TEMPLE LAW REVIEW

VOL. 90 NO. 3 **SPRING 2018**

ARTICLES

TAX PRIVACY?

Adam B. Thimmesch[*]

"Nothing is secret from us anymore."
– Tom Bishop, IRS Criminal Investigations[1]

ABSTRACT

The academic literature addressing privacy in the context of the U.S. tax system has generally discussed tax privacy as nothing more than a limited right of confidentiality. That literature fails to account for the broader range of privacy interests identified in the general privacy literature. In turn, the privacy scholarship has failed to account for the vast information flows that occur in our tax system. This Article addresses that disconnect by evaluating tax privacy through the lens of that broader literature. It shows that some privacy conceptions might support a limited view of tax privacy on the surface but that there are significant reasons to doubt that tax privacy should be as narrow as mere confidentiality. The Article thus proposes a tax-privacy framework that draws from the strengths of each different privacy conception without adopting any one conception as correct. That

* Associate Professor of Law, University of Nebraska College of Law. This Article benefited from the thoughts and comments of many kind colleagues, including Alice Abreu, Eric Berger, Michael Hatfield, Hayes Holderness, Jessica Shoemaker, and Maggie Wittlin. I also owe thanks to the participants at the 2016 Junior Tax Scholars' Workshop, the Fourth Annual Junior Faculty Works-in-Progress Conference at Marquette University, the 2016 Law & Society Annual Meeting, the University of Washington Fourth Annual Tax Symposium, the 2016 Southeastern Association of Law Schools Annual Conference, and the University of Nebraska College of Law's Faculty Workshop Series. Finally, thank you to the *Temple Law Review* editors for your careful work and helpful suggestions. All errors and omissions are my own.

1. Mindy Herzfeld (@InternationlTax), TWITTER (Oct. 28, 2016, 11:56 AM), http://twitter.com/InternationlTax/status/792077655646633984 [perma: http://perma.cc/G6QT-YNBL].

framework provides a foundation for future work in this area even though the more general concept of privacy continues to be debated. The Article concludes by identifying the top tax-privacy issues that should be addressed in the near term—the secondary use of tax information and the security of tax information.

TABLE OF CONTENTS

INTRODUCTION

The meaning and importance of privacy is unclear in today's society. At times, privacy appears to be an anachronism. We now share an immense amount of personal information on social media, subject ourselves to online data tracking, and even buy devices that eavesdrop on the conversations in our own homes.[2] At the same time, though, we often express discomfort with how our information is used and communicate a desire for greater privacy protections.[3] Scholars also broadly critique the collection and use of data by the government and by private companies like Google and Facebook.[4] The concept of privacy is thus evolving, but it continues to be the subject of intense debate.

Concurrent with these broader discussions, the topic of tax privacy is starting to emerge as a field of interest. To date, "tax privacy" has been synonymous with "tax confidentiality," but scholars are beginning to think of the concept more broadly.[5] For example, recent papers have questioned the quality and quantity of information collected by the government for tax purposes, how the government is using big data in tax administration, and how governments worldwide are sharing tax information.[6] This broader focus makes sense. The

2. *See, e.g.*, *Amazon Echo*, AMAZON, http://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E [perma: http://perma.cc/SH95-2YBL] (last visited May 14, 2018). The use of the plural pronoun "we" is not intended to suggest that *all* individuals engage in this behavior, but to indicate a common practice among contemporary Americans. As discussed throughout this Article, individual beliefs about privacy differ significantly, and many people eschew these modern practices precisely to protect their privacy.

3. *See* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [perma: http://perma.cc/TB2S-967U] (summarizing the results of surveys regarding Americans' attitudes about privacy and concluding that they have "exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age"). Individuals also take a variety of privacy-protecting actions, like browsing in privacy mode, using virtual private networks, and even putting tape over their laptop cameras. *See id.* Even Mark Zuckerberg puts tape over his laptop camera. Katie Rogers, *Mark Zuckerberg Covers His Laptop Camera. You Should Consider It, Too.*, N.Y. TIMES (June 22, 2016), http://www.nytimes.com/2016/06/23/technology/personaltech/mark-zuckerberg-covers-his-laptop-camera-you-should-consider-it-too.html [perma: http://perma.cc/J4W8-QFBK].

4. *See generally, e.g.*, James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009) (discussing the privacy aspects of Facebook); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) (discussing the privacy dangers of governmental and nongovernmental surveillance); David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1073 (2014) (discussing a shift in the literature to evaluations of the privacy aspects of data collection by private companies); Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433 (discussing the privacy implications of data tracking by private companies).

5. *See, e.g.*, Michael Hatfield, *Privacy in Taxation*, 44 FLA. ST. U. L. REV. (forthcoming 2018) [hereinafter Hatfield, *Privacy in Taxation*].

6. *See id.*; *see also* Arthur J. Cockfield, *Big Data and Tax Haven Secrecy*, 18 FLA. TAX REV. 483, 502–05 (2016) [hereinafter Cockfield, *Big Data*] (discussing the privacy aspects of big data and multijurisdictional tax enforcement efforts); Arthur J. Cockfield, *How Countries Should Share Tax Information*, 50 VAND. J. TRANSNAT'L L. 1091, 1096–1108 (2017) [hereinafter Cockfield, *How Countries Should Share*] (noting the differential privacy rights that exist across the globe); Steven A.

U.S. tax system is built on information collection, and it touches nearly every aspect of taxpayers' lives. The Internal Revenue Service (IRS) collects information about taxpayers' medical conditions, the sleeping arrangements in their homes, their sexual histories, the terms of their divorce agreements, and even the types of appliances that they own.[7] It uses Stingray devices to capture information sent over the cellular networks and monitors taxpayers' social media accounts.[8] Congress and the IRS are also prioritizing making tax services available online even though the IRS has shown a vulnerability to data breaches.[9] In all, tax information flows extensively in today's world without any significant privacy critique. One scholar has responded to this situation by labeling tax privacy as "a bomb waiting to go off."[10]

Given this backdrop, it is fortunate that tax privacy is starting to get more attention. But as scholars begin to think about tax privacy more broadly, it is essential to realize that privacy is an inherently uncertain concept. To claim that a particular tax practice "violates privacy" is to beg the broader questions of what privacy is and when it is harmed. For example, does it really harm taxpayers' privacy if the Tax Code requires them to disclose their dependents? What about if taxpayers are required to disclose their medical expenses in order to claim a deduction? Is there any harm that stems from the IRS aggregating taxpayer information if it does not use it for some nefarious purpose? Would we really change the Tax Code to prevent these situations?

Dean, *The Incomplete Global Market for Tax Information*, 49 B.C. L. REV. 605, 668–70 (2008) (discussing the privacy aspects of international exchanges of tax information); Kimberly A. Houser & Debra Sanders, *The Use of Big Data Analytics by the IRS: Efficient Solution or the End of Privacy as We Know It?*, 19 VAND. J. ENT. & TECH. L. 817, 819–20 (2017) (discussing the IRS's use of taxpayer data and data analytics).

7. See *infra* Parts I.A and I.B for a discussion of the information-collection powers of the IRS. Tax scholars and economists also continue to evaluate whether and how taxpayers could be "tagged" or screened by certain characteristics to better structure optimal tax instruments. *See, e.g.*, George A. Akerlof, *The Economics of "Tagging" as Applied to the Optimal Income Tax, Welfare Programs, and Manpower Planning*, 68 AM. ECON. REV. 8, 8 (1978); Lily L. Batchelder, *What Should Society Expect from Heirs? The Case for a Comprehensive Inheritance Tax*, 63 TAX L. REV. 1, 23 (2009) (discussing the use of inheritances as a tag); Kyle Logue & Joel Selmrod, *Genes as Tags: The Tax Implications of Widely Available Genetic Information*, 61 NAT'L TAX J. 843, 848–51 (2008) (discussing the use of genetic information as a tag); N. Gregory Mankiw & Matthew Weinzierl, *The Optimal Taxation of Height: A Case Study of Utilitarian Income Redistribution*, 2 AM. ECON. J. 155, 156, 174–76 (2010) (discussing the use of height as a tag); Leigh Osofsky, *Who's Naughty and Who's Nice? Frictions, Screening, and Tax Law Design*, 61 BUFF. L. REV. 1057, 1074–81 (2013) (discussing the use of screening mechanisms, like tagging, in optimal tax theory); Alex Raskolnikov, *Accepting the Limits of Tax Law and Economics*, 98 CORNELL L. REV. 523, 563 (2013) (listing potential characteristics that could be used as proxies for ability to pay). Using these tags or screens necessarily requires that the government collect the underlying data. *See* Osofsky, *supra*, at 1080.

8. *See* Houser & Sanders, *supra* note 6, at 822–23; Nicky Woolf & William Green, *IRS Possessed Stingray Cellphone Surveillance Gear, Documents Reveal*, GUARDIAN (Oct. 26, 2015, 8:25 AM), http://www.theguardian.com/world/2015/oct/26/stingray-surveillance-technology-irs-cellphone-tower [perma: http://perma.cc/8CT9-5TJS].

9. See *infra* notes 73–77 and accompanying text for a discussion of online tax services and the issues the IRS has faced surrounding data breaches.

10. Ryan Calo, *Privacy and Markets: A Love Story*, 91 NOTRE DAME L. REV. 649, 680 (2015).

These are not easy questions to answer because people view privacy very differently. Some view it broadly and define privacy as control over information or the state of perfect isolation.[11] Others define privacy by reference to normative values, or to the nature of the underlying information, or even the methods by which information is disclosed.[12] This variance in opinion significantly complicates the newfound interest in tax privacy. For those interested in protecting taxpayer privacy more than we do today, it will not suffice merely to say that a tax provision harms privacy and that it therefore must be changed. They will have to explain why and how a current or proposed tax choice actually harms privacy and why the privacy interest at stake should prevail over the other end being sought—generally the collection of revenue in a way that is efficient, equitable, and administrable.[13]

This Article addresses those issues and sets the stage for more meaningful discussions of tax privacy by grounding those discussions in existing privacy theory.[14] Specifically, it outlines and critiques the potential meaning of tax privacy under three different approaches that have developed in the broader privacy literature: (1) a broad, neutral approach; (2) a normative approach; and (3) a context-dependent approach.[15] The Article shows that a neutral approach to tax privacy would identify deviations from "perfect" privacy and would indicate that nearly every tax choice comes with privacy loss, but it would provide no guidance on whether, when, or how we should respond to such losses.[16] The second approach to tax privacy, a normative approach, would address that issue by focusing on where the tax system impacts privacy problematically.[17] The weakness of that approach, however, is that there is no uniformly accepted normative framework to evaluate privacy more generally, much less to apply to tax privacy specifically.[18] As a result, it is not clear that this way of viewing tax privacy would do much as a practical matter. The final

11. See *infra* Part II.A for a discussion of what constitutes privacy.

12. See *infra* Part II.B for a discussion of the concept of tax privacy.

13. These three interests are the hallmarks of tax policy analyses. *See* Neil H. Buchanan, *The Role of Economics in Tax Scholarship*, *in* BEYOND ECONOMIC EFFICIENCY IN UNITED STATES TAX LAW 11, 11 (David A. Brennen, Karen B. Brown & Darryll K. Jones eds., 2013); Victor Fleischer, *A Theory of Taxing Sovereign Wealth*, 84 N.Y.U. L. REV. 440, 497–98 (2009) (labeling these three interests as "the traditional tax policy goals"); Leandra Lederman, *"Stranger than Fiction": Taxing Virtual Worlds*, 82 N.Y.U. L. REV. 1620, 1658 (2007) (noting that these three interests are "[t]he tax policy concerns usually considered in evaluating the appropriateness of a tax or provision"); Shu-Yi Oei, *Getting More by Asking Less: Justifying and Reforming Tax Law's Offer-in-Compromise Procedure*, 160 U. PA. L. REV. 1071, 1082 (2012) (identifying these interests as the "three traditional criteria of tax policy analysis").

