Hatfield, *supra* note 38, at 332–35.

88. *Id.* at 339.

89. This Article is focused on the taxation of individuals.

90. BRYAN, *supra* note 19, at 5.

91. *U.S. and World Population Clock*, *supra* note 20. The U.S. income tax is imposed on all United States Persons defined in I.R.C. § 7701(a)(30), which also includes residents of the country.

92. This is the most commonly filed individual income tax return.

93. I.R.S. Form 1040, U.S. Individual Income Tax Return Signature Block (occupation); Lines 15, 16, 20 (retirement benefits); Line 19 (unemployment benefits); Line 59 (early distributions from retirement accounts); Line 26 (moving expenses) [hereinafter I.R.S. Form 1040]; I.R.S. Form 3903, Moving Expenses; Hatfield, *supra* note 77, at 40–41.

94. I.R.S. Form 1040 Line 34 (tuition); I.R.S. Form 8863, Education Credits Line 22 (educational institution identifying information); Line 24 (study program and course load); Line 25 (more than four years post-secondary education); Line 26 (drug-related felony conviction); Hatfield, *supra* note 77, at 41.

recently died.[95] It reveals whether or not the taxpayer and dependents have health insurance or medical expenses.[96] It shows the number of children who live with the taxpayer and also shows the number of the taxpayer's children who live with someone else due to divorce or separation.[97] If the taxpayer has adopted a child, it reveals if the child has a disability, special needs, or is foreign born.[98] The return also shows whether the taxpayer has placed a child or disabled spouse in day care, and, if so, the name and address of the day care provider.[99]

Although all of this information is on the face of the return, far more information may be tax relevant and collected by the IRS. The IRS is authorized to demand whatever information it determines relevant to a tax liability.[100] The IRS need not suspect a taxpayer misreported any item or miscalculated a tax liability in order to demand more detailed information. As I have explained elsewhere, the more detailed information within the legal grasp of the IRS includes such detailed and deeply personal information as who sleeps how often in the taxpayer's house,[101] the taxpayer's

---

95. I.R.S. Form 1040, Lines 2, 4, and 5 (marital status); Lines 11 and 31a (alimony received and paid); Line 39a (blind spouse); I.R.S. Form 2441, Child and Dependent Care Expenses (Part 2 (identifying care recipient)); Hatfield, *supra* note 77, at 41.

96. I.R.S. Form 1040, Line 61 (health care coverage); Line 40 (itemized deductions); Schedule A, Itemized Deductions, Line 1 (medical and dental expenses); *see* Hatfield, *supra* note 77, at 41.

97. I.R.S. Form 1040, Line 6 (dependent children exemptions); Hatfield, *supra* note 77, at 41.

98. I.R.S. Form 8812, Additional Child Tax Credit; I.R.S. Form 1040, Line 54 (credits); I.R.S. Form 8839, Qualified Adoption Expenses (disability, special needs, or foreign birth of adopted child); Hatfield, *supra* note 77, at 41.

99. I.R.S. Form 2441, Child and Dependent Care Expenses (Part 1 (identifying care provider); Part 2 (identifying child or dependent)); Hatfield, *supra* note 77, at 41.

100. I.R.C. § 7602 (2012) (permitting the examination of books and records); I.R.C. § 7801 (granting authority to Treasury Department); I.R.C. § 7803 (Westlaw through Pub. L. 115-97) (outlining the duties and authority of the IRS Commissioner). With respect to this tax-relevant information, Congress has granted the Treasury broad authority to prescribe the taxpayer's obligations to provide the information. I.R.C. § 6001 (2012). The Secretary is entitled to require any person to "make such returns, render such statements, or keep such records as the Secretary deems sufficient to show whether or not such person" has an income tax liability, and every person who does have an income tax liability must "keep such records, render such statements, make such returns, and comply with such rules and regulations as the Secretary" prescribes. *Id.*; *see also* Treas. Reg. § 1.6001-1(a) (as amended in 1990); BORIS I. BITTKER, MARTIN J. MCMAHON, JR. & LAWRENCE A. ZELENAK, FEDERAL INCOME TAXATION OF INDIVIDUALS ¶ 39.01[8] (2013).

101. This information may be relevant to determining tax consequences of payments to a separated spouse who is living in the taxpayer's house and dependency status in the case of a child. *See* I.R.C. § 71(b)(1)(C) (2012) (defining alimony payments to a separated spouse who is in the same household as not excludable from income); I.R.C. § 152(c)(1)(B) (Westlaw through Pub. L. 115-97) (defining a qualifying child as a dependent residing at the same principal place of abode as the taxpayer for more than one-half of the year); Treas. Reg. § 1.152-1(b) (as amended in 1971) (defining the dependent including special circumstances of absences of less than six months); *see also* Hatfield, *supra* note 38, at 321 n.5.

hobbies,[102] reading preferences,[103] religious affiliation,[104] travel plans,[105] weight and his or her doctor's recommendations about it,[106] the taxpayer's or taxpayer's spouse's or dependent's abortion, sterilization,[107] gender identity disorder,[108] and sexual relations.[109] The IRS can even reach information about individuals who are not the taxpayer's spouse or dependents, such as the taxpayer's married children and the taxpayer's lovers (including, for example, letters between the taxpayer and her lover).[110]

3. Types of Future Attacks

To anticipate the types of attacks for which the IRS should be prepared, it is useful to review the types of attacks perpetrated against other organizations. The IRS has already been hit with financially motivated attacks, which may be the type of motivation we most often remember when we think of cyberattacks. Financially motivated cyberattacks are the use of new tools to commit old crimes, such as theft, fraud,

---

102. *See* Treas. Reg. § 1.183-2(b) (as amended in 1972) (listing factors for determining if an activity is a hobby for which losses are not deductible).

103. Reading habits may be relevant, for example, to determine whether one has undertaken an activity with a motive of making a profit. *See, e.g.*, Nickerson v. Comm'r, 700 F.2d 402, 407 (7th Cir. 1983) (stating that facts including a taxpayer's reading about farming were evidence that he pursued that activity with a profit-seeking motive).

104. Not only may financial support of religious organizations be tax relevant but also the distance from a taxpayer's home to any of her religious organizations. *See* I.R.C. § 170(b)(1)(A)(i) (Westlaw through Pub. L. 115-97) (covering charitable contributions and gifts to a church or convention or association of churches); Treas. Reg. § 1.121-1(b)(vi) (as amended in 2002) (stating that location of religious organization with which taxpayer affiliates is relevant to determining principal residence for gain exclusion).

105. For example, was the travel for personal, business, educational, or medical purposes—or some combination? *See* I.R.C. § 213(a), (d)(1)–(2) (Westlaw through Pub. L. 115-97) (stating that transportation and lodging expenses for medical care are deductible); Treas. Reg. § 1.162-2 (as amended in 1960) (covering travel for business, mixed business, and personal reasons); Treas. Reg. § 1.162-5(b) (as amended in 1967) (covering travel as a form of education).

106. *See* I.R.S. Priv. Ltr. Rul. 80-04-111 (Oct. 31, 1979) (setting out weight loss program fees as deductible where prescribed by physicians for the alleviation of specific ailments); Rev. Rul. 79-151, 1979-1 C.B. 116 (noting that weight loss program fees are not deductible even though physician-recommended where not prescribed for the alleviation of specific ailment).

107. *See* Rev. Rul. 73-201, 1973-1 C.B. 140 (deeming legal abortions and vasectomies deductible medical care under I.R.C. § 213).

108. *See, e.g.*, Rev. Rul. 2003-57, 2003-22 I.R.B. 959 (deeming breast reconstruction following mastectomy to be deductible). *But see* O'Donnabhain v. Comm'r, 134 T.C. 34, 70–71 (2010) (finding that hormone therapy and sex reassignment surgery are deductible expenses to treat "gender identity disorder" disease but that breast augmentation was merely cosmetic and not a deductible expense).

109. Transfers to a sexual partner may be characterized as either nontaxable gifts or as taxable compensation for sexual activity. *See, e.g.*, United States v. Harris, 942 F.2d 1125, 1131–35 (7th Cir. 1991) (reviewing the "current law on the tax treatment of payments to mistresses").

110. Hatfield, *supra* note 77, at 45–47.

and extortion.[111] The IRS has been attacked to steal refunds and taxpayer information, but it has yet to be hit with ransomware, which is an increasingly common malware. It restricts an organization's access to its own system or information (e.g., customers' orders or contact information) until the attacker is paid. For example, online casinos have been targeted with demands for payment and threats to disrupt their sites just as Super Bowl or World Cup betting began.[112] Imagine the information held by the IRS being held for ransom, just as April 16 began and individual taxpayers had just finished filing their return, payments, and claims for refunds.[113]

However, many breaches of cybersecurity are not financially motivated. For example, there may be an attack by an insider who has an idiosyncratic motive. Organizational insiders are especially worrisome as their position inside the organization allows access that outsiders would need a great deal of technical expertise to obtain.[114] Particularly dangerous to cybersecurity are the disgruntled insiders who seek revenge against the organization for personal wrongs.[115] For example, after he learned of his pending termination, a network administrator for the City of San Francisco held the city's computer systems hostage, preventing access to information, including police and payroll files.[116] While disgruntled insiders are a risk at any organization, the IRS has over 80,000 employees, who are overworked and underappreciated and difficult to retain,[117] and, as has been revealed recently, the IRS regularly fails to remove computer access privileges from former employees, including those subjected to disciplinary proceedings.[118] As the IRS increases its store of digital information, the risk of a disgruntled insider holding information hostage or disabling the IRS computer system also increases.

There also are politically motivated cyberattacks. These attacks, often by "hacktivists,"[119] such as Anonymous,[120] often make headline news and often are

111. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 22, at 4.

112. *See* P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 36, 88 (2014).

113. *See, e.g.*, Chris Frates, *IRS Believes Massive Data Theft Originated in Russia*, CNN POLITICS (June 4, 2015, 9:23 PM), http://www.cnn.com/2015/05/27/politics/irs-cyber-breach-russia [https://perma.cc/H3TS-36N8].

114. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 22, at 4.

115. *Id.*

116. Jaxon Van Derbeken, *Ex-S.F. Tech Guilty of Walling Off City System*, SFGATE (Apr. 28, 2010, 4:00 AM), http://www.sfgate.com/crime/article/Ex-S-F-tech-guilty-of-walling-off-city-system-3190937.php [https://perma.cc/5EAE-8ESG].

117. *See infra* Part II.C.

118. TREASURY INSPECTOR GEN. FOR TAX ADMIN., ACCESS TO GOVERNMENT FACILITIES AND COMPUTERS IS NOT ALWAYS REMOVED WHEN EMPLOYEES SEPARATE 1–3 (2016).

119. The first use of this term is often credited to the Cult of the Dead Cow, a group whose name reflects its operation's headquarters in an old slaughterhouse in Lubbock, Texas. Their early efforts included hacking "Chinese government agencies and Western companies cooperating with them" as part of their dedication to fighting internet censorship. SINGER & FRIEDMAN, *supra* note 112, at 77.

120. Anonymous's headline attacks (on religious groups, large corporations, and foreign governments) and Guy Fawkes masks probably make them the best-known hacktivists in the world. *Id.* at 78, 80–84; *see also Anonymous Activist Forum*, WHYWEPROTEST, https://whyweprotest.net [https://perma.cc/EWC3-HKRK].

against high profile targets. Government, corporations, human rights organizations, and religious groups have all been attacked for political purposes.[121] Over 100,000 Russian hacktivists launched a denial-of-service attack against the Estonian government for removing a Russian grave marker.[122] Iranian hacktivists attacked a U.S. business for its owner's political support of Israel.[123] About 100,000 Chinese hacktivists knocked out the White House website and planted viruses in the Justice Department's network in retaliation for a collision of U.S. and Chinese planes.[124] Imagine the IRS as the target of a politically motivated attack such as a massive denial of service.[125] There is quite a history of anti-IRS sentiment: anti-IRS activists have attacked IRS property, stolen files, threatened IRS employees, and even killed IRS employees in the past.[126] Given the visibility of the IRS, and both its symbolic and practical role of revenue collection for the federal government, it is easy to imagine an attack against the IRS motivated by antipathy to the IRS or to U.S. foreign or other policies.

While politically motivated attacks may attempt to embarrass a government, impede its functioning, and frustrate its citizens, politically motivated breaches also may be aimed at securing and disclosing certain information. For example, Edward Snowden stole 1.7 million records from the National Security Agency (NSA) —records with more top secrets than had ever been stolen from the U.S. government—in order to disclose politically objectionable behavior by the NSA.[127]

---

121. SINGER & FRIEDMAN, *supra* note 112, at 78, 80–84; *see also Anonymous Activist Forum*, *supra* note 120; *Significant Cyber Incidents*, CTR. FOR STRATEGIC & INT'L STUD., https://www.csis.org/programs/strategic-technologies-program/cybersecurity/significant-cyber-events [https://perma.cc/FH5A-RS6N].

122. SINGER & FRIEDMAN, *supra* note 112, at 111.

123. *Significant Cyber Incidents Since 2006*, CTR. FOR STRATEGIC & INT'L STUD., https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Significant_Cyber_Events_List.pdf [https://perma.cc/RU2W-7ZMD] (2014 Las Vegas incident).

124. SINGER & FRIEDMAN, *supra* note 112, at 78.

125. A "denial-of-service" attack is one that impairs the authorized use of a system. It is an intentional overwhelming of a system so that authorized users are unable to access it. It is as if someone were so persistently dialing your phone number, no one could get a call through to you. Except, of course, it is not merely a single user's phone number that is taken out of service, but all of a bank's customers' access, for example. These attacks often are a coordinated effort of many individual attackers. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 22, at 5; SINGER & FRIEDMAN, *supra* note 112, at 44.

126. Michael Brick, *Man Crashes Plane into Texas I.R.S Office*, N.Y. TIMES (Feb. 18, 2010), http://www.nytimes.com/2010/02/19/us/19crash.html [https://perma.cc/C2DP-RBPZ]; Benedict Carey, *When Does Political Anger Turn to Violence?*, N.Y. TIMES (Mar. 27, 2010), http://www.nytimes.com/2010/03/28/weekinreview/28carey.html [https://perma.cc/GC96-W7UY]; Joe Weisenthal, *The Insane Manifesto of Austin Texas Crash Pilot Joseph Andrew Stack*, BUS. INSIDER (Feb. 18, 2010, 1:11 PM), http://www.businessinsider.com/joseph-andrew-stacks-insane-manifesto-2010-2 [https://perma.cc/88HA-UBGE]; Robert W. Welkos & Joel Sappell, *Burglaries and Lies Paved a Path to Prison*, L.A. TIMES (June 24, 1990), http://www.latimes.com/local/la-scientologysidec062490-story.html [https://perma.cc/UMN9-JBDD].

127. Chris Strohm & Del Quentin Wilber, *Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers*, BLOOMBERG (Jan. 10, 2014, 1:01 PM), http://www.bloomberg.com/news

While IRS operations do not have the top political secrecy the NSA's operations do, some of its operations raise significant political objections. For example, consider the ongoing saga of the IRS review of Section 501(c)(4) applications by right-leaning groups in the United States, which has led to a finding against the IRS in court,[128] the resignation of key IRS employees,[129] bills intended to slash IRS power, and a push for the impeachment of the IRS commissioner.[130] In addition to information on IRS activities, the IRS, of course, has a great deal of information on taxpayers that may be of political interest. Consider, for example, how the disclosure of the compensation paid by Sony followed the 2014 cyberattack against Sony and the damage to Sony that followed the disclosure.[131] This type of information is readily held by the IRS, as is information as to the tax liabilities of the wealthy, the powerful, and the controversial—and, potentially, information on their health, families, and various activities, as described in more detail below.

Another type of cyberattack is one intended to affect the political process. There have been hacks of political parties and political campaigns with the intention of finding and disclosing embarrassing information.[132] That these attacks appear to have been organized and conducted from outside the United States underscores the rapidly changing nature of cyberattacks.[133] The use of tax information against political enemies by government insiders is not unknown in the United States, though concerns over this use led to greater legal protection for tax information.[134] With tax information increasingly digitized and vulnerable to cyber theft, legal protection is not real protection, and the threat is not just by those within the government or even within the United States who might seek tax information on political adversaries. This may be tax information of individual candidates who refuse voluntary revelation,[135] or it may be other information contained in tax records that reveal relationships among taxpayers not otherwise public or other details of a targeted taxpayer's personal or family life.

/articles/2014-01-10/pentagon-says-snowden-took-most-u-s-secrets-ever-rogers [https://perma.cc/7MET-CAZR].

128. True the Vote, Inc. v. IRS, 831 F.3d 551 (D.C. Cir. 2016).

129. Josh Hicks, *Central Figure in IRS Tea Party Controversy Resigns*, WASH. POST (Sept. 23, 2013), https://www.washingtonpost.com/politics/federal_government/central-figure-in-irs-tea-party-controversy-resigns/2013/09/23/db0d3d28-248a-11e3-b75d-5b7f66349852_story.html [https://perma.cc/B7Z5-RU8L].

130. Paul Caron, *The IRS Scandal, Day 1108*, TAXPROF BLOG (May 21, 2016), http://taxprof.typepad.com/taxprof_blog/2016/05/the-irs-scandal-day-1108.html [https://perma.cc/KD4V-SQ9C].

131. *Sony To Pay Staff $8M Compensation over Cyber Attack,* BBC (Nov. 26, 2015), https://www.bbc.com/news/entertainment-arts-34931148 [https://perma.cc/6WCY-C7JD].

132. David E. Sanger & Nick Corasaniti, *D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump*, N.Y. TIMES (June 14, 2016), http://nyti.ms/1S4a1Dw [https://perma.cc/DGR4-VDS8].

133. David E. Sanger & Eric Schmitt, *Spy Agency Consensus Grows that Russia Hacked D.N.C.*, N.Y. TIMES (July 26, 2016), http://nyti.ms/29Yfv9A [https://perma.cc/M848-7MCL].

134. *See generally* Hatfield, *supra* note 77.

135. David Barstow, Susanne Craig, Russ Buettner & Megan Twohey, *Donald Trump Tax Records Show He Could Have Avoided Taxes for Nearly Two Decades, The Times Found*, N.Y. TIMES (Oct. 1, 2016), http://nyti.ms/2d51X9E [https://perma.cc/983X-QF6U].

Cyberattacks can cross into physical attacks. The Department of Homeland Security has reported the U.S. electrical grid has been persistently probed by unauthorized foreign actors and that twenty-three gas pipeline companies have had information stolen, presumably for sabotage purposes.[136] The energy sectors in Spain, France, Italy, Turkey, and Poland have all been hacked.[137] Concerns over physical destruction waged through IT have motivated governments to develop information warfare programs and capabilities.[138] The most high-profile instance of such an attack is Stuxnet, a worm that destroyed centrifuges at an Iranian nuclear facility.[139] Stuxnet was extraordinarily sophisticated and powerful, and apparently an intensive collaborative effort of the United States and Israel to produce a unique weapon with a unique purpose.[140] While it is unlikely weapons like Stuxnet will soon become common, its development was "the absolute game changer" in global security.[141] It bought the world into "an arms race where countries start stocking weapons, only it isn't planes and nuclear reactors they're stocking, but it's cyberweapons."[142]

What would be the equivalent of such an attack through the IRS? Cybersecurity experts have warned of attacks on a nation's economy.[143] An attack on the U.S. economy easily can be imagined. A short-term denial-of-service attack on the IRS, as mentioned above, would not only have symbolic consequences but would cost taxpayers and the IRS time, money, and frustration. But imagine the consequences of taking the IRS "offline" for months, not hours. Imagine an adversary targeting not the utilities infrastructure of the United States but the U.S. revenue collection infrastructure. While terrorists brought down the World Trade Center on 9/11, the IRS could be a "Cyber 9/11" target, taking it down would be taking down revenue collection and stirring up chaos by destroying data evidencing payments, filings, and all other taxpayer information.

Cyber weapons like Stuxnet achieve the ages-old war goal of physical destruction, merely using information technology as a new method. However, the rapidly expanding power of IT has produced new war goals that are more complex and more difficult to discern. One such goal is stealing as much data as can be stolen. Once massive data is stolen, the attacker can then use cutting-edge, "big data" algorithms to mine

---

136. Mark Clayton, *Exclusive: Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage*, CHRISTIAN SCI. MONITOR (Feb. 27, 2013), http://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage [https://perma.cc/63BS-MFYB]; Michael Riley & Jordan Robertson, *UglyGorilla Hack of U.S. Utility Exposes Cyberwar Threat*, BLOOMBERG (June 13, 2014, 5:01 PM), http://www.bloomberg.com/news/articles/2014-06-13/uglygorilla-hack-of-u-s-utility-exposes-cyberwar-threat [https://perma.cc/59FT-EZF6].

137. *Energy Firms Hacked by 'Cyber-Espionage Group Dragonfly,'* BBC (July 1, 2014), https://www.bbc.com/news/technology-28106478 [https://perma.cc/N8LN-H6CY].

138. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 15-573T, CYBERSECURITY: ACTIONS NEEDED TO ADDRESS CHALLENGES FACING FEDERAL SYSTEMS 2 (2015).

139. SINGER & FRIEDMAN, *supra* note 112, at 114–18.

140. *Id.* at 117–18.

141. *Id.* at 118 (quoting Mikko Hypponen).

142. *Id.* (quoting Mikko Hypponen).

143. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 4; Dan Holden, *Is Cyber-Terrorism the New Normal?*, WIRED (Jan. 2015), http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal [https://perma.cc/TZS4-6T57].

usefulness from the information. The Chinese government has been said to organize its hackers into a "vacuum cleaner" to suck up electronic information for big data mining.[144] The Chinese government is also said to be "becoming much more sophisticated in tying" data together in useful ways.[145] Both the theft of data on four million government employees from the OPM and tens of millions individuals whose health care was insured by Anthem were part of the Chinese government's effort, as have been many other big data thefts.[146] The Chinese government's goal appears to be building "massive databases of Americans' personal information."[147] Among other uses of the data may be identifying potential intelligence targets within the United States, as well as their weaknesses, histories, and personal relationships and identifying individuals within China who have relationships with Americans.[148] If the current stores of information held by the IRS are the "gold standard" for cyber thieves, a future in which the IRS pursues cutting-edge IT, rather than being tied to magnetic tapes, as it currently is,[149] tax account information will be even more appealing. A single agency would house sensitive information on almost everyone in the country.

But vacuum cleaner attacks are not the cutting-edge of cyberattacks. The cutting-edge is not stealing the data but manipulating it.[150] Intelligence experts believe that this is a far greater risk than the use of cyber weapons.[151] This "data sabotage" may be used to affect the decisions of corporate executives, investors, and government officials.[152] As damaging as it might be for an adversary to take down the IRS, or to steal all the information held by the IRS, a cutting-edge cyberattack would be an adversarial power controlling the IRS by manipulating its data. Such control could wreak havoc not only on the taxpayers involved and the IRS itself, but reverberate economically and politically, undermining not only taxpayer confidence and the ability of the IRS to collect revenue but also the confidence of Americans in the federal government's ability to function.

II. THE IRS WILL FAIL TO IMPLEMENT ADEQUATE CYBERSECURITY

There are several reasons to predict the IRS will fail to develop adequate cybersecurity. One reason, explained in Part II.A, is the IRS's poor track record improving its technology over the past forty years. As explained in Part II.B, another reason is expecting the IRS to be underresourced indefinitely. Part II.C outlines a third reason to doubt: it is unlikely the IRS can recruit and retain the needed technical expertise. As discussed in Part II.D, a fourth reason to predict IRS failure is that

144. Nakashima, *supra* note 15.

145. *Id.*

146. *See id.*

147. *Id.*

148. *See id.*

149. *See infra* notes 157–67.

150. This is according to the former U.S. director of national intelligence, James Clapper, and the director of the NSA, Admiral Michael Rogers. Ackerman, *supra* note 17.

151. *Id.*

152. Maggie Overfelt, *The Next Big Threat in Hacking—Data Sabotage*, CNBC (Mar. 9, 2016, 6:56 AM), http://www.cnbc.com/2016/03/09/the-next-big-threat-in-hacking--data-sabotage.html [https://perma.cc/Y5KC-GU9Y].

success would require a system used not only by the tens of thousands of IRS employees but hundreds of millions of taxpayers, third-party reporters, and outside professionals. Finally, the fifth reason to doubt is set forth in Part II.E: cybersecurity is too difficult for most organizations, and no organization does what the IRS does—annually process hundreds of millions of returns, pay hundreds of billions of refunds, and collect trillions in payment.

A. Very Poor History of Improving Technology

The IRS history with computerization began very early, at the close of World War II. What in 1917 had been an income tax requiring only 3.5 million individual returns to be filed[153] had, as a result of funding World War II, become a tax on 42.6 million.[154] The difficulties of tracking 42 million taxpayers prompted the IRS[155] to begin experimenting with automation in 1948.[156] Ten years later, the IRS formalized its plan for "Automated Data Processing" (ADP).[157] The ADP plan was for regional centers to record tax information onto magnetic tape, which would then be posted once a week to a "National Computer Center" in Martinsburg, West Virginia, that would house mainframes with a master file on each taxpayer (the "IMF system"). Within five years, ADP was operating,[158] and in fewer than ten years—that is, by 1967—was fully implemented: every tax return was handled through ADP and the National Computer Center maintained a master file on every taxpayer.[159] The IRS then began pursuing significant improvements: using keyboards to transcribe data

153. INTERNAL REVENUE SERV., IRS HISTORICAL FACT BOOK: A CHRONOLOGY 91 (1993).

154. W. ELLIOT BROWNLEE, FEDERAL TAXATION IN AMERICA: A SHORT HISTORY 115 (2004).

155. The IRS was at the time known as the Bureau of Internal Revenue (BIR).

156. Sheldon S. Cohen, *Automation and Tax Administration*, 28 OHIO ST. L.J. 69, 69 (1967) (arguing that automation in tax administration facilitates the IRS's ability to effectively and accurately administer the tax code); Robert L. Jack, *Internal Revenue Service Automatic Data Processing System and Its Significance to Taxpayers and Their Representatives*, 8 JURIMETRICS J. 1, 2 (1966) (arguing that the automation in data processing benefited the IRS's capacity, while noting some problems). In 1948, return processing was essentially as had it been in 1862 (when first federal income tax had been introduced). Bryan T. Camp, *Theory and Practice in Tax Administration*, 29 VA. TAX REV. 227, 246 (2009) (arguing that automation in tax administration gave rise to new problems for the IRS such as centralization and insufficient personnel to effectively serve). The BIR began experimenting with automation by first automating mass mailing with a punch card system. INTERNAL REVENUE SERV., *supra* note 153, at 143.

157. The 1958 plan followed a 1955 experiment in which over a million returns were processed with computers. These returns were Form 1040As filed in the Omaha Region. INTERNAL REVENUE SERV., *supra* note 153, at 161. Also, by 1958, the IRS was using a computer shared with the Bureau of the Census for compiling statistics. *Id.* at 161, 163–64. Congress approved ADP in 1959. *Id.* at 166, 174; Camp, *supra* note 156, at 243.

158. By 1962, ADP was processing business returns. INTERNAL REVENUE SERV., *supra* note 153, at 176; Cohen, *supra* note 156, at 69.

159. Mortimer M. Caplin, *Commissioner Caplin Reviews His Record as IRS Chief*, 29 VA. TAX REV. 177, 178 (2009); Cohen, *supra* note 156, at 69–70.

directly to tape;[160] implementing algorithms to identify returns with a high probability of error;[161] using computers to determine how to improve compliance and collection;[162] developing ways for forms to be submitted on magnetic tape;[163] automating deposit and payments;[164] and even experimenting with IRS employees using microcomputers to prepare returns for taxpayers while they waited.[165] IRS computer operations were held out as an example for the private sector,[166] and foreign governments sought IRS help in moving their systems toward computerization.[167]

Buoyed by a successful first decade of computerization, the IRS set out to transform its system.[168] In 1975, the plan for transformation—the Tax Administration System (TAS)—was approved for implementation.[169] TAS focused on improving how taxpayer accounts would be developed and maintained, computerizing applications used by agents, reducing errors, and smoothing audits.[170] But the plan quickly fell to Watergate-era political anxieties about the inappropriate use of private information held by the IRS.[171] There was no political appetite for increasing the computerization of the IRS; Congress was only willing to fund the replacement of old equipment, not the upgrade.[172]

Within a decade of announcing TAS, computerization at the IRS was in shambles. The 1985 filing season was the worst in IRS history: insufficient computer capacity tanked taxpayer service.[173] It was a technological, public relations, and political disaster.[174] The Treasury Department rejected IRS requests for additional funding for

---

160. Herman J. Rothberg, *A Study of the Impact of Office Automation in the IRS*, 92 MONTHLY LAB. REV. 26, 30 (1969).

161. Singleton B. Wolfe, *The Use of Computers in Tax Administration*, 17 JURIMETRICS J. 215, 215 (1977); *see also* INTERNAL REVENUE SERV., *supra* note 153, at 191.

162. Cohen, *supra* note 156, at 72.

163. Magnetic tape reporting was used by 591 entities in 1966. INTERNAL REVENUE SERV., *supra* note 153, at 183; Jack, *supra* note 156, at 6–7.

164. INTERNAL REVENUE SERV., *supra* note 153, at 197.

165. The four sites were Boston, Brooklyn, Philadelphia, and Washington; at two other sites, the IRS offered to taxpayers a review of their returns for accuracy before they were filed. *Id.* at 201.