14. The Article largely focuses on the privacy impacts of the federal personal income tax. It does not consider the privacy impacts of other taxes like the corporate income tax. The underlying privacy interests of a corporate entity are different than those discussed herein. *See generally* Joshua D. Blank, *Reconsidering Corporate Tax Privacy*, 11 N.Y.U. J.L. & BUS. 31 (2014) [hereinafter Blank, *Reconsidering Corporate Tax Privacy*] (discussing corporate privacy interests).

15. See *infra* Parts II.B–D for a discussion of these different privacy conceptions.

16. *See infra* Part II.B.

17. *See infra* Part II.C.

18. *See infra* Part II.C.

approach, a context-dependent approach, would suggest that tax privacy is best understood as a set of expectations regarding the use of our tax information and could explain the apparent inconsistencies that we observe in how we approach privacy generally and tax privacy more specifically.[19] That approach is intellectually appealing and seems to best reflect how people intuitively think about privacy. The context-dependent approach, however, is also imperfect. Specifically, it presumes that individuals optimally manage their own privacy and that current norms reflect those optimal choices. Both propositions are arguable at best.[20]

So how do we define or begin to think about tax privacy given the unsettled theoretical foundation? This Article considers that issue not by attempting to provide some unifying theory of privacy,[21] but by showing how the different ways of thinking about privacy can be used together to address tax privacy in a more comprehensive, intentional way. The first step is acknowledging, consistent with a neutral privacy conception, that privacy is about much more than just confidentiality.[22] We might not pursue "perfect" tax privacy, but looking at tax privacy though a neutral lens would help us to be more aware of the potential privacy harms of our tax choices and should also result in an approach to tax design that differs from current practice. Privacy interests impact equity, efficiency, and administrability just like economic interests impact those factors, but privacy interests cannot be considered in tax design if they are not first recognized.

Once our collective view of tax privacy is broadened beyond a limited interest in confidentiality, normative and context-dependent approaches to privacy can help us to prioritize our responses even if we disagree with the exact values, goals, or tradeoffs inherent in those approaches. The precise meaning of privacy will always be debated, but modern privacy theory can guide us in developing a tax system that more optimally considers taxpayers' privacy interests. In that vein, the Article provides a method for making those normative judgments and identifies the most pressing of tax-privacy goals in the near term—evaluating the secondary use of taxpayer information and addressing data security.

These issues stand out as particularly important for many reasons. As a practical matter, our collective lack of agreement on the nature or value of privacy will likely mean that reform efforts to address other tax-privacy goals (like limiting the amount of information collected by the government or by third parties) will be subject to more intense scrutiny and fail to overcome the public's interest in collecting or using taxpayer information for tax purposes. The

19. *See infra* Part II.D.

20. *See infra* Part II.E.

21. To do that would be to accomplish a feat that privacy scholars themselves have found elusive.

22. "Confidentiality," for these purposes, refers to the general expectation that the information shared between two parties not be shared either outside of those parties or outside of a limited group of people who are expected to have access to the information.

situation is very different when taxpayer information is used for other, nontax purposes or is taken by thieves. The latter, specifically, has no normative justification and creates significant privacy harms.[23]

Attention to the secondary use of taxpayer information and data security is also particularly warranted because those flows of information are becoming increasingly common and push the boundaries of how tax information has been used historically.[24] They thus challenge settled expectations and privacy norms in the tax area. Secondary uses of taxpayer information also involve flows of information over which taxpayers have very little control and involve the use of taxpayer information for purposes other than tax administration or the provision of benefits through the tax system. As a consequence, they involve tradeoffs that go beyond those generally involved with tax-policy choices and that might escape individual analysis.[25] Finally, these transfers of information occur after tax information is aggregated, which means that the privacy harms are magnified. Taxpayers might be comfortable with the IRS knowing their medical history based on an assumption that the information will be used only for tax purposes, but they may feel differently if they knew that the IRS would share that information with third parties or fail to keep it secure. All together, this Article demonstrates that the privacy harms in our tax system are cumulative. A lax approach to tax privacy on the front end of the tax process makes protecting information on the back end even more critical and a failure to do so even more problematic.

The Article builds toward these conclusions as follows. Section I provides an overview of the information flows that currently exist in our tax system and an overview of how the existing law and legal literature address taxpayer privacy. That discussion demonstrates the current disconnect between the extensive use of information in our current tax system and the protections that exist for taxpayers with respect to that information. Section II then evaluates the extensive flows of tax information through the lens of general privacy theory. It introduces the three different conceptions of privacy noted above and evaluates what tax privacy would mean under each. That discussion shows how modern privacy theories might well suggest that concern for tax privacy is overwrought, but concludes by explaining why directing attention to tax privacy is warranted nonetheless. Section III addresses how to move forward. It first outlines the broad range of privacy harms that potentially occur under the current Tax Code and explores how to prioritize those harms by using lessons from normative privacy theories. It concludes by identifying the top tax-privacy issues that need to be addressed in the short term.

23. See *infra* Part III.A for a discussion of the wide variety of privacy harms identified in the literature, including those created by data theft.

24. See *infra* Parts I.A.3 and III.B.1 for a discussion of protecting taxpayer information and monitoring the secondary use of such information.

25. See *infra* Part II.E for a discussion of the factors that prevent individuals from optimally managing tax privacy.

I. TAX AND TAX PRIVACY

The topic of privacy has received significant academic attention.[26] Privacy concerns are at the fore of modern questions regarding the government's powers and the power of private actors like Google and Facebook.[27] Notwithstanding this general attention to privacy, however, the topic of *tax* privacy has been severely undertheorized. Information is a necessary part of the tax system, and it is absolutely needed to raise revenue in a way that is both efficient and equitable—two central goals of the tax system. Privacy concerns thus appear to have taken a backseat to those more pressing goals. Nevertheless, we can be more discerning about how we approach tax privacy. Just as modern technology provides the government with ways to increase the information flows that occur in the name of tax, it might also permit the development of tax instruments and enforcement mechanisms that are more protective of individual and societal interests in privacy.

Working toward a more complete account of tax privacy requires an upfront assessment of where it stands today. To that end, the following Parts provide background on just how extensively information is utilized in the current tax system and the legal protections that currently exist in this area.

A. Information Flows Within the Tax System

Privacy interests can be implicated each time that information is observed, captured, disseminated, or used.[28] In the tax system, those opportunities are plentiful and can roughly be broken into three different stages of the administrative process of collecting tax revenue: the tax-filing process, the tax-enforcement process, and the process of securing taxpayer information.[29] These are discussed separately below.

1. The Tax-Filing Process

The filing of a tax return is probably the most obvious transfer of tax information. The IRS Form 1040 contains over eighty lines and can be accompanied by a wide range of supporting schedules.[30] Every person filing a tax

26. *See* Sklansky, *supra* note 4, at 1069–73.

27. *See supra* note 4 and accompanying text.

28. *See* Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 209 (2012) [hereinafter Bambauer, *New Intrusion*] (utilizing a "taxonomy that tracks the flow of data . . . through four distinct states").

29. There is, of course, a difference between privacy and security. *See generally* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667 (2013) [hereinafter Bambauer, *Privacy Versus Security*] (discussing the difference between privacy and security).

30. IRS, OMB NO. 1545-0074, FORM 1040: U.S. INDIVIDUAL INCOME TAX RETURN (2016), http://www.irs.gov/pub/irs-pdf/f1040.pdf [perma: http://perma.cc/WV6-DHJM]; *see also* Hatfield, *Privacy in Taxation*, *supra* note 5 (manuscript at 40–42) (discussing the wide variety of information that is disclosed on a tax return). The IRS requires taxpayers to attach schedules to their tax returns in certain situations, including if they take itemized deductions (Schedule A), if they are reporting business profit or loss (Schedule C), and if they have capital gains or losses (Schedule D). *See Schedules for Form 1040*, IRS, http://www.irs.gov/forms-pubs/schedules-for-form-1040 [perma:

return discloses her name, address, social security number, marital status, information regarding her children or other dependents, where she works, and how much money she makes.[31] A taxpayer with a more complicated financial or living arrangements might also disclose whether she has been divorced, where she banks, where she invests her money, and how much she saves for retirement. Of course, a taxpayer who wants to reduce her tax burdens will disclose much more than that.[32]

The Tax Code contains a wide range of deductions, credits, and exclusions from gross income. The information required to obtain those benefits extends well beyond basic demographic or financial information.[33] This can include information like a taxpayer's medical expenses, religious affiliations, and information regarding where her children sleep, play, or are cared for.[34] It can include information on whether she has moved, her educational expenses, and how she has funded her home purchases.[35] The information provided on a tax return is limited only by the policies that Congress wants to administer through the Tax Code, and those policies appear to be boundless.

http://perma.cc/QND8-UZRF] (last updated Aug. 9, 2017).

31. One of the major changes to the Tax Code made by the Tax Cuts and Jobs Act of 2017 (TCJA) was the elimination of personal exemptions. *See* TCJA, Pub. L. No. 115–97, § 11041, 131 Stat. 2054, 2082 (codified as amended at I.R.C. § 151). The TCJA retained and expanded the Child Tax Credit, however, which means that taxpayers will still disclose information regarding their children on their tax returns. *See id.* § 11022, 131 Stat. at 2073 (codified as amended at I.R.C. § 24).

32. The fact that the Tax Code does not *mandate* these disclosures raises a reasonable question about whether they are really privacy harms that should be included in this framework. See *infra* Part II.B for a discussion of factors that might undercut claims of privacy harm. *See also* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 69 (2010) [hereinafter NISSENBAUM, PRIVACY IN CONTEXT] (discussing the linguistic issues that arise when discussing privacy and privacy harms).

33. Congress provides some of those tax benefits to ensure that a taxpayer's taxable income more properly reflects her "economic income" net of the expenses of generating that income, but Congress also provides some tax benefits for other policy reasons (e.g., promoting education, home ownership, or retirement savings). *See* Hatfield, *Privacy in Taxation*, *supra* note 5 (manuscript at 39) (discussing the "competing policies and compromises" in the Tax Code); Kristin E. Hickman, *Administering the Tax System We Have*, 63 DUKE L.J. 1717, 1725 (2014) (noting that the Tax Code "is not and probably could never be entirely value neutral"); Daniel N. Shaviro, *Rethinking Tax Expenditures and Fiscal Language*, 57 TAX L. REV. 187, 199–206 (2004) (providing a history of the concept of tax expenditure analysis, which tracks the tax revenue losses that are attributable to "deliberate departures from accepted concepts of net income" (quoting STANLEY S. SURREY, PATHWAYS TO TAX REFORM 3 (1973))); David A. Weisbach & Jacob Nussim, *The Integration of Tax and Spending Programs*, 113 YALE L.J. 955, 964 (2004) (recognizing that "there are a vast number of programs implemented through the tax system").

34. *See* Hatfield, *Privacy in Taxation*, *supra* note 5 (manuscript at 40–46) (outlining the types of information required as a part of the tax filing process). *See generally* Hayes Holderness, *Taxing Privacy*, 21 GEO. J. ON POVERTY L. & POL'Y 1 (2013) (discussing the impact of public assistance programs on the privacy of low-income individuals in the United States). The deduction for childcare expenses requires a taxpayer to identify her care provider and perhaps a dependent's disability. *See* I.R.C. § 21(b)(1)(B), (e)(9)(A) (2012); IRS, OMB NO. 1545-0074, FORM 2441: CHILD AND DEPENDENT CARE EXPENSES (2017), http://www.irs.gov/pub/irs-pdf/f2441.pdf [perma: http://perma.cc/FP4Z-Z5VU].

35. Hatfield, *Privacy in Taxation*, *supra* note 5 (manuscript at 40–46).

Taxpayer information is also transferred in the tax filing process before the actual filing of a tax return. Over one-half of U.S. taxpayers use third-party tax return preparers,[36] and among those who claim the Earned Income Tax Credit,[37] the number is approximately two-thirds.[38] That means that tax information is not only transferred to the IRS, but to third parties as well. It is also the case that those third parties will often receive more of a taxpayer's information than the IRS. That is because information is often required for a return preparer to determine the propriety of a tax return position, but that information is not disclosed to the IRS unless the taxpayer is chosen for an audit.[39]

For example, the deduction for alimony requires only its inclusion on Line 31 of the Form 1040, but determining the eligibility for that deduction requires a tax advisor to evaluate the terms of a marital settlement, the taxpayer's child support arrangements, and perhaps where the taxpayer sleeps.[40] Excludable gain from the sale of a principal residence does not show up anywhere on a tax return,[41] but determining the eligibility for that exclusion can require assessing a taxpayer's living arrangements, where she votes, and her recreational activities.[42] Similarly, evaluating whether a benefit received by a taxpayer was taxable income or a nontaxable gift depends on whether the transfer was made with "detached and disinterested generosity" and, for that purpose, the intent of the donor controls.[43] Making that determination can require that a tax advisor know

36. IRS data show that roughly sixty percent of the individual income tax returns filed in 2015 were filed by tax practitioners. IRS, 2015 DATA BOOK: OCTOBER 2, 2014 TO SEPTEMBER 30, 2015, at 9–10 (2015), http://www.irs.gov/pub/irs-soi/15databk.pdf [perma: http://perma.cc/U6PB-LEWT] (reporting that over 78 million of the 127.8 million individual returns were filed by tax practitioners).

37. The Earned Income Tax Credit (EITC) is a refundable tax credit available to certain low-income individuals who have earned income. I.R.C. § 32 (2012). The provision is notoriously complex, however, and most recipients will require the use of a tax return preparer to claim the credit. *See* MARGOT L. CRANDALL-HOLLICK, CONG. RESEARCH SERV., R43873, THE EARNED INCOME TAX CREDIT (EITC): ADMINISTRATIVE AND COMPLIANCE CHALLENGES 15 (2015) (explaining that nearly two-thirds of EITC claimants have historically used a paid tax return preparer). Claiming an EITC requires taxpayers to disclose information regarding their income level, marital status, parental status—including information regarding adoption—and information about their children's marital statuses, disabilities, and living arrangements. I.R.C. § 32(a)–(d). This might not seem like much of an encroachment beyond that required by a normal return, but many EITC filers would not otherwise be required to file a return at all. *See* CRANDALL-HOLLICK, *supra*, at 1. In isolation, then, the privacy harms of this provision are distributed solely to those of lower income levels.

38. CRANDALL-HOLLICK, *supra* note 37, at 15. A small percentage of EITC claimants use free tax preparation services provided by the IRS and the remainder self-prepare their returns. *Id.* at 17 tbl.3.

39. *See* IRS, 2016 DATA BOOK: OCTOBER 1, 2015 TO SEPTEMBER 30, 2016, at 21 (2016), http://www.irs.gov/pub/irs-soi/16databk.pdf. [perma: http://perma.cc/4CVZ-N2PV]. That occurs relatively infrequently because the IRS currently audits less than one percent of taxpayers' returns. *Id.*

40. *See* I.R.C. § 71. The alimony deduction was eliminated from the Tax Code under the TCJA for divorce or separation instruments executed after December 31, 2018. *See* TCJA, Pub. L. No. 115–97, § 11051, 131 Stat. 2054, 2089 (repealing I.R.C. § 215).

41. *See* IRS, PUB. 523, SELLING YOUR HOME 18 (2017), http://www.irs.gov/pub/irs-pdf/p523.pdf [perma: http://perma.cc/KB7K-M9QW].

42. Treas. Reg. § 1.121-1(b)(2) (2002).

43. Comm'r v. Duberstein, 363 U.S. 278, 285–86 (1960) (quoting Comm'r v. LoBue, 351 U.S.

the intimate details of a personal relationship.[44]

The involvement of third parties in the tax system also goes further. For example, the current structure of the Tax Code requires that taxpayers' employers play an integral role in the tax process. This includes everything from determining the appropriate rate of withholding[45] to intervening in their employees' health.[46] One key tax expenditure in the Tax Code is the exclusion from income for employer-provided health insurance, which means that employees get a tax advantage for letting their employer control that expenditure.[47] Employers often seek to reduce their premiums, in turn, by implementing wellness programs that might require taxpayers to disclose personal health and wellness information.[48] Employers also often control taxpayers' retirement savings, which involves employers in their employees' lives to an even greater degree than just paying them wages.[49]

Finally, third parties often piggyback on the tax system and request taxpayers' returns for purposes other than tax administration. That can include lenders trying to assess credit risk or the public trying to assess political candidates.[50] This results in the disclosure of nonfinancial, tax-relevant information to those third parties. The tax-filing process thus creates the risk of disclosures to third parties beyond those directly anticipated by the government or by existing law.

2. The Tax-Enforcement Process

After a tax return is filed, it is first processed by the IRS, and then it

243, 246 (1956)).

44. *See, e.g.*, United States v. Harris, 942 F.2d 1125, 1131–35 (7th Cir. 1991) (evaluating the tax treatment of payments by a deceased widower to two of his mistresses by looking at the details of their relationships); Reis v. Comm'r, 33 T.C.M. (CCH) 1333 (1974) (evaluating the details of a relationship between a nightclub dancer and a generous patron); Starks v. Comm'r, 25 T.C.M. (CCH) 676 (1966) (evaluating the terms of a relationship between a woman and an older married man and determining that her companionship was not a "service[] rendered").

45. All employees must fill out a Form W-4 as a part of the employment process. That document informs the employer how much tax to withhold from the taxpayer's wages. *See* Treas. Reg. § 31.3402(m)-1 (1983) (providing the process for employers to determine the appropriate withholding allowances for purposes of wage withholding).

46. *See* I.R.C. § 106 (2012) (providing an exclusion from gross income for coverage provided to employees under certain accident and health plans).

47. *See* U.S. DEP'T OF THE TREASURY, TAX EXPENDITURES 16 (2016), http://www.treasury.gov/resource-center/tax-policy/Documents/Tax-Expenditures-FY2018.pdf [perma: http://perma.cc/GFT5-JE2Z].

48. *See* Ifeoma Ajunwa, *Workplace Wellness Programs Could Be Putting Your Health Data at Risk*, HARV. BUS. REV. (Jan. 19, 2017), http://hbr.org/2017/01/workplace-wellness-programs-could-be-putting-your-health-data-at-risk [perma: http://perma.cc/NYW4-5JNM].

49. *See* BORIS I. BITTKER & LAWRENCE LOKKEN, FEDERAL TAXATION OF INCOME, ESTATES AND GIFTS ¶ 61.1.1–2 (database updated Feb. 2018), Checkpoint (discussing the variety of tax-advantaged retirement plans provided in the Tax Code).

50. The disclosure of tax information by candidates for political office garnered significant attention during the 2016 presidential election. *See infra* note 83.

generally sits idle in a warehouse or on a server at an IRS computing center.[51] The information flows are largely done. That changes, however, if a taxpayer is the subject of an audit or if litigation implicates a tax matter. Those situations can result in additional flows of tax information that could potentially impact taxpayer privacy. Specifically, they can result in the collection of additional information by the IRS and the transfer of information to a variety of third parties.

a. Additional Transfers of Information to the IRS

The IRS will often collect additional taxpayer information during an audit or a litigated tax case in order to determine the accuracy of the taxpayer's return-filing positions.[52] The IRS can collect this additional information directly from the taxpayer or from third parties.[53] The information requested in those ways frequently includes the request of credit card or bank statements,[54] which can be used to prove expenses or to reconstruct a taxpayer's income but can also provide incredible insight into taxpayers' interests and preferences more generally.[55] The IRS has also started monitoring taxpayers' social media accounts and requesting information from those platforms as well.[56] Finally, the

51. IRS, *IRS Submission Processing Pipeline*, IRS VIDEO PORTAL, http://www.irsvideos.gov/Professional/IRSWorkProcesses/SubmissionProcessingPipeline [perma: http://perma.cc/2MJ2-J3P4] (last visited May 14, 2018) (discussing the IRS's process for evaluating filed tax returns before their storage in a processing center or a computing center).

52. See *supra* notes 39–44 and accompanying text for a discussion of the information that a taxpayer might disclose to a tax return preparer but not to the IRS.

53. The IRS has the power to summons any information that is "relevant or material" to a tax dispute. I.R.C. § 7602(a) (2012).

54. The Right to Financial Privacy Act of 1978 limits the government's access to some financial records, but that merely limits the IRS to using the § 7602 summons process. *See* Boris I. Bittker, MARTIN J. MCMAHON, JR. & LAWRENCE A. ZELENAK, FEDERAL INCOME TAXATION OF INDIVIDUALS ¶ 47.02[3][c] (3d ed.), Checkpoint (database updated Nov. 2017) (discussing the IRS's summons power regarding bank and financial statements).

55. *But see* I.R.C. § 7602(e) (prohibiting the IRS from doing fishing expeditions by requesting all available information unless it has a "reasonable indication" that a taxpayer has underreported her income).

56. *See* Houser & Sanders, *supra* note 6, at 823–24; Marcia Hofmann, *EFF Posts Documents Detailing Law Enforcement Collection of Data from Social Media Sites*, ELECTRONIC FRONTIER FOUND. (Mar. 16, 2010), http://www.eff.org/deeplinks/2010/03/eff-posts-documents-detailing-law-enforcement [perma: http://perma.cc/8ENW-XVRR]; T. Steel Rose, *IRS Mining Data for Tax Dodgers*, CPA MAG. (Dec. 19, 2016, 3:05 PM), http://www.cpataxmag.net/feature-articles/65-feature-stories/1554-knock-down-money [perma: http://perma.cc/ZRC8-4GWZ]; Richard Satran, *The IRS Has More Data About You than Ever Before*, BUS. INSIDER (May 13, 2013, 11:48 AM), http://www.businessinsider.com/the-irs-ramps-up-online-tracking-2013-5 [perma: http://perma.cc/35L3-P6HS]. The information that taxpayers disclose on those platforms can be tax relevant in many ways. For example, a taxpayer's Instagram feed might show whether a trip was really business travel or a Facebook feed might show a lifestyle that is inconsistent with reported income. *See* Rose, *supra*. Professor Michael Hatfield has theorized a world where the IRS's use of this information gathering is more extensive. *See* Michael Hatfield, *Taxation and Surveillance: An Agenda*, 17 YALE J.L. & TECH. 319, 340–50 (2015) (discussing the potential for a "Tax Surveillance System" based on the information collection in the private sector).

IRS has general law enforcement powers, which are extensive. For example, the IRS owns and utilizes so-called "Stingray" devices, which are devices that mimic cell phone towers and capture information sent over the cellular networks.[57]

The information collected by the IRS in this process can get quite intrusive, as Professor Michael Hatfield shows more fully in his piece *Privacy in Taxation*.[58] In that piece, he relays the story of one taxpayer who was required to defend her medical expense deduction by disclosing detailed information about her psychological history with regard to her gender identity and gender confirmation surgery.[59] Another case involved a married couple who disclosed information regarding one of their children's college applications and information regarding a different child's sexual activities in order to secure an exclusion from income for the proceeds of the sale of the couple's home.[60] Other cases have evaluated love letters or other features of personal relationships to determine whether transfers between sexual partners were gifts or transfers in the nature of compensation.[61] These inquiries obviously go beyond the type of information that the public might generally think of as tax relevant—and well beyond basic financial information.

b. Additional Information Dissemination

The tax-enforcement process also results in additional flows of information in the form of the transfer of taxpayer information to additional parties. To begin, a tax-enforcement action obviously means that taxpayer information will be transferred to an IRS auditor. That transfer can result in additional transfers if the auditor requests assistance from additional IRS personnel, requests information from third parties,[62] or discloses the taxpayer's information to unauthorized individuals.[63]

57. Woolf & Green, *supra* note 8. Those devices are placed in mobile law enforcement units and located near the target of an investigation. Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659, 666–68 (2018) (discussing the use of Stingray devices). When the target uses a cell phone, the phone identifies the Stingray as a cell phone tower and sends its data to that device, which then forwards it on to a traditional tower. *Id.* This allows the government to capture the data of the subject (and others who use a cell phone in the vicinity) without the target's knowledge. The IRS Commissioner testified that the IRS uses the technology only in limited criminal cases and with a court order. Letter from John A. Koskinen, Comm'r, IRS, to Ron Wyden, Senator, U.S. Senate (Nov. 25, 2015), http://www.techdirt.com/articles/20151201/17313132961/irs-looking-to-purchase-another-stingray-promises-to-start-obtaining-warrants.shtml [perma: http://perma.cc/5LJP-PZDW].