166. *See* Rothberg, *supra* note 160, at 26.

167. *See, e.g.*, INTERNAL REVENUE SERV., *supra* note 153, at 176.

168. *Id.* at 191.

169. *Id.* at 191, 207.

170. *Id.* at 191; Elana Varon, *E-Government: IRS Modernization—Will Third Time Be the Charm?*, CIO (Apr. 1, 2001, 8:00 AM), http://www.cio.com/article/2441695/process-improvement/e-government--irs-modernization--will-third-time-be-the-charm-.html [https://perma.cc/PG3G-VDTL].

171. After Nixon's political use of the IRS, there were hearings on the use of executive orders, which Nixon then revoked. The political climate at the time was concerned with the vast gathering of information, and eventually led to the 1974 Privacy Act. *See* INTERNAL REVENUE SERV., *supra* note 153, at 212; Hatfield, *supra* note 77.

172. This was known as the Equipment Replacement Program (ERP). INTERNAL REVENUE SERV., *supra* note 153, at 212–13.

173. *Id.* at 215, 223; Varon, *supra* note 170.

174. INTERNAL REVENUE SERV., *supra* note 153, at 215.

modernizing its technology on grounds that the IRS had no comprehensive modernization plan.[175]

In 1988, over twenty years after ADP had been fully implemented, the IRS formalized a comprehensive modernization plan: the Tax System Modernization plan (TSM).[176] The primary goal of TSM was to replace the 1960s IMF system at the National Computing Center with a state-of-the-art network.[177] In pursuit of this state-of-the-art network, the IRS quickly spent $4 billion.[178] Unfortunately, the systems the IRS developed "d[id] not work in the real world."[179] As a result, Congress cut funding for TSM,[180] and the President appointed an IRS commissioner with a high-tech, business background.[181] In describing the situation with IRS technology at this time, one former IRS executive said the IRS had spent billions of dollars in order to rebuild a 1960 Chevy.[182] The IRS system still relied on "a series of very large tape files—virtually unheard of" as still being used in the late 1990s.[183] Except for a small amount of data that had been put on separate integrated data retrieval system for use by frontline employees,[184] taxpayer data could not be accessed or updated on a real-time basis.[185] Once a week, in a process that took three days, taxpayer data was updated at the National Computing Center.[186]

In 1997, the new commissioner launched a new, $7 billion plan: Business Systems Modernization (BSM).[187] The plan included replacing the thirty-five-year-old magnetic tape system at the National Computing Center with a modern database, the Customer Account Data Engine (CADE).[188] This was the third major plan in twenty

---

175. *See id.* at 223.

176. *Id.* at 230, 236.

177. Varon, *supra* note 170.

178. Zach Noble, *The Taxman's Tech Troubles*, FCW (Apr. 8, 2016), https://fcw.com/articles/2016/04/08/taxman-tech-troubles.aspx [https://perma.cc/VQ5E-BQVA].

179. *Id.*

180. Congress cut the funding in 1995. James R. Thompson, *Fixing the IRS*, GOV'T EXECUTIVE (Apr. 1, 2012), http://www.govexec.com/magazine/features/2012/04/fixing-irs/41637 [https://perma.cc/2YMR-FA6A].

181. Charles Rossotti was appointed in 1997. George Guttman, *The IRS: Still Trying To Modernize, 30 Years Later*, 86 TAX NOTES 723, 725 (2000).

182. *Id.* at 726.

183. Charles O. Rossotti, *Modernizing the IRS*, 1 J. TAX PRAC. & PROC. 17, 21 (1999).

184. This information was stored on the Integrated Data Retrieval System (IDRS). Guttman, *supra* note 181, at 725.

185. *Id.*

186. *See* Rossotti, *supra* note 183, at 21.

187. James R. Thompson, *System Error*, GOV'T EXECUTIVE (Sept. 1, 1996), https://www.govexec.com/magazine/1996/09/system-error/405 [https://perma.cc/P2GS-VRX2]. BSM was a fifteen-year plan, intended to phase in the modern database, beginning with the simplest of taxpayer accounts (a subset of Form 1040EZ filers) in 2002. *See* INTERNAL REVENUE SERV., BUSINESS SYSTEMS MODERNIZATION PROGRAM PROGRESS REPORT 8, 9, 33, (2000), https://www.irs.gov/pub/irs-utl/bsm-prog.pdf [https://perma.cc/JJL2-CKHN]. For a discussion of the political context of the reforms at the IRS in the 1990s, see Leandra Lederman, *Tax Compliance and the Reformed IRS*, 51 U. KAN. L. REV. 971 (2003).

188. INTERNAL REVENUE SERV., *supra* note 187, at 6.

years to update the National Computing Center.[189] However, unlike the other plans, the new commissioner's plan relied not on inside but outside tech experts.[190] But, due to both IRS management failures and the failures of the outside tech experts to understand the IRS processes, the BSM was soon behind schedule and over budget, prompting the Government Accountability Office to conclude that the BSM was too ambitious for the IRS to pursue.[191]

In 2008, almost a decade after the new commissioner announced BSM, the IRS had a new commissioner who scaled down the other aspects of BSM so as to have a single goal: fully implementing CADE.[192] While some progress had been made with CADE,[193] the 1960s IMF system at the National Computing Center remained the center of IRS computing,[194] decades after other organizations had begun using modern databases.[195] Despite the single focus, over the next few years, the budget for CADE was exceeded and the goals for CADE were lowered.[196] Some progress was made, including enabling the daily rather than weekly processing and posting of some information.[197] But project delays and cost overruns continued.[198]

By 2016, CADE was still not fully implemented and the push to fully replace the IMF system at the National Computing Center had slowed.[199] Sounding resigned, the technical director for strategic planning at the IRS described the system in 2016 as "not broken" but "difficult to maintain."[200] Describing a system developed piecemeal over the prior fifty years, the IRS commissioner said, "We've got more IT challenges than you can shake a stick at . . . [we have] literally thousands of patches [and] security upgrades [and] we don't have the resources to implement them all."[201] With so many problems, the IRS could not focus on fully implementing CADE. Even though the IRS technology budget had reached $2.4 billion—over 20% of its total annual budget—both its focus and its budget were on nineteen separate, "major" investments.[202] CADE was competing with projects to implement the Affordable Care

189. *See* Guttman, *supra* note 181, at 725.

190. INTERNAL REVENUE SERV., *supra* note 187, at 8.

191. Thompson, *supra* note 180; *see also* INTERNAL REVENUE SERV., PROGRESS REPORT 33–34 (2001), https://www.irs.gov/pub/irs-utl/pub3970_2-2002.pdf [https://perma.cc/T8QG-M5PF].

192. The new IRS commissioner was Doug Shulman. Thompson, *supra* note 180.

193. Some progress had been made: about fifteen million of the simplest tax returns were being processed with CADE in 2008. Noble, *supra* note 178.

194. Thompson, *supra* note 180.

195. *Id.*; *see also* Brianna Ehley, *The IRS's Unusual IT 'Success Story' Is Failing*, FISCAL TIMES (Nov. 26, 2013), http://www.thefiscaltimes.com/Articles/2013/11/26/IRS-s-One-IT-Success-Story-Failing [https://perma.cc/S9MQ-4CTP].

196. *See* Jack Moore, *When IRS Tech Projects Start To Slip, Congress Is the Last To Know*, NEXTGOV (Mar. 2, 2015), http://www.nextgov.com/cio-briefing/2015/03/when-irs-tech-projects-start-slip-congress-last-know/106449.

197. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 28, at 3–4.

198. Moore, *supra* note 196.

199. By 2016, it was CADE 2. Noble, *supra* note 178.

200. *Id.*

201. *Id.*

202. Each of these cost at least $10 million annually. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 28, at 3.

Act[203] and the Foreign Account Tax Compliance Act;[204] "to eliminate the issuance of fraudulent tax refunds";[205] to provide web-based services to taxpayers, support electronic filing, convert paper returns into electronic format;[206] and a dozen other major projects, including, of course, funding the maintenance of the magnetic tapes and mainframes at the National Computing Center.[207] Moreover, "[o]f all the federal agencies, IRS [was] maybe suffering the most in terms of an IT backlog."[208] The backlog, patched system, and lack of focus mean that even routine IT maintenance goals fail to be met. For example, between 2011 and 2015, the IRS spent $139 million to update its workstations from Windows 2003 to Windows XP—and failed.[209]

While the history of technology modernization at the IRS does not inspire confidence for its future, there have been some successes. Indeed, until the 2015 cyberattacks, the public-facing technology used by the IRS was largely a success story.[210] Over 125 million returns are now filed electronically,[211] which is 86% of the total individual returns filed.[212] This can be attributed to the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA),[213] which required that the IRS develop ways for taxpayers to access their accounts online and file tax returns electronically.[214] It mandated that 80% of all returns be filed electronically within a decade,[215] and that, more generally, the IRS "convert its interactions with taxpayers and practitioners to electronic form as rapidly as possible."[216] It also established a special funding mechanism for these efforts[217] and charged the Treasury Inspector General for Tax Administration with annually evaluating the IRS's progress.[218] With the RRA, Congress forced prioritization of public-facing technology.[219] Politically, this was understandable, as it responded to massive complaints about difficulties interacting with the IRS. And, practically, the most significant positive developments in IRS IT have been with the electronic filing mandated by Congress.[220] But Congress's decision about technology also meant a de-prioritization of the technology used by the

---

203. Noble, *supra* note 178.
204. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 28, at 3–4.
205. *Id.* at 4.
206. *Id.*
207. *See id.*
208. Noble, *supra* note 178 (quoting Rep. Gerry Connolly (D-VA)).
209. TREASURY INSPECTOR GEN. FOR TAX ADMIN., *supra* note 27, at 2.
210. Noble, *supra* note 178.
211. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-151, 2015 TAX FILING SEASON: DETERIORATING TAXPAYER SERVICE UNDERSCORES NEED FOR A COMPREHENSIVE STRATEGY AND PROCESS EFFICIENCIES 28 (2015).
212. *Id.*
213. Guttman, *supra* note 181, at 725.
214. Varon, *supra* note 170.
215. Thompson, *supra* note 180.
216. INTERNAL REVENUE SERV., *supra* note 187, at 21.
217. *Id.* at 3.
218. TREASURY INSPECTOR GEN. FOR TAX ADMIN., NO. 2005-20-102, ANNUAL ASSESSMENT OF THE BUSINESS SYSTEMS MODERNIZATION PROGRAM 1 (2005).
219. INTERNAL REVENUE SERV., *supra* note 187, at 3, 21; Guttman, *supra* note 181, at 725; Thompson, *supra* note 180; Varon, *supra* note 170.
220. Noble, *supra* note 178; Thompson, *supra* note 180.

IRS to process returns, payments, and refunds. Public-facing programs like electronic filing have been something of a façade, obscuring the greater technological needs of the IRS. But the façade is no longer obscuring these needs. It is the electronic filing program that enables the filing of fraudulent returns with payments made to criminals' bank accounts.[221] And it was the Get Transcript program that enabled criminals to steal personal information to sell, to use in other crimes, and to file even "better" fraudulent returns in the future.[222]

B. Inadequate Funding

In 2016, the House Appropriations Committee approved cutting the IRS budget to lower than its 2008 level.[223] Given recent funding cuts, this was not much of a surprise.[224] While IRS funding has been decreasing, its work load has been increasing. The number of tax returns has increased,[225] as has the number of tasks assigned the IRS by Congress, such as its duties implementing the Affordable Care Act.[226] Concern over the funding cuts, especially their negative impacts on individual taxpayers, has been widely expressed. The IRS Oversight Board,[227] the National Taxpayer Advocate,[228] the IRS Advisory Council,[229] the Treasury Inspector General for Tax Affairs,[230] and tax scholars[231] have pointed to the serious problems caused

---

221. *See supra* notes 62–65 and accompanying text.

222. *See supra* notes 62–65 and accompanying text.

223. Press Release, U.S. House of Representatives Comm. on Appropriations, Appropriations Committee Releases Fiscal Year 2017 Financial Services Bill (May 24, 2016), http://appropriations.house.gov/news/documentsingle.aspx?DocumentID=394563 [https://perma.cc/F6ST-LQB5]; Naomi Jagoda, *House Panel Votes To Cut IRS Funding*, HILL (June 9, 2016, 2:47 PM), http://thehill.com/policy/finance/282916-house-panel-approves-bill-that-cuts-irs-funding [https://perma.cc/BX39-W33Z].

224. *See* NAT'L TAXPAYER ADVOCATE, 2014 ANNUAL REPORT TO CONGRESS vii (2014); Jonathan Barry Forman & Roberta F. Mann, *Making the Internal Revenue Service Work*, 17 FLA. TAX REV. 725, 764 (2015).

225. NAT'L TAXPAYER ADVOCATE, *supra* note 224, at 9–10; Forman & Mann, *supra* note 224, at 763–64.

226. NAT'L TAXPAYER ADVOCATE, *supra* note 224, at 12; Forman & Mann, *supra* note 224, at 774.

227. *See, e.g.*, IRS OVERSIGHT BD., FY 2015 IRS BUDGET RECOMMENDATION SPECIAL REPORT 11 (2014).

228. *See, e.g.*, NAT'L TAXPAYER ADVOCATE, 2013 ANNUAL REPORT TO CONGRESS ix, 21 (2013).

229. *See, e.g.*, INTERNAL REVENUE SERV. ADVISORY COUNCIL 2014 PUBLIC REPORT 9 (2014), https://www.irs.gov/pub/irs-utl/2014-IRSAC-Full-Report.pdf [https://perma.cc/BGT7-WDM5].

230. *See, e.g.*, TREASURY INSPECTOR GEN. FOR TAX ADMIN., NO. 2014-10-025, IMPLEMENTATION OF FISCAL YEAR 2013 SEQUESTRATION BUDGET REDUCTIONS 9 (2014).

231. *See, e.g.*, Forman & Mann, *supra* note 224, at 763–72; Leandra Lederman, *The IRS, Politics, and Income Inequality*, 150 TAX NOTES 1329, 1329 (2016); Bryan Camp, *Overlooked Costs of IRS Budget Cuts Will Hit Taxpayers Hardest*, CONVERSATION (Apr. 14, 2015, 5:49 AM), https://theconversation.com/overlooked-costs-of-irs-budget-cuts-will-hit-taxpayers-hardest-39762 [https://perma.cc/QLS7-N6N9].

by so limiting the resources for the IRS. But with many members of Congress convinced that reducing funding will increase efficiency,[232] no one is predicting funding will be increasing. At this point, funding has so decreased that it would require a significant increase to return future funding to past levels.

Given that—despite billions spent[233]—the IRS already has more information technology problems "than you can shake a stick at"[234] and suffers the greatest IT backlog of all federal agencies,[235] it is most unlikely that it will be able to meet its cybersecurity needs without an extraordinary increase in funding specifically for the task. That seems extraordinarily unlikely. In the current bill approved by the House Appropriations Committee, there is $290 million specifically set aside as additional spending on cybersecurity, customer service, and fraud prevention.[236] While cybersecurity is related to customer service and fraud prevention, to lump these three together spotlights the absence of congressional concern to push the cybersecurity for tax information to a cutting-edge state. It is also not encouraging to recognize that the $290 million is about twice what the IRS spent trying and failing to upgrade from Windows 2003.[237] Even if Congress were willing to write the checks, there is no reason to believe the IRS would use the money successfully.

C. Inability To Recruit and Retain Experts

A third reason to doubt the IRS will be able to provide adequate cybersecurity is that it is unlikely to recruit and retain the needed experts. In general, the IRS has significant personnel problems. In 2014, it employed a total of 91,018 employees, which is about the same level as in the 1970s. Between 2011 and 2015, the agency lost 18,138 employees—a decline of 16.7%.[238] Its employees are overworked, overwhelmed, and miserable.[239] The IRS especially struggles to recruit and retain its most

---

232. *See, e.g.*, Colleen Murphy, *House Appropriations Bill Cuts IRS Funding by $236 Million*, BLOOMBERG BNA (May 25, 2016), http://www.bna.com/house-appropriations-bill-n57982072964 (Representative Ander Crenshaw criticized the agency as inefficient and for "a history of inappropriate behavior").

233. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 2.

234. Noble, *supra* note 178 (quoting IRS commissioner John Koskinen).

235. *Id.* (quoting Rep. Gerry Connolly (D-VA)).

236. Jagoda, *supra* note 223.

237. *See* TREASURY INSPECTOR GEN. FOR TAX ADMIN., *supra* note 27, at 2.

238. INTERNAL REVENUE SERV., 2014 DATA BOOK 70 tbl.31 (2015); Lisa Rein, *Declining IRS Workforce Leaves Calls Unanswered as Tax Day Approaches, Union Says*, WASH. POST (Apr. 6, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/04/06/declining-force-of-irs-employees-leaves-calls-unanswered-as-tax-day-approaches-union-says [https://perma.cc/76KR-2DRZ].

239. William Hoffman, *Almost Half of IRS Leadership Gone Since 2011, Koskinen Says*, 147 TAX NOTES 33, 33–34 (2015); William Hoffman, *Koskinen's Tough Job Likely To Get Tougher in 2015*, 146 TAX NOTES 18, 18–19 (2015); William Hoffman & Tom Kasprzak, *Omnibus Prompts IRS Hiring Freeze, Travel Cuts*, 145 TAX NOTES 1323, 1323 (2014); *Koskinen Outlines How 2015 Budget Cuts Will Affect IRS Employees*, 2015 TAX NOTES TODAY 9–18 (Jan. 13, 2015); Devin Leonard & Richard Rubin, *An Emotional Audit: IRS Workers Are Miserable and Overwhelmed*, BLOOMBERG BNA (Apr. 8, 2015), https://www.bloomberg.com

valuable employees.[240] In addition to the difficulty of retaining valuable employees in a low morale work force, the IRS is also hampered by the limited compensation it can offer and the bureaucratic constrictions of federal recruitment and employment.[241]

While the IRS has had these general personnel struggles, its history with highly qualified IT personnel has been especially problematic. It has succeeded in hiring high-profile individuals charged with correcting decades of technological mistakes,[242] but these individuals tend to be short lived in their positions, and competition over their plans and positions undermines consistent progress.[243] Competition for IT personnel is stiff, especially with the private sectors, and bureaucratic processes often disadvantage the IRS even when compensation and other factors appeal to potential recruits.[244] Turnover of IT personnel also has hampered modernization efforts.[245] A final personnel difficulty is the need for IT personnel to be not only technically skilled but to understand the peculiarities of both the IRS and the IRS system. There have been problems with hiring outside experts who did not have the inside knowledge needed to devise workable technological solutions.[246]

Unfortunately for the IRS, cybersecurity experts are both crucial to success and difficult to recruit. The cybersecurity problem is a cyber "people" problem. Former Director for Information Assurance at the NSA Richard George says that finding the people who can respond to growing cyber threats was one of the most worrisome challenges he faced.[247] It is a very small talent pool, and a "lot of people" are trying to hire from it.[248] The "cyberwarfare market has grown so fast that it outstripped available labor pools."[249] The U.S. government has only three to ten percent of the cybersecurity experts it needs, and government agencies are disadvantaged in the competition for this talent.[250] The agencies cannot compete in terms of compensation offered in the private sector.[251] Perhaps just as importantly, the work culture of government agencies is not as appealing as dynamic, high-tech firms where employees prefer "cargo shorts and a T-shirt over khakis and a tie."[252] While these problems are common to government agencies, the IRS is even worse off, struggling with limited resources, low office morale, and arguably less mission appeal than, say, the NSA, the Pentagon, or the White House.

/news/features/2015-04-08/an-emotional-audit-irs-workers-are-miserable-and-overwhelmed [https://perma.cc/ZKE8-GJLP].

240. *See* Hoffman, *supra* note 239, at 33.
241. Guttman, *supra* note 181, at 727.
242. *Id.*
243. *See id.*
244. *See* Noble, *supra* note 178.
245. *See* Guttman, *supra* note 181, at 727.
246. *See* Noble, *supra* note 178.
247. SINGER & FRIEDMAN, *supra* note 112, at 235–36.
248. *Id.* at 236.
249. *Id.*
250. *Id.*
251. *Id.* at 236–37.
252. *Id.* at 237.

D. Too Many Users

A fourth reason to doubt the IRS's ability to master cybersecurity is recognizing the greatest weakness in cybersecurity: human users. The greatest leak of top U.S. secrets was not a great technical feat; rather, it was a single individual's politically motivated choice to download and disclose documents.[253] One of the largest cyber breaches in U.S. military history occurred when a U.S. soldier picked up a flash drive in a parking lot near his base and plugged it into his computer to see what was on it.[254] What was on the flash drive was a worm devised by a foreign intelligence agency to attack the military computer system and that took the Pentagon more than a year to clean out of its systems.[255] The tactic of relying on authorized users plugging infected drives into protected systems is so well known it has its own name: "candy drop."[256] It is not just soldiers who take this infectious candy from strangers. An executive at an IT company did the same with a malware-ridden CD that had been left in his company's restroom.[257] It's not just candy that tempts humans, of course. A defense company employee used his business computer to share music online, allowing Iranian hackers to access design details for the U.S. President's helicopters.[258] In one high profile "spear phishing"[259] attack, British military officers' systems were hacked because the officers responded to a faked "friend request" from a well-known British admiral.[260] Such poor cybersecurity hygiene is ubiquitous. It accounts for the most common computer password being "password," and the second most common being "123456."[261] In one very disturbing case, password laziness was taken to near its limit by a U.S. Air Force base commander who insisted on being given a single-digit password to access classified information because he was "too important" to type in multiple digits.[262] In another disturbing case, a Secretary of State, responsible for the international relationships of the United States with all other nations, sidestepped all protocols for e-mail usage, storing her e-mail on a private server at her house, violating general government policies, and ignoring

253. Strohm & Wilber, *supra* note 127.
254. SINGER & FRIEDMAN, *supra* note 112, at 64–65.
255. *Id.*
256. *Id.* at 64.
257. *Id.* at 65.
258. *Id.*
259. "Phishing" is a familiar type of attack. It is a "digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information." U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 5. If a specific individual or group is targeted, it is called "spear phishing." For example, rather than receiving a phishing e-mail from a Nigerian prince, the user receives one from his mother, wife, or friend. *Id.* The specific information used for spear phishing, whether it is the e-mail addresses of military officers or the name of a user's mother, wife, or friend, often are obtained by simple word searches of widely accessible information. As it turns out, the "most impressive tool in the attackers' arsenal is Google." SINGER & FRIEDMAN, *supra* note 112, at 57.
260. SINGER & FRIEDMAN, *supra* note 112, at 58.
261. *Id.* at 241.
262. *Id.* at 242.

specific advice to her personally.[263] In another disturbing case directly on point, IRS employees sidestepped protocols for e-mail, sending unencrypted email that may have exposed the personal information of twenty-eight million taxpayers.[264] While there are many technical difficulties that make our defense difficult, it is the human activity that makes us most vulnerable.

Notably, not even the military has been able to manage the human elements in its systems. The IRS is even less likely able to manage them. First, the IRS already suffers significant personnel problems: low morale and difficulty retaining its more experienced employees. Second, unlike the military systems that are not accessible by the public, the IRS system is. No matter how problematic employees may be in terms of cybersecurity hygiene, the IRS system involves hundreds of millions of nonemployee users. There are hundreds of millions of taxpayers, third-party reporters, and tax professionals providing and seeking taxpayer information. The evidence is clear that very few individuals appreciate cybersecurity risks: we do not read the terms of service; we upload and download what we should not; and we make ourselves vulnerable through poor passwords, public posting of private information, and, in general, not taking cyber risks seriously.[265] It is extraordinarily unlikely that the IRS will be able to implement a security system that covers hundreds of millions of users providing and receiving private information while following appropriate protocols.

E. Cybersecurity Is Difficult

A final reason to predict the IRS will be unable to master cybersecurity is simply that cybersecurity is very difficult. The U.S. government has been focused on cybersecurity since 1997,[266] yet its failings are headline news: personnel records on

---

263. *See* Mark Landler & Eric Lichtblau, *F.B.I. Director James Comey Recommends No Charges for Hillary Clinton on Email*, N.Y. TIMES (July 5, 2016), http://nyti.ms/29k3gCm [https://perma.cc/R889-NZN9].

264. TREASURY INSPECTOR GEN. FOR TAX ADMIN., NO. 2017-30-010, EMPLOYEES SOMETIMES DID NOT ADHERE TO E-MAIL POLICIES WHICH INCREASED THE RISK OF IMPROPER DISCLOSURE OF TAXPAYER INFORMATION 4 (2016), https://www.treasury.gov/tigta/auditreports/2017reports/201730010fr.pdf [https://perma.cc/29NF-8KFL].

265. SINGER & FRIEDMAN, *supra* note 112, at 241; Allison S. Brehm & Cathy D. Lee, *Click Here To Accept the Terms of Service*, 31 ABA COMM. LAW. 1 (2015), https://www.americanbar.org/publications/communications_lawyer/2015/january/click_here.html [https://perma.cc/WF3S-FWRC]; Troy Hunt, *The Science of Password Selection*, TROY HUNT (July 18, 2011), https://www.troyhunt.com/science-of-password-selection [https://perma.cc/Y9HT-WNQP]; Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR. (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is [https://perma.cc/4HZ4-FZPL]; Shankar Vedantam, *Do You Read Terms of Service Contracts? Not Many Do, Research Shows*, NPR (Aug. 23, 2016, 5:06 AM), http://www.npr.org/2016/08/23/491024846/do-you-read-terms-of-service-contracts-not-many-do-research-shows [https://perma.cc/LX48-MT7V].

266. In 1997, the Government Accountability Office first designated cybersecurity as a "government-wide high-risk area." U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-294, INFORMATION SECURITY: DHS NEEDS TO ENHANCE CAPABILITIES, IMPROVE PLANNING, AND SUPPORT GREATER ADOPTION OF ITS NATIONAL CYBERSECURITY PROTECTION SYSTEM 1

twenty-five million individuals stolen from OPM;[267] Edward Snowden stealing more top secrets than had ever been stolen;[268] and successful cyberattacks against the White House, Joint Chiefs of Staff, Department of Defense, Department of State, Postal Service, National Aeronautical Space Agency, United States Geological Service, and the Oak Ridge National Laboratory.[269] And, of course, corporations are focused on cybersecurity, but their failures too are headline news: personal information from 83 million JPMorgan Chase account holders stolen, personal information from 56 million Home Depot customers and 110 million Target customers, and health insurance information from Anthem on 80 million Americans.[270] There is no reason to believe that the IRS will be able to succeed where so many agencies and corporations have failed, especially given that the treasure trove of information that the IRS likely will be storing in the future is far more valuable information than credit card numbers.

Cybersecurity is a very difficult goal to achieve, which is why, despite the efforts of agencies and corporations, there continue to be huge failures. Cybersecurity "is harder than building bridges . . . . [p]rotecting the Internet and online computerized systems from attack is a difficult, messy problem."[271] In addition to the difficulties raised by a shortage of qualified IT experts, the tremendous problems caused by widespread human negligence, and the difficulties of a system being used by hundreds of millions, there are other factors that make cybersecurity so difficult—not just for the IRS but any organization. First, cyber systems are extraordinarily complex.[272] Windows 10 uses 50 million lines of code, and Mac OS 10.04 uses 86 million.[273] Each line potentially contains errors to be exploited. These systems are being upgraded, revised to be improved, but with each revision potentially bringing new vulnerabilities.[274] Second, cyberattacks have high reward potential and low costs and risks.[275] Cyberspace has valuable targets, which can be hit—their data to be stolen, sold, and used in further attacks—for financial or political purposes.[276] And cyberattacks are "relatively cheap, easy to conduct, and of low risk to their perpetrators,"[277] who may be in foreign countries thousands of miles away. Third, security measures that protect access to a system (such as a password) do not provide protection for "data in transit over networks."[278] Protecting this data requires

---

(2016). Each year since 2001, Congress has held cybersecurity-related hearings. RITA TEHAN, CONG. RESEARCH SERV., R43317, CYBERSECURITY: LEGISLATION, HEARINGS, AND EXECUTIVE BRANCH DOCUMENTS 1 (2017).

267. *See supra* note 144 and accompanying text.

268. *See supra* note 127 and accompanying text.

269. *See Significant Cyber Events*, *supra* note 121.

270. Moisés Naím, *Why Cyber War Is Dangerous for Democracies*, ATLANTIC (June 25, 2015), http://www.theatlantic.com/international/archive/2015/06/hackers-cyber-china-russia/396812 [https://perma.cc/T9PM-EYT9].

271. Denning & Denning, *supra* note 3, at 154.

272. *Id.*

273. *Id.* at 156.

274. *Id.*

275. *Id.*

276. *See id.* at 155.

277. *Id.* at 156.

278. *Id.* at 155.

different measures (such as encryption), which raise far more difficult problems to solve.[279]

While these are the difficulties for every other organization, the IRS is unlike any other organization. One of the reasons that its efforts to modernize its technology, generally, have failed so often is that it is such a complex project. One outside tech expert who worked on the BSM project said it was the most complex project he had in his thirty years of high-tech work.[280] In addition to the complex technical issues that have accrued over the past fifty years of patched and piecemeal updates, the work of the system is inherently complex. This is a system that, whatever its technical shortcomings, is, in fact, processing more than 243 million returns of various sorts,[281] $3.3 trillion in gross tax payments, and $403 billion of refunds each year.[282] While it may be the IT modernization efforts at the IRS involved the IRS spending billions order to rebuild a 1960 Chevy,[283] trying to improve IT at the IRS must be akin to trying to rebuild a car's engine while driving it. Some sympathy for the IT employees at the IRS is due. Their failures over the decades to solve the IT problems at the IRS may well be due more to the difficulty of the problem than lack of skill or effort. But that makes it even less likely, not more likely, that the IRS will solve the cybersecurity problems other organizations cannot solve.