58. *See* Hatfield, *Privacy in Taxation*, *supra* note 5.

59. *Id.* (manuscript at 38). The medical expense deduction often results in the disclosure of highly sensitive medical information. For example, the costs of a breast augmentation can be deductible as medical expenses if they are incurred after a mastectomy that is performed due to breast cancer, but are nondeductible if done for cosmetic purposes. *See* I.R.C. § 213(d)(9); Rev. Rul. 2003-57, 2003-1 C.B. 959.

60. *See* Hatfield, *Privacy in Taxation*, *supra* note 5 (manuscript at 43–44).

61. *See id.* (manuscript at 45–46); *see also* Linda Galler, *Everything You Always Wanted to Know About* Farid *but Were Afraid to Ask*, 13 FLA. TAX. REV. 461, 484–85 (2013).

62. Such third parties could include a taxpayer's employer or bank if the IRS takes a lien or levy action against the taxpayer. *See* I.R.C. § 6331(a), (e).

63. See *infra* Part I.A.3 for a discussion of the unauthorized disclosure of taxpayer information.

Significant taxpayer information can also be transferred if a tax dispute ends up being litigated. The occurrence of an audit or dispute is generally not known or discoverable because the IRS is bound by confidentiality rules,[64] but the dispute is a matter of public record once it goes to court.[65] This can be especially problematic for two reasons. For one, the IRS's methods for flagging tax returns for audits can produce false positives.[66] In addition, the IRS has greatly reduced its network of local agents in recent years.[67] These factors have resulted in more cases proceeding to litigation without real merit, which in turn results in unnecessary exposure of taxpayers' information.[68]

3. Protecting Taxpayer Information

The transfers of information discussed above all occur in the process of administering our Tax Code, but tax information can also be used for purposes wholly unrelated to that task. These could include nonenforcement internal use, intentional disclosures of information to third parties for purposes other than federal tax enforcement, and unintentional disclosures of information due to security lapses. The first two of these categories raise the types of privacy issues that have long been discussed in the tax literature and that have been the focus of scholars and policymakers.[69] They include IRS personnel snooping into taxpayer records, the use of taxpayer information for political harassment, and the use of that information for statistical analyses or to enforce other laws.[70] Those practices are largely addressed under the existing law by § 6103 of the Tax

64. See *infra* Part I.B.1 for a discussion of the confidentiality provisions of § 6103.

65. This is not unlimited. *See* I.R.C. § 7461(b) (providing exceptions to the general rule that reports of the Tax Court and evidence received by the Tax Court are public records); Meghan M. Walsh, Note, *The Anonymous Taxpayer: What the Tax Court Failed to Reveal in* Anonymous v. Commissioner, 61 TAX LAW. 999, 999–1000 (2008). Federal courts, including the Tax Court, also allow litigants to redact or omit certain information, including the names of minor children and financial account numbers. *See* TAX CT. R. 27. The Tax Court also limits electronic access to case filings. *Id.* Tax Court opinions, though, contain an immense amount of personal information. *See, e.g.*, O'Donnabhain v. Comm'r, 134 T.C. 34, 35–42 (2010) (discussing a taxpayer's genitalia, psychiatric history, cross-dressing behavior, hormone treatment, and gender confirmation surgery); Estate of Barnhorst v. Comm'r, 112 T.C.M. (CCH) 335 (2016) (discussing a deceased individual's loss of sexual, bowel, and urinary functions after a prostate removal).

66. *See* 1 NAT'L TAXPAYER ADVOCATE, 2016 ANNUAL REPORT TO CONGRESS 32–33, 151–60 (2016), http://taxpayeradvocate.irs.gov/Media/Default/Documents/2016-ARC/ARC16_Volume1.pdf [perma: http://perma.cc/P4CP-8Q5B].

67. *Id.* at 86–97 (discussing the geographic constriction of IRS offices).

68. *See* 2 NAT'L TAXPAYER ADVOCATE, 2012 ANNUAL REPORT TO CONGRESS 71–93 (2012), http://taxpayeradvocate.irs.gov/2012-Annual-Report/downloads/Volume-2.pdf [perma: http://perma.cc/8UQU-K5SR] (reporting on the results of a study of EITC cases that proceeded to trial and in which the IRS conceded the taxpayer's position).

69. See *infra* Part I.B for a discussion of the existing law on tax privacy.

70. *See* IRM 1.13.1 (Dec. 3, 2015) (discussing the IRS's use of taxpayer data for statistical purposes); Cynthia Blum, *Sharing Bank Deposit Information with Other Countries: Should Tax Compliance or Privacy Claims Prevail?*, 6 FLA. TAX REV. 579, 616–17 (2004) (discussing the unauthorized access of taxpayer information by IRS employees).

Code, which is discussed more completely below.[71]

The last category involves data security, which is different than privacy, but can protect privacy if done well and can harm privacy if done poorly.[72] This is, of course, not an abstract issue for the IRS. Criminals target that agency over one million times each week.[73] Those attacks are generally unsuccessful, but some succeed. The most notable success involved a breach of the IRS's "Get Transcript" online application, which resulted in over 700,000 taxpayers' records being compromised in 2014 and 2015.[74] The data breach led to the temporary removal of the Get Transcript feature from the IRS's website, the implementation of more robust procedures to confirm taxpayers' identities, and the ongoing delay of refund payments to millions of Americans.[75] More recently, the IRS's system that allowed taxpayers to transfer their tax information to the federal FAFSA form was compromised.[76] That led to the removal of that tool, which greatly impacted taxpayers who relied on FAFSA for educational financial aid.[77]

B. Tax Privacy Today

The sheer amount of information that is transferred in our tax system might suggest that the regulation of tax privacy is robust. That is not the case. Taxpayers' privacy rights are governed by a few limited statutes and by informal policies of the IRS.

1. Statutory Taxpayer Privacy Rights

Taxpayers' privacy rights are governed nearly exclusively by two sections of the Internal Revenue Code. Section 6103 (Confidentiality and Disclosure of

71. *See infra* Part I.B.

72. *See generally* Bambauer, *Privacy Versus Security*, *supra* note 29 (discussing the difference between privacy and security).

73. *See* Steve R. Johnson, *The Future of American Tax Administration: Conceptual Alternatives and Political Realities*, 7 COLUM. J. TAX L. 5, 17 (2016) (citing Letter from Mortimer M. Caplin; Sheldon S. Cohen; Lawrence B. Gibbs; Fred T. Goldberg, Jr.; Shirley D. Peterson; Margaret M. Richardson & Charles O. Rossotti, Former Comm'rs, IRS, to Thad Cochran, Harold Rogers, Barbara A. Mikulski & Nita M. Lowe, Members, Senate and House Comms. on Appropriations, U.S. Cong. (Nov. 9, 2015) (on file with *Temple Law Review*)).

74. *See IRS Statement on "Get Transcript"*, IRS (Feb. 26, 2016), http://www.irs.gov/uac/newsroom/irs-statement-on-get-transcript [perma: http://perma.cc/6WQM-ZYNH] (discussing the data breach). The "Get Transcript" feature allows taxpayers to receive different types of transcripts of their tax accounts and activity, including information on their tax returns and wages statements. *See Welcome to Get Transcript*, IRS, http://www.irs.gov/individuals/get-transcript [perma: http://perma.cc/HY7B-FFRG] (last updated Jan. 8, 2018).

75. *See As Holidays Approach, IRS Reminds Taxpayers of Refund Delays in 2017*, IRS (Nov. 22, 2016), http://www.irs.gov/uac/as-holidays-approach-irs-reminds-taxpayers-of-refund-delays-in-2017 [perma: http://perma.cc/A29P-BKKE].

76. Alan Rappeport, *Up to 100,000 Taxpayers Compromised in FAFSA Tool Breach, I.R.S. Says*, N.Y. TIMES (Apr. 6, 2017), http://www.nytimes.com/2017/04/06/us/politics/internal-revenue-service-breach-taxpayer-data.html [perma: http://perma.cc/8TQA-LQCW].

77. *Id.*

Returns and Return Info) addresses the obligations of the federal government to protect taxpayer information,[78] and § 7216 (Disclosure or Use of Information by Preparers of Returns) addresses the responsibilities of private tax advisors.[79] Each section provides taxpayers with rights of confidentiality. They do little else.

Section 6103 is the general "tax privacy" statute in the United States and broadly provides that "[r]eturns and return information shall be confidential."[80] The term "return" is defined to include "any tax or information return, declaration of estimated tax, or claim for refund," as well as "any amendment or supplement thereto."[81] The term "return information" includes data like the taxpayer's identity, specifics regarding his income and deductions, the status of his return, and any enforcement actions taken against him.[82] Section 6103 thus fulfills an important role in protecting taxpayer privacy. It also played an unanticipated role in the 2016 presidential election, as it provided legal protection for then-candidate Donald Trump and his desire to keep his tax returns from the public.[83]

The general rule of § 6103 seems very protective of taxpayer privacy, and it is actually very protective with regard to the disclosure of taxpayer information

78. I.R.C. § 6103 (2012).

79. *Id.* § 7216.

80. *Id.* § 6103(a).

81. *Id.* § 6103(b)(1).

82. *Id.* § 6103(b)(2).

83. *See* Julie Hirschfeld Davis, *Trump Won't Release His Tax Returns, a Top Aide Says*, N.Y. TIMES (Jan. 22, 2017), http://www.nytimes.com/2017/01/22/us/politics/donald-trump-tax-returns.html [perma: http://perma.cc/9556-8X56]; Kelly Phillips Erb, *White House Petition to Release Trump's Tax Returns Closes in on a Half Million Signatures*, FORBES (Jan. 31, 2017, 6:21 PM), http://www.forbes.com/sites/kellyphillipserb/2017/01/31/white-house-petition-to-release-trumps-tax-returns-closes-in-on-a-half-million-signatures/#2b623dce5934 [perma: http://perma.cc/9M4P-7NS9]. Then-candidate Trump's refusal became even more contentious after the *New York Times* published a copy of what appeared to be one of his old filings. *See* David Barstow et al., *Donald Trump Tax Records Show He Could Have Avoided Taxes for Nearly Two Decades, The Times Found*, N.Y. TIMES (Oct. 1, 2016), http://www.nytimes.com/2016/10/02/us/politics/donald-trump-taxes.html [perma: http://perma.cc/VZ3E-T3E7]. That return showed a loss of nearly one billion dollars and only increased the public's interest in the matter. *See id.* Academics have debated the application of § 6103 in the election and whether it should be changed, but it has continued to protect now-President Trump from the public disclosure of his returns. *See* Daniel J. Hemel, *Can New York Publish President Trump's State Tax Returns?*, 127 YALE L.J. F. 62, 72–93 (2017) (discussing potential legal changes to allow the release of President Trump's returns); Kelly Phillips Erb, *Senate Bill Would Require Presidential Candidates, Including Trump, to Release Tax Returns*, FORBES (May 25, 2016, 10:13 PM), http://www.forbes.com/sites/kellyphillipserb/2016/05/25/senate-bill-would-require-presidential-candidates-including-tax-to-release-tax-returns [perma: http://perma.cc/5UDM-57CQ] (same). *Compare* George K. Yin, *Congress Has the Power to Obtain and Release Trump's Tax Returns*, WASH. POST (Feb. 7, 2017), http://www.washingtonpost.com/opinions/congress-has-the-power-to-obtain-and-release-trumps-tax-returns/2017/02/07/aa53254c-ea63-11e6-80c2-30e57e57e05d_story.html [perma: http://perma.cc/82XE-KWKP] (arguing that Congress might have the power to release this particular president's returns under § 6103), *with* Andy Grewal, *Can Congress Get President Trump's Tax Returns?*, YALE J. ON REG.: NOTICE & COMMENT (Feb. 13, 2017), http://yalejreg.com/nc/can-congress-get-president-trumps-tax-returns/ [perma: http://perma.cc/2XVL-XVHD] (arguing that "these proposals are a long shot").

to the public. It does much less to protect against disclosures of that information to other governmental units or actors. For example, § 6103 contains exceptions for disclosures to state tax officials, state law enforcement agencies, people with a "material interest" in the information, committees of Congress, the President, and other federal officers.[84] Those statutory exceptions are subject to a number of conditions and qualifiers, but the exceptions are extensive.[85] Section 6103 thus does not provide a complete right of confidentiality, but it does seek to ensure that taxpayer information is not freely available and that the IRS does not use taxpayer information to harass or embarrass members of the public. Violations of § 6103 are felonies, punishable by fines of up to $5,000 and potential imprisonment of up to five years.[86] Taxpayers can also bring civil actions for violations of that section.[87]

In addition to these rights with respect to information given to the government, taxpayers also have certain confidentiality rights with respect to information given to their tax advisors.[88] Section 7216 makes it a misdemeanor for any tax advisor to either disclose information that is provided to him in the process of preparing a tax return or use that information for purposes other than preparing a tax return.[89] Section 7216 contains limited exceptions for disclosures made pursuant to other provisions of the Tax Code or a court order.[90] It also allows for certain disclosures made to the IRS, related taxpayers, governmental bodies or professional boards, and fiduciaries, as well as for disclosures of statistical information, disclosures for the purpose of preparing the tax return, and disclosures to report the commission of a crime.[91] Knowing or reckless violations of § 7216 are misdemeanors punishable by fines of up to $1,000 and

84. I.R.C. § 6103(d)–(m).

85. *See* MICHAEL I. SALTZMAN & LESLIE BOOK, IRS PRACTICE AND PROCEDURE ¶ 4.07[3] (2018), Checkpoint (discussing the permissible disclosures under § 6103); *see also* BITTKER & LOKKEN, *supra* note 49, ¶ 111.4 (discussing § 6103 and permissible disclosures of taxpayer information thereunder). In June of 2016, President Obama signed a bill into law that allows the IRS to share information with local law enforcement officials in missing child cases. *See* Recovering Missing Children Act, Pub. L. No. 114–184, 130 Stat. 536 (2016) (codified as amended at I.R.C. § 6103(i)(1)).

86. *See* I.R.C. § 7213(a). Taxpayers affected by the recent IRS data breaches noted above claimed that the IRS was liable under the Privacy Act of 1974 and the Administrative Procedure Act (APA). *See* Class Action Complaint & Demand for Jury Trial at 5, Welborn v. IRS, 218 F. Supp. 3d 64 (D.D.C. 2016) (No. 1:15-cv-01352). The court evaluated the claims under the Privacy Act as two different claims: (1) a claim that the IRS's lack of security resulted in an unauthorized disclosure of taxpayer information, and (2) a claim that the IRS's security failures resulted in a failure to safeguard taxpayer information. *See Welborn*, 218 F. Supp. 3d at 81–85. The court dismissed the first claim as preempted by § 6103 and § 7431. *Id.* at 81, 83–85. The court dismissed the second claim because it held that the taxpayers had failed to present a claim of actual damages. *Id.* at 82–83. The court rejected the taxpayers' APA claim because it held that they did not have standing. *Id.* at 81.

87. *See* I.R.C. § 7431(a).

88. This protection applies to "[a]ny person who is engaged in the business of preparing, or providing services in connection with the preparation of, returns of the tax imposed by chapter 1, or any person who for compensation prepares any such return for any other person." *Id.* § 7216(a).

89. *Id.* § 7216(a)(1)–(2).

90. *Id.* § 7216(b).

91. *See* Treas. Reg. § 301.7216-2 (as amended in 2012).

imprisonment of up to one year.[92] Section 6713 (Disclosure or Use of Information by Preparers of Returns) of the Code also imposes civil penalties for violations of § 7216.[93] Like Section 6103, then, § 7216 protects the confidentiality of taxpayer information, but not completely.

There is little real privacy protection for taxpayers outside of the three aforementioned Tax Code sections. Taxpayers have limited constitutional rights to informational and decisional privacy, but those rights have not been specifically extended to tax matters.[94] Taxpayers have Fourth Amendment rights, for example, but those are limited in the tax context and do not apply in civil tax matters.[95] Congress and the IRS thus have incredibly wide latitude with respect to the information that they can require of taxpayers for the purpose of raising revenue and what they can do with that information after it is collected.

2. Aspirational Taxpayer Privacy Rights

Outside of the statutory privacy rights discussed above, taxpayers theoretically have privacy rights under the Taxpayer Bill of Rights (TBOR), which was drafted by the National Taxpayer Advocate, adopted by the IRS, and ultimately incorporated by reference into the Internal Revenue Code.[96] One of the rights listed in the TBOR is a right to privacy.[97] The IRS defines that right to mean a "right to expect that any IRS inquiry, examination, or enforcement action will comply with the law and be no more intrusive than necessary, and will

92. I.R.C. § 7216(a).

93. *See id.* § 6713.

94. The concept of decisional privacy refers to the rights recognized in cases like *Roe v. Wade*, 410 U.S. 113 (1973), and *Lawrence v. Texas*, 539 U.S. 558 (2003). Those cases involve a limited constitutional right to make certain intensely personal decisions—whether to have an abortion, take birth control, or engage in sexual intercourse—without government interference. *See* 1 WILLIAM J. RICH, MODERN CONSTITUTIONAL LAW § 15:2, Westlaw (database updated Dec. 2017). *See generally id.* § 15:1–6 (discussing privacy issues involving family relationships, parental issues, marriage, procreation, sexual intimacy, abortion, and health care decisions). The concept of "informational privacy" is less developed but involves the right to keep the government from collecting or disclosing certain information. In *Whalen v. Roe*, 429 U.S. 589 (1977), that included certain medical information. In *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977), it involved the private papers of President Nixon. Unfortunately, the Supreme Court has said very little about informational privacy since *Nixon*. *See* Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 182 (2015). Any right to informational privacy is not clearly defined, and no such right has been extended to general taxpayer concerns about tax information.

95. *See* SALTZMAN & BOOK, *supra* note 85, ¶ 13.04[4][b]; Stephen W. Mazza, *Taxpayer Privacy and Tax Compliance*, 51 U. KAN. L. REV. 1065, 1100–01, 1100 n.160 (2003) (discussing the limited Fourth Amendment rights of taxpayers in tax matters). Issues can arise when a tax audit moves to a criminal investigation. *See* SALTZMAN & BOOK, *supra* note 85, ¶ 12.05[4][a].

96. *See* I.R.C. § 7803(a)(3) (requiring the Commissioner of the IRS to ensure that IRS employees are familiar with and act consistently with the Taxpayer Bill of Rights). The National Taxpayer Advocate is the head of the Taxpayer Advocate Service, which is an independent organization within the IRS that was created to help taxpayers resolve problems that have not been resolved directly through the normal IRS dispute-resolution channels. *Our History*, TAXPAYER ADVOC. SERV., http://taxpayeradvocate.irs.gov/about/our-history [perma: http://perma.cc/9RXE-FE2Z] (last visited May 14, 2018).

97. *See* I.R.C. § 7803(a)(3)(G).

respect all due process rights, including search and seizure protections and will provide, where applicable, a collection due process hearing."[98]

That right can thus be broken into three components: (1) a right that an IRS action will comply with the law, (2) a right that an IRS action will "be no more intrusive than necessary," and (3) a right that the IRS will respect all due process rights. The first would clearly encompass any privacy rights under § 6103, the Constitution, or any other statutory right of privacy, and it appears to add nothing to those rights. The second seems broader than those other rights, but it is loose and subjective. The third seems to replicate the first, to the extent that it addresses privacy at all. Notably, there is no apparent remedy for violations of these rights.[99] On their faces, they are merely advisory, except to the extent that the Commissioner could violate his or her obligation to ensure that IRS officials are aware of and act consistently with them.[100]

Another source of taxpayer privacy protection is the Internal Revenue Manual (IRM), which sets out the IRS's policies and procedures for a number of administrative matters, including audits.[101] The IRM explicitly recognizes that there are privacy interests inherent in the auditing process.[102] It explains that to the extent possible information should be collected from a taxpayer rather than from a third party, that only "necessary and relevant" information should be collected from third parties, and that information collected from third parties should be verified with the taxpayer before any action is taken on that information.[103] It also explains that "[c]aution should be taken to not disclose any tax information of a confidential nature when contacts are made with third parties."[104] These provisions show sensitivity to taxpayers' privacy interests, but they provide only limited actual protections.[105]

3. Tax Privacy in the Academic Literature

The legal academic literature has largely replicated the narrow view of taxpayer privacy that is reflected in the positive law. Again, Professor Hatfield's

98. *Taxpayer Bill of Rights*, IRS, http://www.irs.gov/taxpayer-bill-of-rights#privacy [perma: http://perma.cc/U736-XRCT] (last updated Nov. 21, 2017).

99. *See generally* Alice G. Abreu & Richard K. Greenstein, *The U.S. Taxpayer Bill of Rights: Window Dressing or Expression of Justice?*, 4 J. TAX ADMIN. (forthcoming 2018).

100. *See supra* note 96. *But see generally* Abreu & Greenstein, *supra* note 99 (arguing that the TBOR could provide enforceable taxpayer rights).

101. *See* IRM 4.2.1 (Nov. 23, 2016).

102. IRM 4.10.1.2.1.7 (Aug. 24, 2017).

103. IRM 4.10.3.3.1.4 (Feb. 26, 2016). The privacy issues addressed in the IRM involve those in the enforcement stage, as well as in the information security stage discussed later in this piece. *See id.* (discussing the IRS's responsibilities with respect to contact with third parties and to its own use of taxpayer information).

104. *Id.*

105. As noted above, the Internal Revenue Manual is an internal manual and is generally understood as not conferring rights on taxpayers. *See* United States v. Jourdan, No. 17-cv-00550 (PAM/LIB), 2017 WL 6016574, at *3 (D. Minn. Sept. 21, 2017), *adopted by* Civ. No. 17-550 (PAM/LIB), 2017 WL 6021424 (D. Minn. Oct. 18, 2017).

recent work discusses this in detail.[106] His review shows that the literature shares five characteristics. It (1) narrowly focuses on taxpayers' rights to prevent the disclosure of their information by the IRS, (2) focuses on the compliance impacts of taxpayer privacy, (3) fails to address the privacy aspects of information collection, (4) does not think about tax information beyond financial information, and (5) focuses on § 6103 and the debates regarding its enactment.[107] The result of this limited view of tax privacy is that nearly all of the academic and legal attention to the topic has focused on the back-end protection of taxpayer information.[108]

That limited focus is beginning to change. Professor Hatfield's recent work, in particular, asks us to consider the privacy implications of the mere *collection* of data by the government through the tax system. He proposes that privacy interests should be incorporated as a policy interest in tax matters.[109] He is not alone. A recent paper by Professors Kimberly A. Houser and Debra Sanders similarly suggests that it is time for greater attention to the privacy aspects of taxation.[110] Their paper looks specifically at the IRS's use of big data and data analytics and questions the legal and privacy implications of those practices.[111] Should the IRS be looking at your Facebook account?[112] Should it be basing

106. *See* Hatfield, *Privacy in Taxation*, *supra* note 5 (manuscript at 27–31) (surveying the tax literature regarding taxpayer privacy and finding that it largely focuses on compliance impacts).