III. BETTER DIGITAL TECHNOLOGY IS NOT THE GOAL

The IRS must collect tax information, and it will increasingly use information technology to increase the tax information it collects. The problem is that the IRS will use technology to collect far more information than it can protect technologically. One approach would be to slow the use of new digital technology, cautiously stepping rather than naively running further into the IT revolution. This approach is considered in Part III.A, though, as a matter of popularity and politics, it is most likely a nonstarter. Part III.B sketches the ways in which commonly proposed tax reforms could address the problem. These reforms would increase the security of information held by the IRS by tasking the IRS with collecting less information, collecting information on fewer individuals, and issuing fewer refunds. Congress reducing these IRS tasks would make the IRS a less appealing and more defensible target for cyberattack.

A. Slowing the Use of Digital Technology

If the IRS cannot technologically defend the information it collects, what is the best way forward? One approach would be to more intentionally, more selectively, and more cautiously employ digital technology in tax administration. This may mean

---

279. *Id.*

280. A vice president of CSC, the outside corporation hired to facilitate BSM, described it as the most complex project he had encountered in his "30 years of working in the technology field." Thompson, *supra* note 180.

281. INTERNAL REVENUE SERV., *supra* note 21, at 6.

282. *Id.* at iii.

283. Guttman, *supra* note 181, at 726.

technological "arrest" or "regression," that is, suspending the use of emerging technology or returning to an earlier technology, as the case may be, out of concerns for cybersecurity.[284] For example, following the revelation of Edward Snowden's leak of top U.S. secrets, Russian security officials ordered manual typewriters.[285] Nikolai Kovalev, a Russian Member of Parliament and former head of the Federal Security Service, explained that "from the point of view of keeping secrets, the most primitive method is preferred: a human hand with a pen or a typewriter" because every "form of electronic communication is vulnerable."[286] There is some expectation that this type of practice will expand in an effort to protect national security.[287] Some government employees in Germany are being encouraged to "stay away from technology whenever they can" when it comes to sensitive communications.[288] "Those concerned talk less on the phone, prefer to meet in person. More coffees are being drunk and lunches eaten together. Even the walk in the park is increasingly enjoying a revival" among these government employees.[289] Presumably, such strategic retreats from the cutting edge will be the exceptions to the general rule of increasing reliance on digital technology. However, the exceptions underscore how difficult cybersecurity is, and that serious consideration of the best way forward does not exaggerate the inadequacies of past ways. The future may be considerably more varied and complicated in terms of how information technology is used than the carefree use of the technology by contemporary American consumers suggest.

In the Russian case, the inability of many government agencies to keep pace with technological innovation has meant that typewriters were not as far from common use as would be the case in the United States.[290] In those situations, it was not intentional technological arrest that may have provided relative cybersecurity benefits, but rather happenstance. It seems likely that this happened at the IRS, too. The IRS computerized its operations in the mid-1960s, and, as explained above, much of its storing and processing of information still relies on the 1960s design and magnetic tapes.[291] None of this information has been hacked. The cyberattacks against the IRS have been aimed at only the most recent technological updates that were public facing. The refund attacks took advantage of the electronic filing processes, which were not fully implemented for more than forty years after the National Computing Center

---

284. *See* Kristen E. Eichensehr, *Giving Up on Cybersecurity*, 64 UCLA L. REV. DIS. 320, 320 (2016) (arguing that the response to increasing digitization will result in disengagement from high technologies).

285. *Id.* at 330; Miriam Elder, *Russian Guard Service Reverts to Typewriters After NSA Leaks*, GUARDIAN (July 11, 2013), https://www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks [https://perma.cc/5GZY-CGTV].

286. Elder, *supra* note 285; *see also* Eichensehr, *supra* note 284, at 330.

287. Eichensehr, *supra* note 284, at 331; Elder, *supra* note 285 (discussing likelihood of expansion of strategy among G20); Philip Oltermann, *Germany 'May Revert to Typewriters' To Counter Hi-Tech Espionage*, GUARDIAN (July 15, 2014), https://www.theguardian.com/world/2014/jul/15/germany-typewriters-espionage-nsa-spying-surveillance [https://perma.cc/CA9A-WHVY] (considering strategy by German government).

288. Oltermann, *supra* note 287 (considering strategy by German government).

289. *Id.*

290. *See* Elder, *supra* note 285 (listing various agencies unable to update technologically).

291. *See supra* notes 156–167 and accompanying text.

was established.[292] And the Get Transcript attack was aimed at a technology that was only months old.[293] It is worth noting that the antiquated and piecemeal nature of the IRS information system may have provided considerable cybersecurity for taxpayer information. While the failure to modernize the system has become an embarrassment to the agency, its technical director has made clear that the system is "not broken."[294] Indeed, if the Future State initiative emphasis on transforming the public-facing aspects of the system were shifted to the refund-processing and fraud-detection functions, if more attention were paid to customer service by phone and mail than through apps and the web, the resulting systems might more adequately serve and protect taxpayers for some time to come.[295] President Obama's vision of making taxpaying like online pizza-ordering may be seeing much further in the future than he thought.[296]

However, given the political pressure on the IRS to close the tax gap and ease the compliance burden, and the IRS's aim to update its information technology fully, it is almost certainly too late for a strategic retreat from the type of vision articulated in the Future State initiative. Even if such a retreat would be the best strategy, persuading the public and the politicians and the bureaucrats that what is older may be better, and, indeed, more cutting-edge than what is newer, is a nonstarter. It is too simple to be persuasive. There is too much popular faith in IT expertise to convince either the public or the politicians that we cannot always get the technology we want and may not even be able to get what we need.

B. Cybersecurity and Tax Reform

If we take as a given that the IRS will increase its use of digital information technology to collect and store information, and that the IRS will not move more cautiously and slowly and counter to the popular imagination, even though its digital technology will be unable to protect the information it holds, what then? If it is too heretical to limit technological aspirations, perhaps it is still acceptable to limit information needs. Congress decides what information is tax relevant, and then the IRS uses computer technology to collect, store, and process the information that Congress has defined as relevant. I suggest we turn our focus from the technology the IRS is

---

292. *See supra* notes 53–61 and accompanying text.

293. *See supra* notes 63–65 and accompanying text.

294. *See* Noble, *supra* note 178.

295. The National Taxpayer Advocate has criticized the Future State initiative for being focused on new technology to the exclusion of human needs, preferences, and behavior. *The National Taxpayer Advocate's 2015 Annual Report to Congress: Hearing Before the Subcomm. on Gov't Operations of the H. Comm. on Oversight and Gov't Reform*, 114th Cong. 42 (2016) (statement of Nina E. Olson, National Taxpayer Advocate) (Olson believes that IRS focusing on online accounts is wrong-headed and will not reduce costs or satisfy taxpayers); Bernie Becker, *Mapping Out the 'Future State,'* POLITICO (Feb. 23, 2016, 10:00 AM), http://www.politico.com/tipsheets/morning-tax/2016/02/mapping-out-the-future-state-uncharted-territory-for-tax-analysts-irs-audit-rate-keeps-slipping-212842 [https://perma.cc/BA2T-FU4G] ("Olson has openly worried that the plan will treat poorer taxpayers as second-class citizens.").

296. *See* Lapowsky, *supra* note 40.

using to the information the IRS is being tasked to collect, store, and process with its technology. My recommendation is this: Congress should make its political compromises on what information is tax relevant in light of the need to protect the information as it is collected and stored and processed.

There is considerable flexibility in tax law. There is no Platonic form of taxation. While natural law may guide legislation on crime, morality, and war, it is of little use in deciding whether a universal standard deduction ought to replace itemized deductions. Tax law is always a matter of political compromises and educated guesses. One approach to improving the cybersecurity of the information collected by the IRS would be to make those compromises and guesses in ways that reduce information security risks. The compromises inhere in the tax legislation process in great part because there is considerable uncertainty and disagreement over fundamental issues, like whether it is preferable to tax labor, capital, or consumption.[297] While these uncertainties and disagreements create flexibility, there is also the flexibility that comes from multiple ways of achieving the same tax result. If the intended result is to tax national consumption, it can be done through a national sales tax comparable to the familiar state sales taxes.[298] Or it can be done by keeping the familiar federal income tax but by deducting savings from income.[299] Between the flexibility of tax theories, which reveal the numerous roads to the same destination, and the reality of political compromises on the trip down any of those roads, there is ample room for Congress to consider information security risks when enacting tax legislation.

The way forward is to ask, what sorts of tax legislation would improve cybersecurity prospects? Tax legislation is usually assessed on familiar points: revenue, efficiency, equity, administrative ease, and political viability.[300] Into this mix of points, and overlapping all of them though not overriding any of them, information security should be added. There is a fair supply of tax reform proposals always on the shelves of Congress, if not on the floor. Given the relative mix of those points of debate at any given time, some proposals are more appealing and others less. Each of the proposals has its proponents and opponents, advantages and disadvantages, uncertainties, unknowns, and politics. The step forward, at this point, is not to argue for a particular proposal to improve cybersecurity, but rather to argue that cybersecurity implications ought to be one of the points of argument on all of the proposals.

What sorts of tax reform would improve cybersecurity prospects? Reform that would make the IRS a less appealing and a more defensible cyberattack target would.

---

297. For an overview of the research on various forms of taxation, see David Gamage, *The Case for Taxing (All of) Labor, Income, Consumption, Capital Income, and Wealth*, 68 TAX L. REV. 355 (2015) (arguing that as all forms of tax measurement are imperfect, it is often better for governments to use multiple forms of tax measurement).

298. *See, e.g.*, David R. Burton & Dan R. Mastromarco, *The National Sales Tax: Moving Beyond the Idea*, 71 TAX NOTES 1237 n.32 (1996) (discussing similar system employed in Quebec to collect both the federal goods and services taxes and the provincial sales tax).

299. *See, e.g.*, Alliance USA, *Unlimited Savings Allowance (USA) Tax System*, 66 TAX NOTES 1485 (1995); William D. Andrews, *A Consumption-Type or Cash Flow Personal Income Tax*, 87 HARV. L. REV. 1113 (1974).

300. *See, e.g.*, PHILIP D. OLIVER, TAX POLICY 1–4 (2011) (overview of primary tax policy criteria).

Reform that made refunds the exception rather than the rule, making the IRS less like an ATM would reduce its appeal to financial thieves. Reform that reduced the amount of information required of taxpayers, and reform that reduces the number of individuals on whom information is collected would reduce the appeal of the IRS to information thieves, as well as the appeal to terrorists and hostile governments who may seek not merely to steal but manipulate or destroy information. These same reforms would make the IRS more likely able to defend itself. Imagine an IRS not burdened with the need to process hundreds of millions of refund claims and pay billions of dollars over a short period of time each year. Imagine that same IRS processing fewer individual returns each year and collecting less information on each return. The IRS would have a greatly reduced need to consume information. It would be a much skinnier IRS. And, a skinnier IRS would be more easily fitted with digital protection. With fewer individuals claiming refunds, there would be less pressure to provide and defend online refund processes. With less information being collected, there would be less information to process and protect. And with fewer individuals covered by the system, there would be fewer online users to accommodate and monitor. With less pressure on its information system, there could be more focus on improving the system. As it is, the IRS is overwhelmed with nineteen major technology projects and unable to make even the simplest of improvements, like upgrading Windows,[301] much less the most complicated of improvements, like providing adequate cybersecurity. Whatever the chances the IRS has for developing an adequate high-tech response to information security, the odds are greater if both the high-tech needs of the IRS and the external users of the IRS system are lessened. The IRS will not be able to secure a system that involves hundreds of millions of individuals reporting and accessing information and claiming and being paid billions in refunds. The IRS may be able to secure something much less ambitious.

Below are sketches of a half dozen common tax reform proposals, considering the extent to which each would—relative to the current system—reduce the number of refunds, require less information, and reduce the number of individuals involved. The proposals are the Pay-As-You-Earn improvements on the withholding mechanisms; efforts to simplify the income tax, or, to purify the income tax, or to transform it from a mass tax to an elite one; and proposals to tax consumption rather than income, either in the form of a sales tax that almost all of the states use, or in the form a value-added tax (VAT) that almost all economically developed nations use. Of course, the extent to which a proposal would achieve these three recommendations would depend upon the details of actual legislation, politically pushed and pulled into place. In their current form, none of these proposals address the impact on cybersecurity prospects, but looking at some of the key features of the proposals, we can compare their relative potential to fit with the recommendations.

1. Pay-As-You-Earn (PAYE)

In the current U.S. income tax system, employers withhold from employees' paychecks and pay the withheld amounts to the IRS throughout the year so the

301. *See supra* notes 199–209 and accompanying text.

amounts can be held and used to pay the employee's year-end income tax liability.[302] To the extent these advance payments exceed the employee's actual tax liability the employee is entitled to a refund.[303] This advance payment system is essential to the function of the U.S. income tax as, otherwise, employees would have to be sufficiently organized and disciplined to estimate their future tax liabilities and save accordingly.[304]

Tax systems worldwide use withholding, but the details vary importantly. In the United States, the system systemically results in overwithholding, which is why the IRS must refund payments to about 117 million of the 149 million of individual taxpayers.[305] The U.S. system works well in the sense of ensuring that the liabilities are covered. But it does so in a way that then burdens many taxpayers with the need to file returns to claim refunds and burdens the IRS with the need to process these returns and issue refund payments. The U.S. system uses a simpler, less precise method than many other countries.[306] For example, if the rate of wages changes during the course of the year, the U.S. system does not adjust the amount of withholding. However, in the United Kingdom, withholding is adjusted with such precision that usually the employee's ultimate tax liability is exactly covered, often through significant adjustments in withholding amounts in the employee's final paycheck of the year.[307] The same approach is often used for withholding interest and other payments to the taxpayer by third parties who are not employers.[308] A more precise withholding system—commonly called a pay-as-you-earn (PAYE) system—means not only that refund payments become the exception rather than the rule but that even individual tax returns do. In the United Kingdom, this system works so well that most lower- and middle-income taxpayers' liabilities are precisely satisfied such that they need not file a return.[309] This covers about two-thirds of the taxpayers in the United Kingdom and about 80% of all wage-earners.[310]

Movement towards a PAYE system in the United States has been promoted for years, largely due to the success of such systems outside the United States. However, moving towards such a system would require significant simplification to the U.S. tax system with respect to the number of tax rates that apply to income, the impact of marital or family status on those rates, and the number of deductions and credits

---

302. NAT'L TAXPAYER ADVOCATE, INTERNAL REVENUE SERV., ANNUAL REPORT TO CONGRESS VOLUME 2: TAS RESEARCH & RELATED STUDIES 148–49 (2011), https://www.irs.gov/pub/tas/irs_tas_arc_2011_vol_2.pdf [https://perma.cc/YH2F-6KNG].