107. *Id.* (manuscript at 29–31). *But see* Boris I. Bittker, *Federal Income Tax Returns—Confidentiality vs. Public Disclosure*, 20 WASHBURN L.J. 479, 482–90 (1981) (mentioning the privacy interests inherent in the tax filing and tax enforcement processes); Blum, *supra* note 70, at 602–06 (discussing taxpayers' privacy interests in financial information). It is common in the literature for the phrase "tax privacy" to be used synonymously with "tax confidentiality." *See, e.g.*, Joshua D. Blank, *In Defense of Individual Tax Privacy*, 61 EMORY L.J. 265, 267–69 (2011) (discussing "tax privacy" as the confidentiality of taxpayer information); Mazza, *supra* note 95, at 1068–76 (purporting to discuss "taxpayer privacy" but discussing tax confidentiality); Paul Schwartz, *The Future of Tax Privacy*, 61 NAT'L TAX J. 883 (2008) (discussing tax privacy, but focusing nearly exclusively on § 6103 and confidentiality).

108. This approach to tax privacy as back-end protection of information is similar to how the privacy-by-design movement has protected privacy more generally. *See* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 410 (2015) ("Privacy by design has delivered strong back-end protection for consumers' personal information that corporations deem proprietary, but it has not delivered strong front-end protection for information as consumers disclose it."); *see also* Bambauer, *New Intrusion*, *supra* note 28, at 213–14 (noting that "the solutions put forward by privacy scholars tend to impose stringent restrictions at the dissemination and use stages of information flow"). Most of this focus on back-end privacy protection has focused more specifically on whether tax information should be public, as noted above. More recently, some authors have considered whether governments should be limited in how they share tax information between themselves. *See, e.g.*, Cockfield, *Big Data*, *supra* note 6, at 502–05 (discussing the privacy aspects of big data and multijurisdictional tax enforcement efforts); Cockfield, *How Countries Should Share*, *supra* note 6, at 1114–19 (noting the differential privacy rights that exist across the globe); Dean, *supra* note 6, at 668–70 (discussing the privacy aspects of international exchanges of tax information). That is, of course, a part of confidentiality, but it is different than disclosures to the public at large.

109. *See* Hatfield, *Privacy in Taxation*, *supra* note 5 (manuscript at 53–55).

110. *See* Houser & Sanders, *supra* note 6, at 817–18.

111. *See id.*

112. *See id.* at 835–36, 839–41.

audit decisions on analytics that might contain biases?[113] These are important privacy-related questions that have not been answered or even addressed.

This emerging focus on tax privacy as something more than just confidentiality is important and welcomed. We do not generally accept the unfettered collection, analysis, and use of our data by the government or by private actors. Imagine the FBI, NSA, or your local school board systematically collecting the same level of information as the IRS with a mere promise of confidentiality. That would hardly go unquestioned or unchallenged.[114] We would ask *why* they need that information. We would question the costs of them having it. We would question what they should be allowed to do with it. The public would expect, and privacy theory offers, much more.

II. PRIVACY THEORY AND TAXATION

The newfound attention to tax privacy is warranted and long overdue, but it raises some very significant issues. To say that privacy should be protected begs the questions of what privacy is and when other interests should yield to its pursuit. For example, does it harm privacy if taxpayers must disclose their addresses or dependents to the IRS? What about if taxpayers volunteer information in exchange for a tax deduction? Do they have legitimate privacy claims, or have they bargained them away? These types of questions are difficult to answer. Privacy is a contested concept, and privacy scholars have long been unable to define it with precision.[115] Individuals also have widely varying preferences and expectations with respect to their own privacy.

This reality means that working toward a more complete account of tax privacy will be difficult. It will not suffice to simply assert that we should protect taxpayer privacy or that a certain tax provision "harms privacy." Scholars will need to be more specific and intentional. They will have to identify the kind of privacy harm that is occurring and evaluate whether there is a normative

113. *See id.* at 848–50.

114. *See* Austen D. Givens, *The NSA Surveillance Controversy: How the Ratchet Effect Can Impact Anti-Terrorism Laws*, HARV. NAT'L SECURITY J. (July 2, 2013, 7:11 PM), http://harvardnsj.org/2013/07/the-nsa-surveillance-controversy-how-the-ratchet-effect-can-impact-anti-terrorism-laws/ [perma: http://perma.cc/QR3N-G3L8] (discussing the disclosure of the NSA's data collection practices under its PRISM program and noting the "public outcry [that] ensued").

115. *See* Bambauer, *Privacy Versus Security*, *supra* note 29, at 672–73 (discussing the broad debates in the privacy literature and claiming that "[s]cholars and courts disagree about virtually everything" related to privacy); Deirdre K. Mulligan et al., *Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy*, PHIL. TRANSACTIONS ROYAL SOC'Y A, Nov. 14, 2016, at 1, 1 (labeling privacy an "essentially contested concept"); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) ("Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."); Sklansky, *supra* note 4, at 1076–85 (discussing the evolution of how privacy is conceived in the legal discourse); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088–90 (2002) [hereinafter Solove, *Conceptualizing Privacy*] (discussing the difficulty that scholars have had in defining privacy); William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1020–21 (1995) (discussing the different conceptions of privacy in the legal discourse).

justification for that encroachment. They will also have to address the skepticism of those who do not share a common vision of what privacy means. This is especially true in an era in which privacy expectations seem to be changing at an increasing pace.

The following Parts address these issues by drawing upon the general legal literature on privacy. Specifically, they outline three different conceptions of privacy that have developed in that literature and evaluate what tax privacy would mean under each. That material shows that modern privacy theory might perfectly explain why tax privacy has come to mean essentially nothing more than tax confidentiality. The Section thus concludes by explaining why those theories ultimately fall short and why tax privacy should be more than tax confidentiality.

A. What Is Privacy?

Legal academic discussions of privacy often start with the seminal 1890 article *The Right to Privacy*, by Samuel Warren and future U.S. Supreme Court Justice Louis Brandeis.[116] In that piece, the authors broke new ground by articulating a common law right to privacy,[117] which they framed as "the right to be let alone."[118] Since that work, scholars have offered many competing theories of privacy and its status as a right under U.S. law,[119] courts have recognized common law causes of action related to privacy,[120] and Congress has adopted a wide-reaching but disjointed series of statutes that recognize a right to privacy in different areas.[121] The Supreme Court also has recognized a right to privacy in limited contexts.[122]

Notwithstanding this broad recognition of an interest in, and right to, privacy, it remains an ill-defined concept. Scholars disagree on whether privacy is a right in and of itself or whether privacy is merely instrumental to other goals.[123] There are also debates regarding the interests served by a right to privacy. Some

116. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

117. Benjamin E. Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623, 624–26 (2002) (noting that their work "is almost universally regarded as the origin of the four invasion of privacy torts" and that judges and scholars continue to cite it as "the original source of a privacy right in American law").

118. Warren & Brandeis, *supra* note 116, at 193.

119. *See* Solove, *Conceptualizing Privacy*, *supra* note 115, at 1088–90.

120. *Id.* at 1100 (noting that there are now "at least four common law tort actions to protect privacy").

121. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 256–60 (2011) (discussing the nonuniform regulation of privacy in the United States).

122. *See supra* note 94.

123. *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 422–23 (1980) (noting the academic disagreement regarding the meaning and existence of privacy as a distinct interest); Solove, *Conceptualizing Privacy*, *supra* note 115, at 1143–46 (noting the differing conceptions regarding privacy's intrinsic and instrumental value); *see also* Bamberger & Mulligan, *supra* note 121, at 257–58 (discussing the instrumental and noninstrumental motivations for privacy policy in the United States).

frame privacy as an issue of personal autonomy, while others believe that it is about dignity, self-fulfillment, or allowing individuals to create intimate relationships and trust.[124] The literature is vast.[125] It is, of course, impossible to do justice to that literature within the confines of this Article, and abstraction is necessary. In that vein, the following Parts summarize three schools of privacy theory and evaluate what tax privacy would mean under each.

Part II.B discusses the "neutral" conception of privacy and how it would support an expansive view of tax privacy. Part II.C then discusses various normative approaches to privacy and the factors that they use to identify privacy encroachments. It explains how those approaches might explain the current status of tax privacy as nothing more than confidentiality. Part II.D introduces the concept of context-dependent privacy. That privacy conception theorizes that whether an action negatively impacts privacy depends on the context in which that action takes place.[126] That approach, too, might provide an adequate ex post justification for equating tax privacy with tax confidentiality. Part II.E concludes by explaining why it would be erroneous to accept any of those justifications and builds the case for why attention to tax privacy is important.

B. Tax Privacy as a Concept

The broadest conception of privacy is one that is value neutral, which means that it evaluates privacy independent of any normative judgment.[127] Privacy

124. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 74–88 (surveying the literature regarding the value of privacy); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 234 (1977); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 141–51 (2004) [hereinafter Nissenbaum, *Privacy as Contextual Integrity*] (discussing the various values put forth by privacy scholars); Skinner-Thompson, *supra* note 94, at 171–75 (discussing the relationship between autonomy and privacy); Solove, *Conceptualizing Privacy*, *supra* note 115, at 1145–46 (discussing the different values noted by scholars); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 923–25 (2005) (discussing the different values that privacy might serve).

125. *See generally, e.g.*, NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32; Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1905 (2013) (discussing the "systemic risk[s]" created when individuals trade away privacy); Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968) (examining the basis of a right of privacy); Richards, *supra* note 4 (discussing the harms that can stem from surveillance activities); Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737 (1989) (broadly evaluating the constitutional right of privacy); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999) (discussing the impact of the Internet on privacy norms); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995) (evaluating the regulation of privacy in the United States); Solove, *Conceptualizing Privacy*, *supra* note 115 (discussing the many different conceptions of privacy); Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59 (2013) (discussing the shifting nature of privacy norms); Warren & Brandeis, *supra* note 116.

126. See *infra* notes 162–70 for an explanation of the context-dependent theory of privacy.

127. Professor Ruth Gavison refers to this characterization of privacy as "privacy as a concept" rather than as a value. *See* Gavison, *supra* note 123, at 423–24. Professor Helen Nissenbaum refers to this type of privacy conception as "descriptive or neutral" as opposed to those that are normative. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 68–69. This conception of privacy is not universally accepted. *Id.* at 68–70.

under this type of conception can be viewed as total isolation. Some view this in terms of control, others about access to information.[128] Under Warren and Brandeis's approach, privacy is "the right to be let alone."[129] Professor Ruth Gavison views privacy similarly, but with a focus on access. Her neutral conception evaluates whether people know about you, pay attention to you, or have access to you.[130] Perfect privacy exists when none of these occur, and a loss of privacy occurs when one does.[131]

Perfect privacy under this neutral conception is, of course, impossible. We lose privacy simply because we are born and because we are known. But this is a feature of neutral privacy, not a bug. The goal of the neutral conception is not to identify the ideal, but to help us identify when a deviation from "pure privacy" occurs so that we can evaluate whether that departure is warranted.[132] For example, few of us would live as hermits to protect our privacy because other values are important to us. Friendship matters. Income matters. Exchanges of ideas and collaboration matter.[133] The neutral conception just recognizes that we exchange privacy for these things and helps us to identify how much privacy we have given up.[134]

The breadth of neutral privacy is its strength, but also its weakness. It tells us very little about how to make policy because it does not consider how to balance privacy interests against other interests. Disclosing one's name on a tax return reduces privacy under a neutral conception, but we would hardly move to an anonymous income tax to protect against that loss.[135] Similarly, disclosing one's medical expenses to a certified public accountant (CPA) results in a loss of privacy under a neutral conception, but that conception would not tell us whether that loss is one that we should care about enough to change the medical-

128. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 70–71.

129. Warren & Brandeis, *supra* note 116, at 193.

130. *See* Gavison, *supra* note 123, at 428 (defining "perfect privacy" as being "completely inaccessible"); *see also* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 68–69 (same); Solove, *Conceptualizing Privacy*, *supra* note 115, at 1099–1105 (same). Under this broad, neutral conception, a person placed on an island with no hope of human contact would have "privacy," but some would argue that privacy has no meaning in that situation. Solove, *Conceptualizing Privacy*, *supra* note 115, at 1104; *see also* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 71 ("Does a person stranded on a desert island really have privacy?"). To them, privacy is a social construct that requires, at a minimum, a person being able to consent to exposure to another. It is not necessary that this particular aspect of privacy be determined for purposes of this piece, though the role of consent will be discussed in much greater detail below. *See infra* Part II.E.1.