303. *Id.*

304. Robert Higgs, *Wartime Origins of Modern Income-Tax Withholding*, FREEMAN: IDEAS ON LIBERTY, Nov. 2007, at 31, 31–32; Jonah Goldberg, *Automatic Tax Withholding*, AM. ENTERPRISE INST. (May 2, 2013), https://www.aei.org/publication/automatic-tax-withholding [https://perma.cc/B4UG-ZFZU].

305. *See* INTERNAL REVENUE SERV., *supra* note 21.

306. NAT'L TAXPAYER ADVOCATE, *supra* note 302, at 148–49.

307. *Id.* at 148 n.16; William J. Turnier, *PAYE as an Alternative to an Alternative Tax System*, 23 VA. TAX REV. 205, 227 (2003).

308. NAT'L TAXPAYER ADVOCATE, *supra* note 302, at 148–49.

309. Turnier, *supra* note 307, at 212.

310. *Id.* at 212, 232.

available to individuals.[311] Without such a simplification, the U.S. tax system would remain too complex for PAYE to be implemented. As such simplification would inevitably target complex yet important benefits, such as the Earned Income Tax Credit (EITC), the benefits of a PAYE system would have to be clearly greater than the benefits of the programs that would be targeted.

As part of counting the costs and benefits of a PAYE system in the United States, we should consider the impact it would have on cybersecurity. In terms of improving information security, the chief benefit of a PAYE system would be reforming the refund system in the United States. To the extent refunds became the exception rather than the rule, the refund payment process could be more tightly controlled, reducing the ease with which fraudulently filed returns succeed at stealing refund payments. Having made it a more difficult fraud, stealing taxpayer information to file fraudulent returns would be a less appealing objective than it currently is. In and of itself, a PAYE system would not have any impact on the other recommendations, that is, collecting less information and reducing the number of individuals covered by the system. However, to the extent that a PAYE system could not be implemented without significant simplification of the substantive tax law, the simplification and PAYE implementation, together, might also result in less information being collected on fewer individuals being covered by the system.

2. Simplified Income Tax

The income tax law is often criticized for being too complex.[312] The provisions that apply to individuals are numerous, technical, and related. For example, by the National Taxpayer Advocate's count, there are eleven different provisions related to college education expenses, each of which has its own eligibility requirements, definitions, income thresholds, phaseouts, and inflation adjustments.[313] There are sixteen different provisions for retirement savings.[314] With over 3.7 million words, the tax code has three times the words it did in 1975.[315] The tax regulations and the summaries of case law and IRS guidance take nine feet of shelf space.[316] The income tax law for individuals is so complex that eighty percent pay for help in preparing their annual income tax returns.[317]

---

311. *Id.* at 249–50.

312. *See, e.g.*, STAFF OF JOINT COMM. ON TAX'N, 107TH CONG., STUDY OF THE OVERALL STATE OF THE FEDERAL TAX SYSTEM AND RECOMMENDATIONS FOR SIMPLIFICATION, PURSUANT TO SECTION 8022(3)(B) OF THE INTERNAL REVENUE CODE OF 1986 (Comm. Print 2001); BORIS I. BITTKER & LAWRENCE LOKKEN, FEDERAL TAXATION OF INCOME, ESTATES & GIFTS ¶ 3.8 (2017); Joseph M. Dodge, *Some Income Tax Simplification Proposals*, 41 FLA. ST. U. L. REV. 71 (2013); Press Release, U.S. Treasury Department, Treasury Statement on the Joint Committee on Taxation Study on Tax Simplification (Apr. 25, 2001), https://www.treasury.gov/press-center/press-releases/Pages/po223.aspx [https://perma.cc/J78N-HRTF].

313. NAT'L TAXPAYER ADVOCATE, *supra* note 83, at 5.

314. *Id.* at 6.

315. *Id.* at 4.

316. *Id.*

317. *Id.* at 5.

The standard deduction and personal and dependency exemptions are among the simplest of tax provisions. The standard deduction allows a taxpayer to deduct a certain amount regardless of expenses.[318] It is based on nothing more than the taxpayer's filing status.[319] The standard deduction is taken in lieu of the itemized deductions.[320] Similarly, the personal and dependency exemptions allow a taxpayer to exempt a certain dollar amount from taxation based on the number of individuals in the household.[321] Together, these simplify compliance for taxpayers and also shield a basic subsistence level of income from taxation altogether.[322] In practice, over sixty percent of taxpayers claim only the standard deduction and exemptions.[323]

It is common for tax simplification proposals to aim at increasing the amount of tax-free income to which a taxpayer is entitled each year while decreasing the number of specific tax benefits available. For example, the bipartisan National Commission on Fiscal Responsibility and Reform (often called the "Simpson-Bowles Commission") proposed eliminating all (nonbusiness or investment-related) itemized deductions and retaining only a standard deduction.[324] Increasing the standard deduction and exemption amounts, even if not completely eliminating all other tax benefits for individuals, has also been proposed by others, such as Senator Rand Paul.[325] Professor Michael Graetz has proposed a "family allowance" of $100,000 to replace not only itemized deductions but the standard deduction and the exemptions

---

318. For a general discussion of the standard deduction and its history, see BITTKER & LOKKEN, *supra* note 312, ¶ 30.5.

319. In 2016, the standard deduction amounts were $12,600 for married filing jointly, $9300 for head of household, and $6300 for single or married filing separately. Rev. Proc. 2015-53, 2015-44 I.R.B. 615. There is an additional standard deduction if the taxpayer is over age 65 or blind. BITTKER & LOKKEN, *supra* note 312, ¶ 30.5.

320. An individual taxpayer takes either (1) the standard deduction, *see* I.R.C. § 63(c) (Westlaw through Pub. L. 115-97), or (2) the total of allowable itemized deductions, but not both, *id.* § 63(b). "Itemized deductions" are the deductions other than (1) the standard deduction, (2) deductions listed in § 62 that are taken in arriving at adjusted gross income, and (3) the deductions for personal and dependency exemptions allowed by § 151. *Id.* § 63(d).

321. In 2016, the personal exemption amount are $4050. Rev. Proc. 2015-53, 2015-44 I.R.B. 615. For a general discussion of the personal and dependency exemptions and their histories, see BITTKER & LOKKEN, *supra* note 312, ¶ 30.2–30.3.

322. BITTKER & LOKKEN, *supra* note 312, ¶ 30.5. While discussion of these provisions often conflates these justifications, the two different functions of these provisions might be better served by focusing on which is most important. *See* Dodge, *supra* note 312, at 78 (calling for the elimination of the standard deduction and the increasing of the personal exemption in order to protect a subsistence level of income from taxation).

323. In 2014, 43,965,083 returns elected to itemize, whereas 102,594,719 took the standard deduction. INTERNAL REVENUE SERV., PUB. 1304, INDIVIDUAL INCOME TAX RETURNS 2014, at 46 (complete report).

324. NAT'L COMM'N ON FISCAL RESPONSIBILITY & REFORM, THE MOMENT OF TRUTH 31 (2010), http://momentoftruthproject.org/sites/default/files/TheMomentofTruth12_1_2010.pdf [https://perma.cc/F22Y-BPQU].

325. For example, see Rand Paul's "Fair and Flat Tax Plan." Rand Paul, Opinion, *Blow Up the Tax Code and Start Over*, WALL ST. J. (Jun. 17, 2015), http://www.wsj.com/articles/blow-up-the-tax-code-and-start-over-1434582592 [https://perma.cc/X4A5-DQGE]; *Senator Rand Paul Releases Flat Tax Plan*, COMMITTEE FOR RESPONSIBLE FED. BUDGET (Nov. 16, 2015) http://crfb.org/blogs/senator-rand-paul-releases-flat-tax-plan-0 [https://perma.cc/XW3B-2Y4F].

with a simpler though similar mechanism.[326] Professor Edward Kleinbard has suggested replacing all itemized deductions with a uniform tax credit.[327]

The opposition to these types of simplification proposals is defense of the more precisely targeted tax benefits that come with itemized deductions. For example, the long-standing policy of encouraging deductions to charities through the charitable income tax deduction, subsidizing medical care through the medical expense deduction, and promoting home ownership through home mortgage interest deduction are accomplished through itemized deductions.[328] The complexity of these and similar tax benefits are arguably justified by the advantages obtained for fairness or other important policies, such as stimulating the economy.[329]

Alongside the advantages and disadvantages of simplifying the tax system this way, we also should consider the cybersecurity advantages. With respect to the recommendations for improving cybersecurity, simplification like providing a more generous standard deduction and exemptions in lieu of more specific tax benefits would succeed in reducing the amount of information required. In and of itself, such a move would not affect the number of refunds paid or the number of individuals covered by the system. Of course, if coupled with movement towards implementing a PAYE system, the number of refunds would be reduced. The most important independent benefit for improving information security prospects would be to reduce the amount of information collected. Depending upon the form of the simplification, the amount of information would reflect nothing more than the number of individuals with some specified relationship with the taxpayer. What would be eliminated would be requirements to provide more detailed information, such as the medical care, child care, and education expenses for those individuals,[330] or any of the other information required by the deductions and credits eliminated by the proposal.

3. Purified Income Tax

Somewhat similarly to criticisms of the complexity of the tax law is the criticism that the tax law is not focused on revenue collection. Beginning with Professor Stanley Surrey, the Assistant Secretary of Treasury for Tax Policy under President

---

326. This is part of a much more fundamental reform described below. Michael J. Graetz, *100 Million Unnecessary Returns: A Fresh Start for the U.S. Tax System*, 112 YALE L.J. 261, 295 (2002) (arguing for the imposition of a VAT and elite income tax).

327. EDWARD D. KLEINBARD, WE ARE BETTER THAN THIS: HOW GOVERNMENT SHOULD SPEND OUR MONEY 382 (2015) (proposing the replacing of all personal itemized deductions with a fifteen percent credit).

328. For a discussion of the role of itemized deductions and the standard deduction, see BITTKER & LOKKEN, *supra* note 312, ¶ 30.4–30.5.

329. For an overview of the defense of this type of complexity, see *id.* ¶ 3.8. More specifically, see Samuel A. Donaldson, *The Easy Case Against Tax Simplification*, 22 VA. TAX REV. 645 (2003) (arguing that complexity in the tax code is a net benefit in achieving policy objectives, and that tax simplification proposals are an overcorrection to the problem and ultimately ineffectual).

330. *See, e.g.*, I.R.C. § 213 (Westlaw through Pub. L. 115-97) (medical expense deduction); *id.* § 21 (dependent care credit); *id.* § 25A (education credits); *id.* § 222 (deduction for education expenses). *See generally* Hatfield, *supra* note 77.

Kennedy, many critics have conceived the tax code as two independent parts.[331] The first part is what is necessary to implement the income tax.[332] The second part is "grafted on to the structure of the income tax."[333] It is a "vast subsidy apparatus that uses the mechanics of the income tax as the method paying the subsidies" by providing "exclusions from income, exemptions, deductions, credits against tax, preferential rates of tax, and deferrals of tax."[334] Although grafted into the income tax, these "tax expenditures" are the equivalent of a subsidy payment. Critics of tax expenditures equate the choice not to tax what should be taxed with a payment to the benefitted taxpayer. As a result of Professor Surrey's conception, each year the President and the Joint Committee on Taxation each prepare a list of these potentially controversial benefits.[335] These two lists—known as the "tax expenditure budgets"—differ in the some of the technical definitions, but the resulting lists are quite similar.[336] The most significant tax expenditure items are those related to employer-provided benefits (i.e., the tax advantages of employer-provided health care and retirement plans), the lower tax rates and other benefits for capital gains (e.g., stepped-up basis at death), the deductibility of home mortgage interest, and three benefits targeted at those with lower incomes: the EITC, the child credit, and the credit for health insurance covered provided by the Affordable Care Act (ACA).[337] The significance of many of these items, especially these latter ones, has prompted the National Taxpayer Advocate to propose the IRS change its mission statement to reflect that it is not so

331. STANLEY S. SURREY, PATHWAYS TO TAX REFORM 6 (1973).

332. *Id.*

333. *Id.*

334. *Id.*

335. Tax incentives cover a wide array of economic activities. The Joint Committee on Taxation identifies the following tax expenditure budget groups: national defense; international affairs; general science, space, and technology; energy; natural resources and environment; agriculture; commerce and housing; financial institutions; transportation; community and regional development; education, training, employment, and social services; health and income security; social security and railroad retirement; veterans' benefits and services; and general purpose fiscal assistance. *See* JOINT COMM. ON TAXATION, 114TH CONG., ESTIMATES OF FEDERAL TAX EXPENDITURES FOR FISCAL YEARS 2015–2019, at 28–42 (2015), https://www.jct.gov/publications.html?func=startdown&id=4857 [https://perma.cc/93BQ-P22E]; OFFICE OF MGMT. & BUDGET, FISCAL YEAR 2016 BUDGET OF THE U.S. GOVERNMENT 119–24 (2015), https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/budget.pdf [https://perma.cc/7JPY-ALBU]; *see also* William McBride, *A Brief History of Tax Expenditures*, TAX FOUND. (2013), https://files.taxfoundation.org/legacy/docs/ff391.pdf [https://perma.cc/XW6H-N9N2].

336. First, there are different baselines for what constitutes a tax expenditure; some use the deviation from a normal tax, or a tax based on the Haig-Simons definition of income, whereas another approach is the reference tax law method, which analyzes deviations from the general rules of a tax law system. BITTKER & LOKKEN, *supra* note 312, ¶ 3.6. Second, a tax expenditure budget can look to revenue loss, to estimates of correspondence expenditures to duplicate the tax benefit, and time value of money losses from deferral of tax items. *Id.* Finally, tax expenditure budgets differ in their categorization of expenses. *Compare* OFFICE OF MGMT. & BUDGET, *supra* note 335, *with* JOINT COMM. ON TAXATION, *supra* note 335.