131. Gavison, *supra* note 123, at 428.

132. *See id.* at 423 (explaining the need for a neutral privacy conception).

133. Privacy concerns are often outweighed by other benefits, like revenue, security, economic efficiency, or the free flow of information. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 108–13 (discussing the tradeoffs inherent in privacy protections); Bambauer, *New Intrusion*, *supra* note 28, at 227–28 ("A defensible system of privacy must analyze whether the social costs of free information flow outweigh the expected benefits.").

134. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 108–13.

135. This highlights how privacy interests must be considered along with the traditional focus on equity, efficiency, and administrability in tax policy. An anonymous tax might protect privacy, but it would likely be inequitable, inefficient, and impossible to administer.

expense deduction. The Tax Code by its existence reduces neutral privacy in many ways. The difficult policy question is when we should protect against those losses.[136]

That very issue has caused many scholars to eschew the neutral approach in favor of normative theories that attempt to capture the essence of when and why we care about privacy. Those scholars care little for when privacy is "diminished" and more for when and why it "has been 'threatened,' 'violated,' or 'invaded.'"[137] While their methods for making those comparisons differ, each scholar seeks to limit the concept of privacy in some way.

C. Tax Privacy as a Value

The difference between neutral privacy and normative privacy can be expressed as the difference between privacy as a concept and privacy as a value.[138] The former is clinical and free of judgment. The latter, however, requires a comparison of the relative values of privacy and whatever other end is being sought. That task naturally requires immense personal judgment. Is protecting information about one's sleeping arrangements worth a suboptimal allocation of the tax burden? There is no objectively "correct" way to answer that question, but we each probably have an idea of how we feel about it.

The difficulty of this balancing has caused many scholars to define privacy by reference to the values that it serves—perhaps autonomy or dignity.[139] Ultimately, though, defining privacy as a normative matter requires a balancing of interests based on personal preference.[140] This leads to a privacy theory that functions much like a neutral conception in that it requires ad hoc judgments about privacy loss. Unfortunately, that approach does little to explain or protect privacy more generally. Some solve this issue by distilling privacy down to public/private dichotomies.[141]

There are three different forms of the public/private dichotomy in the privacy scholarship. The first looks at the public or private status of the *actor* allegedly infringing on privacy.[142] Consider the Fourth Amendment's

136. The failure of neutral privacy to address this question is a key critique of that theory, but privacy scholars offering these neutral frameworks argue that there is value in setting forth those conceptions nonetheless. *See* Gavison, *supra* note 123, at 423–40 (discussing the value of starting with a neutral conception of privacy).

137. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 72.

138. *Id.* at 68–74.

139. *See id.* at 73–88 (discussing privacy theories that define privacy based on its "promot[ion of] other significant moral and political values"); Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, 101 VA. L. REV. 691, 699–700 (2015) (discussing normative conceptions of privacy that define the concept "in terms of the values, or human goods, that privacy fosters or protects").

140. *See* Bambauer, *Privacy Versus Security*, *supra* note 29, at 672–73 (noting that how one views privacy depends on "one's prior normative commitments"); Strahilevitz, *supra* note 124, at 931–32 (discussing the difficulty of defining privacy as a normative matter and noting that "normative disagreements about what is or is not private may be impossible to resolve").

141. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 89–102.

142. *See id.* at 91–94; Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 124, at 125–28;

prohibitions on "unreasonable searches and seizures," for instance,[143] which applies only to "the activities of sovereign authority."[144] Other analyses look to *where* the conduct at issue took place.[145] This is again reflected in Fourth Amendment doctrine, which might allow the government to collect information from the garbage outside your house but not from within your kitchen.[146] A third form of the public/private distinction relies on the public or private nature of the *information* that is involved.[147] Consider, here, the tort of public disclosure of private facts, which is marked by the disclosure of "a matter concerning the private life of another" if that matter is of a kind that "would be highly offensive to a reasonable person" and "not of legitimate concern to the public."[148]

Privacy theories that depend on a public/private distinction are intended to guide our real-world determinations about whether, when, and how we protect privacy.[149] They attempt to clearly mark particular actions as problematic and therefore supplant ad hoc determinations of the interests involved. For that reason, the public/private distinction appears to be the approach that is broadly accepted outside of academic circles.[150]

The concept of tax privacy could be very limited under this type of approach. It might ignore disclosures of information to private parties and might flag as problematic very little of the information collected by the government for tax purposes. After all, how much tax information is really unknown to others? Our employers know our wages. Our doctors know our medical conditions. Our financial advisors know our savings. Even information regarding a child's sleeping arrangements could be found in a publicly available divorce decree.[151] Defining tax privacy through a public/private lens might thus support the tax-confidentiality version of privacy that has emerged by chance. Tax information just may not be "private."

Victoria Schwartz, *Overcoming the Public-Private Divide in Privacy Analogies*, 67 HASTINGS L.J. 143, 146 (2015); *see also* S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 828–30 (1998) (noting the public/private dichotomy in the context of employees' privacy rights).

143. *See* U.S. CONST. amend. IV.

144. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 335 (1985) (quoting Burdeau v. McDowell, 256 U.S. 465, 475 (1921)).

145. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 94–96.

146. *See* California v. Greenwood, 486 U.S. 35, 39–41 (1988). Of course, the doctrine is much more complicated than this simple example would suggest. *See generally* Kimberly J. Winbush, Annotation, *Searches and Seizures: Reasonable Expectation of Privacy in Contents of Garbage or Trash Receptacle*, 62 A.L.R. 5th 1 (1998) (providing an overview of privacy law in searches of garbage).

147. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 96–98.

148. *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977); *see also id.* cmt. b (explaining the distinction between a person's private life and public life).

149. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 90–91.

150. *See id.* at 90.

151. Parenting plans will often govern the physical location of a child, and those are a part of the divorce proceeding and can be a part of the public record of that case unless sealed. *See* Margaret M. Mahoney, *The Enforcement of Child Custody Orders by Contempt Remedies*, 68 U. PITT. L. REV. 835, 836, 839–41 (2007) (discussing the nature and scope of parenting plans).

Modern privacy theory might suggest that tax privacy is limited by another factor as well—consent. Consent is generally an absolute bar to the privacy torts,[152] and it will bar a Fourth Amendment claim.[153] Consent is also one of the tenets of the Fair Information Practice Principles (FIPPs), which have been incorporated into various legislative directives.[154] A focus on notice and consent is an outgrowth of viewing privacy as control over personal information, and it is the hallmark of much of the modern privacy movement.[155] This appears intuitive at first blush. Why should we allow an individual to raise a privacy claim when she had control over the release of that information in the first place?[156]

Incorporating consent into how we think about tax privacy would significantly reduce the world of tax-privacy harms. To be blunt, we seem to care very little about privacy because we consent to being monitored all of the time.[157] We exchange our location information for directions to the nearest coffee shop. We use online search engines that track all sorts of information regarding our preferences and consumption behavior.[158] We let Amazon put microphones in our homes,[159] we use store loyalty cards that let retailers track our purchasing behavior, and we give our children toys that spy on them.[160] The

152. *See* Strahilevitz, *supra* note 124, at 929 n.27; *see also* 77 FRANCIS C. AMENDOLA, C.J.S. RIGHT OF PRIVACY AND PUBLICITY § 36, Westlaw (database updated Dec. 2017).

153. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 222, 248–49 (1973); Nancy Leong & Kira Suyeishi, *Consent Forms and Consent Formalism*, 2013 WIS. L. REV. 751, 754–68 (discussing the role of consent in Fourth Amendment jurisprudence).

154. *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882 (2013) [hereinafter Solove, *Privacy Self-Management*] (discussing the development and implementation of the "FIPPs," sometimes referred to as "FIPs"); *see also* Bamberger & Mulligan, *supra* note 121, at 255–56 (noting that the "FIPPs approach . . . relies largely on procedural protections, such as providing notice to the 'data subject' and securing 'consent' to informational use").

155. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 70 ("For the most part, however, conceptions of privacy adopted in scholarship, law, and policy incorporate control as a component of privacy, or, one might say, constitute privacy as a particular form of control."); Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1183–85 (2011) (discussing the focus on control in much of the modern privacy literature); Sklansky, *supra* note 4, at 1092 (noting that "[p]rivacy did not always mean control over information, but that is how the concept is generally understood today"); Solove, *Privacy Self-Management*, *supra* note 154, at 1880 (noting that, under the current approach to privacy, "[c]onsent legitimizes nearly any form of collection, use, or disclosure of personal data").

156. This focus on control is not universally accepted. *See, e.g.*, Peppet, *supra* note 155, at 1183–85 (discussing challenges to the control model).

157. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 105 ("In almost all situations in which people must choose between privacy and just about any other good, they choose the other good."). A. Michael Froomkin has characterized this problem as one of "privacy myopia," and has noted that "even Americans who place a high value on information privacy will sell their privacy bit by bit for frequent flyer miles." A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1502 (2000).

158. *See* Adam B. Thimmesch, *Transacting in Data: Tax, Privacy, and the New Economy*, 94 DENVER L. REV. 145, 149–57 (2016) (explaining the use of data as an asset in the modern economy).

159. *See Amazon Echo*, *supra* note 2.

160. *See generally* FUTURE OF PRIVACY F. & FAM. ONLINE SAFETY INST., KIDS & THE

adage that "privacy is dead" is oft repeated.[161]

Tax privacy may indeed be dead if we take consent into account as a factor in defining privacy. Many of the information flows that occur as a part of the tax system are done with the consent of, or even at the request of, taxpayers. They choose to seek the advice of tax professionals. They choose to take deductions. They choose to take tax cases to court. If we remove consensual disclosures of information from our theory of tax privacy, there might not be much left to worry about.[162] The Tax Code absolutely requires that you disclose your name, your address, your social security number, your marital status, the amount of your income, and the sources of that income, but little else. You can pay more tax if you wish to keep your other information from the IRS. But if you trade that information for a tax deduction, you may forfeit the right to complain about a privacy violation.

D. Context-Dependent Tax Privacy

One prevailing challenge for privacy scholars has been to define privacy in a way that is both internally consistent and robust. Not only do people exhibit drastic inconsistencies in how they protect their own privacy, but privacy expectations change over time and vary with demographics and context.[163] We might keep financial information private from a new acquaintance or from a business adversary, but we might also readily share that information with our spouse or with our accountant. Similarly, prior generations might have felt that their daily whereabouts were private, but now we often share that information through social media. What we consider to be "private" is therefore subject to

CONNECTED HOME: PRIVACY IN THE AGE OF CONNECTED DOLLS, TALKING DINOSAURS, AND BATTLING ROBOTS (2016), http://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf [perma: http://perma.cc/PRR6-K8NU] (discussing the privacy aspects of "connected" toys).

161. Sklansky, *supra* note 4, at 1085 (noting the academic concern that privacy is dead); Sherry D. Sanders, Comment, *Privacy Is Dead: The Birth of Social Media Background Checks*, 39 S.U. L. REV. 243, 243 (2012); Suzanne Barber, *Is Privacy Dead?*, U. TEX. AUSTIN, CTR. FOR IDENTITY: IDENTITY EXPERTS BLOG, http://identity.utexas.edu/id-experts-blog/is-privacy-dead [perma: http://perma.cc/7QFR-G2L2] (last visited May 14, 2018); Adam Levin, *Privacy Is Dead: What You Still Can Do to Protect Yourself*, HUFFINGTON POST: BLOG (Aug. 27, 2015, 6:19 AM, updated Aug. 27, 2016), http://www.huffingtonpost.com/adam-levin/privacy-is-dead-what-you_b_8047530.html [perma: http://perma.cc/27W9-BVYY]; Jacob Morgan, *Privacy Is Completely and Utterly Dead, and We Killed It*, FORBES (Aug. 19, 2014, 12:04 AM), http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#30b76e15dfbd [perma: http://perma.cc/VD7T-KXSW]; Alex Preston, *The Death of Privacy*, GUARDIAN (Aug. 3, 2014, 3:00 PM), http://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston [perma: http://perma.cc/6YSE-RK6G].