337. See the Tax Policy Center's assessment of 2016 tax expenditure items. TAX POLICY CTR., BRIEFING BOOK, http://www.taxpolicycenter.org/briefing-book/what-are-largest-tax-expenditures [https://perma.cc/AT79-BAYE].

much a tax collection agency as a social service agency.[338] Indeed, a recent study of the publication of new Treasury Regulations suggests that at least half, if not more than half, of what the IRS is concerned with these days is not related to tax collection.[339]

Purifying the income tax of tax expenditures and focusing the IRS on tax collection is a common call among tax reformers. For example, the Simpson-Bowles Commission recommended the elimination of all tax expenditure items except a few, such as those for employer-provided retirement benefits.[340] The National Taxpayer Advocate has suggested the presumption should be against tax expenditures, with rebuttal only if a "compelling business case can be made that the benefits of providing the tax incentive through the tax code outweigh the tax-complexity challenges."[341] The National Taxpayer Advocate has said "that the fundamental design question is whether a program would be better suited to the tax system or to a pure spending program," especially when the program is outside the revenue collection competence of the IRS.[342] Here specifically is concern for the antipoverty benefits that are clearly more social service-oriented than tax collector-oriented. With respect to the largest of these benefits, the EITC, Professor Michael Graetz has suggested it would be improved considerably by changing it from a refundable income tax credit to a payroll tax adjustment.[343]

There are also those who defend tax expenditures. Among academics, there has long been resistance to the claim that the tax law can be clearly divided between the "normal" taxing part and the suspicious "expenditure part."[344] Among politicians, there has long been recognition that some tax expenditures are so popular, that no one should suggest their elimination. For example, even the Simpson-Bowles Commission defended employer-provided retirement benefits. It is not only political popularity that protects at least some tax expenditures but also political consensus that one of the most significant antipoverty expenditures, the EITC, works well.[345]

---

338. NAT'L TAXPAYER ADVOCATE, 2010 ANNUAL REPORT TO CONGRESS 4, https://www.irs.gov/pub/tas/execsummary_2010arc.pdf [https://perma.cc/RZW5-DADE].

339. *See* Kristin E. Hickman, *Administering the Tax System We Have*, 63 DUKE L.J. 1717, 1749 (2014) (arguing the administrative functions of the IRS have transformed to program administration as opposed to revenue raising).

340. NAT'L COMM'N ON FISCAL RESPONSIBILITY & REFORM, *supra* note 324, at 31 n.6.

341. NAT'L TAXPAYER ADVOCATE, *supra* note 338, at 29.

342. *Id.* at 54.

343. Graetz, *supra* note 326, at 291–93.

344. *See* BITTKER & LOKKEN, *supra* note 312, ¶ 3.6; Boris I. Bittker, *Accounting for Federal "Tax Subsidies" in the National Budget*, 22 NAT'L TAX J. 244 (1969); Douglas A. Kahn & Jeffrey S. Lehman, *Tax Expenditure Budgets: A Critical View*, 54 TAX NOTES 1661 (1992).

345. Peter A. Muennig, Babak Mohit, Jinjing Wu, Haomiao Jia & Zohn Rosen, *Cost Effectiveness of the Earned Income Tax Credit as a Health Policy Investment*, 51 AM. J. PREVENTATIVE MED. 874 (2016), http://www.sciencedirect.com/science/article/pii/S0749379716302495 [https://perma.cc/2FP6-XZBS]; Chuck Marr, Chye-Ching Huang, Arloc Sherman & Brandon DeBot, *EITC and Child Tax Credit Promote Work, Reduce Poverty, and Support Children's Development, Research Finds*, CTR. ON BUDGET & POL'Y PRIORITIES (Oct. 1, 2015), http://www.cbpp.org/research/federal-tax/eitc-and-child-tax-credit-promote-work-reduce-poverty-and-support-childrens [https://perma.cc/3944-9875]; *Earned Income Tax Credit Program Is a Boon for Health, Report Suggests*, SCIENCEDAILY

Into this mix of considering the appropriate role of tax expenditures needs to be their relationship to cybersecurity. With respect to the information security recommendations described above, purifying the income tax of tax expenditures would succeed in reducing the amount of information required simply by reducing the number of benefits for which information is relevant. The effect would be similar to replacing itemized deductions with a standard deduction. However, unlike merely simplifying the income tax that way, eliminating all tax expenditures would also reduce the number of refunds paid and the number of individuals filing returns. Of the most significant tax expenditures are three administered as refunds: the EITC, the child care credit, and the ACA credit for health insurance coverage provided. The total "refunds" paid for these programs amounts to $134.4 billion.[346] As entitlement to these payments is not conditioned on tax liability, many individuals who file a tax return to claim one of these payments otherwise would not be filing a return.[347] Thus, the elimination of tax expenditures would contribute to improving the cybersecurity prospects of tax information by reducing the amount of information collected by the IRS, reducing the number of refunds paid by the IRS, and reducing the numbers of individuals filing returns.

4. Elite Income Tax

The individual income tax is a progressive tax.[348] By design, as one's income increases one's tax rate increases. In the past few years, some journalists have focused on reporting on circumstances in which the theoretical progressivity fails, and taxpayers with lower incomes have their income taxed at higher rates.[349] These circumstances are not surprising to tax experts, who understand progressivity as a general

---

(Sept. 7, 2016), https://www.sciencedaily.com/releases/2016/09/160907095442.htm [https://perma.cc/E8GG-VGJJ].

346. Payments of the EITC totaled $68.34 billion and were claimed on 28,537,908 returns. Credits of the Child Tax Credit totaled $27.20 billion and were claimed on 22,394,927 returns. Refundable payments of the Additional Child Tax Credit totaled $27.06 billion and were 20,225,421 returns. Payments of the Premium Tax Credit totaled $11.18 billion and were claimed on returns 113,468,824 (111,969,378 returns had a net premium tax credit payment, where net premium tax credits were claimed on 1,499,446 returns). INTERNAL REVENUE SERV., PUB. 4801, INDIVIDUAL INCOME TAX RETURNS, LINE ITEM ESTIMATES, 2014, https://www.irs.gov/uac/soi-tax-stats-individual-income-tax-returns-line-item-estimates [https://perma.cc/AKK9-QPCC].

347. In 2014, 24,644,1999 returns claimed the refundable portion of the earned income tax credit, meaning the tax liability was offset by withholding and other credits; 19,482,011 returns claimed the refundable portion of the child tax credit. *Table 3.3 All Returns: Tax Liability, Tax Credits, and Tax Payments, by Size of Adjusted Gross Income, Tax Year 2014 (Filing Year 2015)*, INTERNAL REVENUE SERV., https://www.irs.gov/statistics/soi-tax-stats-individual-statistical-tables-by-size-of-adjusted-gross-income [https://perma.cc/AY7Z-JRNF].

348. *See* I.R.C. § 1 (West 2014); *see also* BITTKER & LOKKEN, *supra* note 312, ¶ 3.6.

349. *See, e.g.*, Lori Montgomery, *Report: Quarter of Millionaires Pay Lower Tax Rate than Some in Middle Class*, WASH. POST (Oct. 12, 2011), https://www.washingtonpost.com/business/economy/report-one-in-four-millionaires-pays-less-in-taxes-than-the-middle-class/2011/10/12/gIQAh8XNfL_story.html [https://perma.cc/DF2R-7MTK]; Greg Sargent, Opinion, *Yup, the Buffett-and-His-Secretary Analogy Is Completely Accurate*, WASH. POST

rule and tax rates variable on income source as an exception.[350] However, as a matter of politics, the call to ensure progressivity in fact and not just theory is one that has gained traction.[351]

It is one matter to push for ensuring progressivity, but a different one to push for increasing progressivity. It is one argument that progressivity requires Warren Buffett to pay tax at a higher rate than his secretary.[352] It is another argument that Warren Buffett's tax rate ought to be much, much higher than his secretary's. There is increasing popular interest in the income and wealth inequality in the United States, and that has led to calls for increasing the tax rates on those with the highest levels of income and wealth.[353] Taken to its extreme, this would be a call for imposing an income tax only on those with the highest levels of income.

Pushing progressivity to the point that the income tax was only a tax on those with the highest levels of income would be returning the income tax to its earliest form. For about the first quarter of the century of the income tax's history, it was an elite tax.[354] It was imposed on only about two percent of American households.[355] The income tax was transformed into a mass tax as a result of the decision to pay for World War II with increased tax revenue.[356] An elite income tax simply did not generate the revenue needed. However, at the time, it was not a foregone conclusion that the additional revenue would be collected by expanding the income tax. Indeed, for quite some while, the congressional preference was to keep the income tax as an elite tax and increase federal revenue with a federal sales tax.[357] President Roosevelt,

---

(Oct. 13, 2011), https://www.washingtonpost.com/blogs/plum-line/post/yup-the-buffett-and-his-secretary-analogy-is-completely-accurate/2011/10/13/gIQAj3NYhL_blog.html [https://perma.cc/CF9A-BYFT].

350. *See* BITTKER & LOKKEN, *supra* note 312, ¶¶ 2.2, 46.2.3.

351. *Bernie Sanders on Tax Reform*, ONTHEISSUES, http://www.ontheissues.org/2016/Bernie_Sanders_Tax_Reform.htm [https://perma.cc/P7DY-6W3B].

352. Warren E. Buffett, Opinion, *Stop Coddling the Super-Rich*, N.Y. TIMES (Aug. 14, 2011), http://www.nytimes.com/2011/08/15/opinion/stop-coddling-the-super-rich.html [https://perma.cc/9MFL-KU44]; Angie Drobnic Holan, *Does a Secretary Pay Higher Taxes than a Millionaire?*, POLITIFACT (Sept. 21, 2011, 12:25 PM), http://www.politifact.com/truth-o-meter/article/2011/sep/21/does-secretary-pay-higher-taxes-millionaire [https://perma.cc/C6LH-757K]; Chris Isidore, *Buffett Says He's Still Paying Lower Tax Rate than His Secretary*, CNN MONEY (Mar. 4, 2013, 11:20 AM), http://money.cnn.com/2013/03/04/news/economy/buffett-secretary-taxes [https://perma.cc/GK7R-7D9R]; Rachel Tiede, *Clinton Correct Buffett Claimed To Pay a Lower Tax Rate than His Secretary*, POLITIFACT (Oct. 18, 2016, 4:52 PM), http://www.politifact.com/truth-o-meter/statements/2016/oct/18/hillary-clinton/clinton-correct-buffett-claimed-pay-lower-tax-rate [https://perma.cc/8JPT-RKGK].

353. Lawrence Summers, Opinion, *Larry Summers: Changing the Tax Code Could Help Curb Inequality*, WASH. POST (Feb. 16, 2014), https://www.washingtonpost.com/opinions/larry-summers-changing-the-tax-code-could-help-curb-inequality/2014/02/16/9e9c736e-9595-11e3-afce-3e7c922ef31e_story.html [https://perma.cc/KS8Y-6NF2].

354. BROWNLEE, *supra* note 154, at 57.

355. *Id.*

356. *Id.* at 115–19.

357. *See* Lawrence A. Zelenak, *The Federal Retail Sales Tax That Wasn't: An Actual History and an Alternate History*, 73 L. LAW & CONTEMP. PROBS. 149, 205 (2010) (detailing

however, insisted on expanding the income tax to a mass tax, and this was made practical by the introduction of withholding from wages on the mass of new taxpayers.[358]

Any push to transform the income tax into an elite tax runs into the reality that such a tax is an insufficient revenue source. It is not feasible to gather the revenue needed from the highest income individuals. However, at least one recent proposal echoes the initial congressional approach during World War II. Professor Michael Graetz has proposed aiming the income tax only on the elites, but supplementing the income tax with a consumption tax.[359] Under his proposal, no family with an income less than $100,000 would be taxed on the income.[360] Those making over the exempted amount would be pay under a scheme comparable to the current alternative minimum tax, meaning their tax liability would be determined with a reduced number of deductions.[361]

Any debate over an elite income tax should be enlarged to include discussion of its cybersecurity impact. In terms of improving information security, the chief benefit of transforming the income tax into a tax only on the elite would be reducing the number of individuals covered. Professor Graetz estimates his proposal would eliminate 100 million individual filers from the system.[362] Whether or not the taxable elite would report less information under the current income tax would depend on the details of the new tax structure. For example, if the new tax were similar to the one envisioned by Professor Graetz, less information would be collected as there would be fewer deductions available. Of course, the number of refunds would be reduced as a matter of reducing the number of taxpayers.

5. Federal Sales Tax

Americans are familiar with the retail sales taxes most states impose.[363] A sales tax may be construed as a tax on the retailer for the privilege of engaging in the retail sales business or as a tax on the retail buyer.[364] Either way, even though it is the buyer who bears the economic burden of the tax, the retailer is the one responsible to collect

---

the history of the Roosevelt administration's rejection of a federal sales tax and the long-term impact of the choice to solely implement an income tax).

358. *Id.* at 149–53.

359. Graetz, *supra* note 326, at 295–97.

360. *Id.*

361. *Id.*

362. *Id.*

363. *See* CHARLES A. TROST, FEDERAL LIMITATIONS ON STATE AND LOCAL TAX § 11:1 (2d ed. 2016) (forty-five states and the District of Columbia).

364. ALL STATES TAX GUIDE, P 5071 (2017), https://1.next.westlaw.com/Document/I5eea8c5eb33d11de9b8c850332338889/View/FullText.html?transitionType=Default&contextData=(sc.Default). The use tax is a complement to the sales tax. It is imposed on the use, storage, withdrawal, or consumption of tangible personal property within the jurisdiction, though it is not levied on goods on which the sales tax has been paid. As a result, it primarily applies on goods purchased outside the taxing jurisdiction. It allows the taxing authority to tax the use of the goods even though the authority would not have the constitutional authority to impose a tax on the transportation of the goods from another state. TROST, *supra* note 363, § 11:1.

the tax due on the sale and pay it to the state.[365] The tax is imposed on the sales price of tangible personal property, usually at a flat rate.[366] Usually, retailers must file returns and pay the tax on a monthly or quarterly basis, though retailers with low tax receipts may file less frequently, while other retailers may provide estimated tax reports and payments. Unlike retail buyers, wholesale buyers (i.e., those buying for resale) are exempt from paying tax on their purchasers.[367] Most states also exempt "purchases made by nonprofit charitable, educational, and religious organizations,"[368] as well as a variety of other retail buyers, such as federal and state government agencies and instrumentalities.[369] It is also common for states to exempt certain sales from the tax, such as drugs, medical supplies, and food.[370]

Historically, and even to this day, the federal government does impose taxes on the sales of certain items, such as alcohol, tobacco products, and fuel-inefficient cars.[371] However, the federal government has never imposed a general sales tax. The widespread use of sales taxes by the states was in response to fiscal emergencies of the states during the Great Depression of the 1930s.[372] As mentioned above, Congress did seriously consider a national sales tax in the 1940s, which would have been imposed in lieu of transforming the income tax from an elite tax to a mass tax, but President Roosevelt persuaded Congress to transform the income tax instead.[373]

Over the past two decades, there has been a consistent but unsuccessful effort to replace that income tax with a national sales tax. In 1996, a House bill was introduced to implement a fifteen percent sales tax on most goods and services, but with an annual rebate to all wage earners based on the sales tax rate applied to the national poverty level and delivered through reduced withholding in order to ensure progressivity.[374] Following a Canadian model, it was intended to be administered

---

365. ALL STATES TAX GUIDE, *supra* note 364, at P 5068, 5071. Even though in some sense the buyer is the taxpayer, the retailer—as the one held responsible—is the only one entitled to bring legal claims against the state regarding the tax.

366. *Id.* at P 5375, 5225, 5465.

367. *Id.* at P 5074.

368. *Id.* at P 5111.

369. *Id.* at P 5090.

370. *Id.* at P 5315 (exemption for drugs and medical supplies); *id.* at P 5320 (exemption for food sold for human consumption off-premises).

371. *See, e.g.*, I.R.C. §§ 5001, 5041, 5051 (Westlaw through Pub. L. 115-97) (imposition of excise taxes on production and importation of distilled spirits, wine, and beer respectively); *id.* § 5701 (imposition of excise tax on the production or importation of tobacco products); *id.* § 4121 (imposition of excise tax on coal manufacture); *id.* § 4081 (imposition of various excise taxes on gasoline); *id.* § 4064 (imposition of excise tax on the manufacture of "gas guzzlers"). In 2009, the total of federal excise taxes amounted to $66 billion. U.S. BUREAU OF THE CENSUS, STATISTICAL ABSTRACT OF THE UNITED STATES: 2010, at 308 tbl.463 (129th ed. 2009).

372. TROST, *supra* note 363.

373. *See* Zelenak, *supra* note 357, at 149–50.

374. H.R. 3039, 104th Cong. (1996) (sponsored by Representatives Dan Schaefer, Dick Chrysler, and Billy Tauzin); *id.* § 1 (tax of fifteen percent on most goods and services); *id.* § 15(c) (rebate to families based on poverty level). *See generally* Burton & Mastromarco, *supra* note 298.

primarily by the states collecting the tax and paying it to the federal government.[375] In 1999, a similar proposal was introduced in both the House and the Senate, giving the movement the proposal's name: the "Fair Tax."[376] The current Fair Tax proposal generally follows the 1996 approach but would apply a much higher rate.[377] While the proposal has been popularized especially among Republicans in the Southeast, its popularity has not spread.[378] Critics doubt it would generate sufficient tax revenue, especially given the potential for evasion with retailers responsible for reporting, collecting, and remitting such a tremendous amount.[379]

Arguing over the appropriate role of sales tax in federal revenue should include arguments over its potential to improve cybersecurity. Whatever its other shortcomings, a national sales tax similar to the Fair Tax proposal would succeed on the three recommendations for improving cybersecurity. First, refunds as known in the current income tax system would be eliminated. Second, the amount of information collected would be minimal. The only relevant information would be the amount of the sale and whether or not it was taxable or exempt. Third, the number of individuals covered by the system would be minimized. Only retailers would file returns, though wage-earners would provide household information relevant to determining the amount of the annual rebate.

6. Value-Added Tax (VAT)

Although economically equivalent to a sales tax in how the tax is borne, a value-added tax (VAT) is administratively quite different. Unlike a sales tax, in which all of the tax due is collected at a single moment—that is, the moment of the sale—a VAT collects incrementally. It is this incremental collection that makes it

375. H.R. 3039 §§ 31(e)(2), 33; *see also* Burton & Mastromarco, *supra* note 298, at 1241 n.32 (discussing similar system employed in Quebec to collect both the federal goods and services taxes and the provincial sales tax). On using state taxing authorities to collect a federal sales tax, see John A. Miller, *State Administration of a National Sales Tax: A New Opportunity for Cooperative Federalism*, 9 VA. TAX REV. 243 (1989) (arguing for the administrative benefits of states collecting a national sales tax).

376. H.R. 2525, 106th Cong. (1999).

377. Fair Tax Act of 2015, S. 155, 114th Cong. (2015); FairTax Act of 2015, H.R. 25, 114th Cong. (2015).

378. Ryan Lovelace, *The FairTax Makes a Comeback*, NAT'L REV. (Jan. 22, 2015, 4:00 A.M.), http://www.nationalreview.com/article/412527/fairtax-makes-comeback-ryan-lovelace [https://perma.cc/PJ7F-UFBK].

379. *See, e.g.*, Bruce Bartlett, *Why the FairTax Won't Work*, 117 TAX NOTES 1241 (2007); William G. Gale, *Don't Buy the Sales Tax*, BROOKINGS INST. (Mar. 1, 1998), https://www.brookings.edu/research/dont-buy-the-sales-tax [https://perma.cc/R6NC-R64Q]; Tim Worstall, *Why the Fair Tax Will Fail*, FORBES (Aug. 22, 2012, 11:24 A.M.), http://www.forbes.com/sites/timworstall/2012/08/22/why-the-fair-tax-will-fail/#64b3d80964d0 [https://perma.cc/ZW55-7PKW].

administratively superior. Consider the following example.[380] Compare a retail sales tax of 10% and a VAT of 10% applied to a gallon of milk with a retail price of $1. Under the retail sales tax, when the grocer sells a gallon, it collects ten cents, which it then remits to the government. If the grocer fails to collect the ten cents, or collects it but fails to remit it, the tax is lost. Under a VAT, the same ten cents will be collected, but incrementally. When the farmer sells a gallon of raw milk to the dairy for fifty cents, the famer collects five cents from the dairy and remits it. When the dairy sells the bottled gallon to the grocer for eighty cents, it would collect eight cents of tax but only pay three cents to the government. It would only pay three cents because it sold the milk for thirty cents more than it paid, so the 10% tax is only three cents. On the government's tax books, the dairy would be credited the five cents it paid to the farmer. When the grocer sells the gallon to the retail purchaser for one dollar, it would collect ten cents from the purchaser. It would only pay two cents to the government, as the government would have credited it for the eight cents it paid to the dairy. The two cents is ten percent of the value added by the grocer. In the end, the retail purchaser pays ten cents tax, but the government collects five cents from the farmer, three cents from the dairy, and two cents from the grocer. The total ten cents was never at risk. The dairy has an interest in ensuring the farmer paid five cents, so that the dairy would get its credit, and the grocer had an interest in ensuring that the dairy had paid its three cents, so that the grocer would get its credit.

The VAT works so well that the United States is the only member of the Organisation for Economic Cooperation and Development (OECD) not to use it.[381] Indeed, membership in the EU requires the use of the VAT.[382] The VAT (in one variation or another) has a history of academic advocates.[383] Its effectiveness has

---

380. This example illustrates an invoice-credit method VAT, which is but one of several types but is the most commonly used. *See* OLIVER, *supra* note 300, at 383 (discussing this example and some of the more complicating details).

381. Kyle Pomerleau, *Sources of Government Revenue Across the OECD, 2015*, TAX FOUND. (Apr. 30, 2015), http://taxfoundation.org/article/sources-government-revenue-across-oecd-2015 [https://perma.cc/U32U-5NDK]. The OECD is an intergovernmental organization comprising many of the world's developed economies. It focuses on improving the economic and social well-being of people around the world. *About the OECD*, ORG. FOR ECON. CO-OPERATION & DEV., https://www.oecd.org/about [https://perma.cc/NB24-CMEN].

382. *See* BERT LAMAN, EUROPEAN VALUE ADDED TAX (VAT), PRAXITY 7 (2013), http://www.bkd.com/docs/solution-sheets/european-value-added-tax.pdf [https://perma.cc/F7YS-UYHR].

383. *See, e.g.*, Michael J. Graetz, *The U.S. Income Tax: Should It Survive the Millennium?*, 85 TAX NOTES 1197 (1999) [hereinafter Graetz, *U.S. Income Tax*]; Graetz, *supra* note 326, at 289–90; Michael J. Graetz, *Taxes That Work: A Simple American Plan*, 58 FLA. L. REV. 1043 (2006) [hereinafter Graetz, *Taxes that Work*] (arguing for a dual system of a VAT and an elite income tax to simplify tax administration); Alan Schenk, *Radical Tax Reform for the 21st Century: The Role for a Consumption Tax*, 2 CHAP. L, REV. 133 (1999) (detailing the history of post-war tax administration and arguing that the United States' rejection of a consumption tax makes it an outlier in other advanced economies); Alan Schenk, *Value Added Tax: Does This Consumption Tax Have a Place in the Federal Tax System?*, 7 VA. TAX REV. 207 (1987) (arguing that the imposition of a VAT fails to account for equity, would have few economic benefits, and may be administratively burdensome).

made it popular among political liberals, especially when combined with the income tax, as Professor Michael Graetz has suggested.[384] It also is popular among political conservatives, who, however, propose it not as an addition to the income tax but as a replacement for it.[385] A bill to implement a federal VAT was first introduced in 1979.[386] The Treasury Department has issued a formal report on the use of the VAT.[387] And, the American Bar Association Section on Taxation has drafted a model VAT statute.[388] Nonetheless, the VAT remains on the sidelines, awaiting a political game change.

While the debate over the VAT has been fairly well rehearsed at this point, perhaps it would be enlivened by adding cybersecurity calls to the voices. In terms of improving information security, the benefit of a VAT would be like those of a national sales tax. There would not be hundreds of millions of refunds to individuals. The relevant information is no more than the amount of the sale and the information relevant to claiming the credit on the resale. The number of taxpayers covered would be substantially fewer than under the income tax but more than under a sales tax. Under the sales tax, only retailers would be burdened with collecting and paying tax, while under a VAT, all those involved in the production of the items sold by the retailer also would be involved. Of course, these would be business taxpayers rather than individuals as such.

---

384. *See, e.g.*, Lori Montgomery, *Once Considered Unthinkable, U.S. Sales Tax Gets Fresh Look*, WASH. POST (May 27, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/05/26/AR2009052602909.html [https://perma.cc/G7PV-R8U2] (quoting Democratic Senator Kent Conrad saying, "a VAT and a high-end income tax have got to be on the table"); Editorial, *Mrs. Pelosi's VAT*, WALL ST. J. (Oct. 8, 2009, 12:01 A.M.), https://www.wsj.com/articles/SB10001424052748703298004574457512007010416 [https://perma.cc/BW9F-XV6P] (quoting Democratic House Speaker Nancy Pelosi as saying, "somewhere along the way, a value-added tax plays into this"). For a description of other liberal politicians supporting a VAT, see OLIVER, *supra* note 300, at 381. For Professor Graetz's proposal to combine an elite income tax and a VAT, see Graetz, *supra* note 326, at 290; Graetz, *Taxes that Work*, *supra* note 383, at 1051.

385. *See, e.g.*, Charles Krauthammer, Opinion, *Obamacare's Next Trick: The VAT*, WASH. POST (Mar. 26, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/03/25/AR2010032502406.html [https://perma.cc/E8K9-P858] (conservative political commentator writes, as "a substitute for the income tax, the VAT would be a splendid idea" but not as a supplement for it); George F. Will, *The Perils of the Value-Added Tax*, WASH. POST (Apr. 18, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/04/16/AR2010041603993.html [https://perma.cc/A4BQ-PSZM] (conservative political commentator writes that a VAT could be used to restore fiscal discipline, but if combined with the income tax, would become a "gargantuan" tax instrument). For a description of other political conservatives supporting a VAT and similar proposals, see OLIVER, *supra* note 300, at 382.

386. Tax Restructuring Act of 1979, H.R. 5665, 96th Cong. (1979) (proposed by Oregon Congressman Ullman, the Chair of the Ways and Means Committee).

387. U.S. DEP'T OF THE TREASURY, TAX REFORM FOR FAIRNESS, SIMPLICITY, AND ECONOMIC GROWTH (vol. 3 1984).

388. AM. BAR ASS'N, SECTION OF TAXATION, VALUE ADDED TAX: A MODEL STATUTE AND COMMENTARY (1989).

7. Comparison of Proposals

The degree to which any of the proposals succeeded at reducing refunds, requiring less information, or reducing the number of individuals covered by the system would depend on the final details. The chart below, however, summarizes a comparison of proposals on these three points, presuming that the proposals were each adopted alone. That is fairly unlikely in some instances, and it would be the combination of proposals that would achieve the best combination of strengths. For example, a PAYE could not be implemented without substantially simplifying or purifying the income tax as the current income tax system is just too complicated and pursues too many goals for PAYE to work. While an elite income tax would not logically require other changes, its revenue levels would be too low to be implemented without a complementary tax, such as a sales tax or VAT. Similarly, neither a sales tax nor a VAT likely would generate sufficient revenue to be enacted independently and would need to be complemented by an income tax. Putting aside each proposal's revenue potential, equity, efficiency, administrative burdens, and political viability, the following figure highlights each proposal's likely impact on improving information security at the IRS.

	Fewer Refunds	Less Information	Fewer Individuals
PAYE	**X**		
Simplified Income Tax		**X**	
Purified Income Tax	**X**	**X**	**X**
Elite Income Tax			**X**
Sales Tax	**X**	**X**	**X**
VAT	**X**	**X**	**X**

Table 1

CONCLUSION

This Article is realistic about information technology. This technology allows us to do more than we can do safely. Perhaps someday it will enable us to do safely all that we want it to do. Probably that day would come sooner if we were more realistic, more modest about what it is we really need it to do. Unfortunately, today, too much information held by the government is vulnerable to being stolen, manipulated, or deleted by criminals, terrorists, or hostile governments.

This Article proposes a way forward for the information technology security of the treasure trove of federal tax information held by the government. There is much more flexibility for deciding how much and what type of tax information is truly needed than there is flexibility to decide how secure the technology will be. Our imagination as to how the technology can be used will never weaken our pushes to do more with it. But our recognition of the real security limits of the technology should push us to being more selective and cautious as to what we try do with the technology.

This Article argues that Congress has ample flexibility to devise a tax system that raises the revenue needed in a fair and efficient way but does so while demanding less information be collected, stored, and processed by the IRS. These types of reforms will do more to improve the cybersecurity of the IRS system than the IRS would ever be able to do through its own technology resources. Congress, rather than the IRS, is the institution most capable of and most responsible for solving the problem. Cybersecurity for tax information should be considered more as a tax code problem than a computer code problem.

This Article commends a particular approach to legislation in this dawning digital age. In the coming decades, more and more attention will need to be given to the relationship between legislation and digital technology. Congress needs to assess how federal agencies will need—or want, or try—to use newer and newer technology to administer the legislation Congress negotiates. Laws that were drafted when practical barriers meant very little of the relevant information would ever be collected, except perhaps in the most important or litigated situations, seem quite different when technology will allow almost all of the relevant information almost always to be collected. Congress ought to consider carefully the relationship between its legislation and federal agencies' technological aspirations, carefully considering what it is they are effectively tasking the agencies to do with their technology and, even more carefully, considering what the consequences of using that technology for those purposes likely will be. That the information technology used by government agencies is being tasked to do more than it can do safely is not the fault of agency employees, but rather it is the fault of those who cobble together the legislation for the agencies to administer.