162. But see *infra* Part II.E.1 for a discussion of the practical considerations that may prevent people from making fully informed, rational choices with respect to these matters.

163. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 107 (noting the "great variability, or relativity" of privacy "across historical periods, societies, and even individuals"); Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509, 511–12 (2015); Solove, *Conceptualizing Privacy*, *supra* note 115, at 1132–40 (discussing the historical changes regarding privacy expectations).

many influences. These factors have led some privacy scholars to adopt conceptions of privacy that are context dependent rather than moored to a particular formulation.[164]

Professor Daniel J. Solove, for example, has argued that privacy should be defined pragmatically with a focus on "understanding privacy in specific contextual situations."[165] He thus adopts an approach that "conceptualizes privacy within particular contexts rather than in the abstract."[166] He evaluates privacy by looking for "disruptions to certain practices" including "activities, customs, norms, and traditions."[167] Protecting privacy under this conception is about "guard[ing] against disruptions" to those practices.[168] It also takes into account the value of privacy.[169] Those values "depend[] upon the purposes of the practices that are involved."[170]

Professor Helen Nissenbaum takes a similar approach and has offered a theory of privacy called "contextual integrity."[171] Under her theory, privacy claims must be evaluated against prevailing informational norms in a given context.[172] That includes established norms regarding (1) the parties involved, (2) the type or nature of the information involved, and (3) the constraints placed on information flows.[173] Professor Nissenbaum notes that people feel harms to their privacy when a particular change in practice violates any of the existing norms related to information flows.[174] At that point, evaluating the potential change requires an assessment of the values and goals involved.[175]

The concept of contextual integrity might very well resolve the disconnect that we observe between the public's general distrust of or opposition to taxation and its lack of concern about the privacy implications of taxation. Tax is a context in which the norms of information flows have developed to be incredibly lax. Federal law generally allows individuals to begin working at age fourteen,

164. *See* Acquisti et al., *supra* note 163, at 511–12; Cohen, *supra* note 125, at 1908 ("In the real world, privacy expectations and behaviors are unruly and heterogeneous, persistently defying efforts to reduce them to neat conceptual schema."); Gerety, *supra* note 124, at 238 (noting that it is impossible to define privacy "because we cannot escape from the bias of our own times and places, our own historical situations"). *See generally* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32 (introducing a context-based conception of privacy); Tene & Polonetsky, *supra* note 125 (discussing the relationship between technology and shifting social norms regarding privacy).

165. Solove, *Conceptualizing Privacy*, *supra* note 115, at 1127–28.

166. *Id.* at 1129.

167. *Id.*

168. *Id.*

169. *Id.* at 1143–46.

170. *Id.* at 1143.

171. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 129.

172. *Id.* ("The heart of the framework of contextual integrity is an elaboration of its key construct: context-relative informational norms."); *see also* Solove, *Conceptualizing Privacy*, *supra* note 115, at 1147 (noting that "[n]ot all privacy problems are the same, and different conceptions of privacy work best in different contexts").

173. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 140–47.

174. *See id.* at 140, 182–83.

175. *Id.* at 182–83.

and that marks the beginning of the taxpaying life for most Americans.[176] Even before we become taxpayers ourselves, our information is disclosed to the IRS on the return of a taxpayer claiming us as a dependent.[177] The IRS knows where we live, how we get our financial support, what disabilities we have, and maybe even whether we have any health conditions before we are old enough to understand that those things might be private. It should come as no surprise, then, that the norms of information flows are permissive in the tax context. Much like consumers who feel resigned to sharing information with online companies, taxpayers might simply feel resigned to sharing information with the IRS.[178]

A contextual-integrity approach to tax privacy might again reduce tax privacy to something close to tax confidentiality. The disclosure of medical information might violate contextual integrity if a doctor were to post it on a message board or talk about it at church because that would presumably violate the norms of information flows that exist in the doctor-patient relationship. The disclosure of that same information to the IRS, though, might not be problematic because it may not violate existing norms. We have consented to the use of medical information for tax purposes for a long time, and taxpayers seem to have accepted that use as long as the information is provided only to the IRS and as long as there are no changes in how that information is protected.[179] We could assume, however, that taxpayers would challenge the medical-expense deduction for privacy reasons if Congress decided to protect the information differently or to share that information more broadly.

Evaluating tax privacy through a contextual-integrity lens may suggest that the lack of any real privacy challenges to our tax system is a function of a stable system that protects existing informational norms—and is not the result of an abdication of responsibility by tax and privacy scholars. We might normally be concerned with a law that required us to disclose our employee benefits to someone other than our spouse, but we accept it for tax purposes. No harm, no foul.

E. The Challenges of Tax-Privacy Minimalism

The sum of the analysis above is that tax privacy could be a broad concept, but that modern privacy theory might perfectly explain and justify something much more limited. The public nature of much tax information and the

176. *See* 29 C.F.R. § 570.2(a)(1)(i) (2017).

177. I.R.C. § 151(c) (2012) (referencing *id.* § 152(a)(1), which defines a "qualifying child" as a dependent).

178. *See* JOSEPH TUROW, MICHAEL HENNESSY & NORA DRAPER, ANNENBERG SCH. FOR COMMC'N UNIV. OF PA., THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 4 (2015), http://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf [perma: http://perma.cc/VY47-X539] (concluding that individuals generally trade their information "while resigned rather than as the result of cost-benefit analysis").

179. The medical expense deduction, currently provided under § 213, has existed in some form since 1942. *See* Revenue Act of 1942, Pub. L. No. 77–753, § 127, 56 Stat. 798, 825 (codified as amended at I.R.C. § 213).

consensual method by which it is disclosed suggest that tax confidentiality might be the extent of what we should care about in tax privacy.[180] Similarly, privacy contextualists might feel that our current system is largely operating within existing informational norms and would evaluate tax privacy only with changes that conflict with those norms.

Following this path is certainly easier than attempting to define and apply some broader theory of tax privacy. Notwithstanding the allure of that approach, though, the easier path should not be taken. Taxpayer privacy rights need not be as extensive as a completely neutral concept of tax privacy, but each of the normative theories offered above is faulty in some way. Three concerns are most pressing and are discussed below. These include (1) the myth of fully informed, rational consent with respect to individual privacy in the tax system; (2) the assumption of a false dichotomy between public and private information; and (3) the status quo bias of contextual integrity.

1. The Myth of Fully Informed, Rational Consent

One critique that can be levied against the privacy-limiting theories offered above is that they rely on a presumption that individuals can adequately bargain for their privacy. This critique applies equally to a model of tax privacy built on contextual integrity and one that defers to taxpayer consent. The former model presumes that existing norms have developed based on some reasoned judgment that should be respected, and the latter presumes that taxpayers purposefully balance their interests before they allow an information flow. The problem with these presumptions is that it is far from clear that individuals manage their privacy in either of those ways.[181]

There are many impediments to individuals' abilities to efficiently bargain away their own privacy.[182] To start, people are generally not adequately informed about their privacy, including about how their information will be protected by the collecting party.[183] Even where they are fully informed, they face their own bounded rationality.[184] For example, taxpayers may

180. "Tax confidentiality" here would include permitted disclosures under § 6103.

181. Professor Solove refers to this process as "privacy self-management." *See* Solove, *Privacy Self-Management*, *supra* note 154, at 1880.

182. *See* Calo, *supra* note 10, at 662 (noting the literature regarding individuals' inabilities to manage their own privacy); Priscilla M. Regan, Response, *Response to* Privacy as a Public Good, 65 DUKE L.J. ONLINE 51, 52 (2016) (responding to Fairfield & Engel, *supra* note 108, noting "[b]ehavioral economics' view that individuals do not behave rationally with respect to privacy protection is widely supported by evidence"). *See generally* Solove, *Privacy Self-Management*, *supra* note 154.

183. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 105–06 (discussing research supporting the idea that people are not fully aware when information is being collected or the legal protections that exist with regard to their information); TUROW, HENNESSY & DRAPER, *supra* note 178, at 4–5, (reporting widespread consumer misunderstanding regarding privacy protections and concluding that "even when Americans do weigh the costs and benefits of giving up their data, they frequently base those choices on incorrect information"); Solove, *Privacy Self-Management*, *supra* note 154, at 1885–86.

184. *See* Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior:*

inappropriately discount the cost and risk of future privacy harms and show an irrational preference toward short-term gains—like a tax deduction.[185] Framing effects might also cause individuals to overweight the perceived loss of a tax deduction.[186]

Taxpayers are also likely unable to adequately determine the costs of each individual disclosure or their costs in the aggregate. Do taxpayers know the security employed by their CPA? Do they know the parties with whom the IRS can share their information? Do they understand the shifting norms regarding the flow of tax information internationally?[187] Do they evaluate how others might use their tax information against them? The argument that taxpayers have systematically made optimal privacy choices in this context seems incredibly weak. Even if they wanted to, taxpayers must make these judgments while handling the stress and complexity of filing a tax return. That is not usually an occasion for reflection for most Americans.

These concerns are especially true for low-income taxpayers. In a sense, low-income taxpayers are spared from much of the privacy loss—in a neutral sense—of the Tax Code because they rarely take itemized deductions.[188] On the other hand, they must disclose significant personal information to receive Earned Income Tax Credits or Child and Dependent Care Credits.[189] These taxpayers may not have the luxury of protecting their information by foregoing a tax benefit. We should at least recognize that these decisions are made under

Losses Gains, and Hyperbolic Discounting, *in* ECONOMICS OF INFORMATION SECURITY 165, 165–66 (L. Jean Camp & Stephen Lewis eds., 2004); Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363, 364–65, 368–70 (Alessandro Acquisti et al. eds., 2008) [hereinafter Acquisti & Grossklags, *Behavioral Economics*]; Laura Brandimarte & Alessandro Acquisti, *The Economics of Privacy*, *in* THE OXFORD HANDBOOK OF THE DIGITAL ECONOMY 547, 555–57, 564 (Martin Peitz & Joel Waldfogel eds., 2012); Solove, *Privacy Self-Management*, *supra* note 154, at 1880–81.

185. *See* Acquisti & Grossklags, *Behavioral Economics*, *supra* note 184, at 369; Edward J. McCaffery & Joel Slemrod, *Toward an Agenda for Behavioral Public Finance*, *in* BEHAVIORAL PUBLIC FINANCE 3, 12–13 (Edward J. McCaffery & Joel Slemrod eds., 2006).

186. *See* Adam B. Thimmesch, *Testing the Models of Tax Compliance: The Use-Tax Experiment*, 2015 UTAH L. REV. 1083, 1104–05 (discussing the impact of framing effects on tax choices).

187. See *supra* note 6 for resources discussing the intercountry sharing of tax information.

188. Taxpayers take itemized deductions only if the itemized deductions exceed their standard deduction, which was recently increased to $24,000 for married couples filing a joint return. *See* TCJA, Pub. L. No. 115–97, § 11021, 131 Stat. 2054, 2072–73 (codified as amended at I.R.C. § 63(c)(7)). That is exceedingly rare for low-income taxpayers. Even before the near doubling of the standard deduction under the TCJA, only one-third of taxpayers itemized their deductions, and the likelihood of one itemizing rose with income. *See* John R. Brooks, *Don't Forget the Standard Deduction*, 150 TAX NOTES 1589, 1592 (2016); SEAN LOWRY, CONG. RESEARCH SERV., R43012, ITEMIZED TAX DEDUCTIONS FOR INDIVIDUALS: DATA ANALYSIS 2–3 (2017). IRS data shows that while only 5% of taxpayers with incomes between $1 and $20,000 took the itemized deduction, that percentage rose to 17% for incomes between $20,000 and $50,000, to 46% for incomes between $50,000 and $100,000, and to 77% for incomes between $100,000 and $200,000. LOWRY, *supra*, at 3 tbl.1. Use of the itemized deduction continues to rise above that point, to a high of 91% of taxpayers with income over $1,000,000. *Id.* It follows that even fewer people will take itemized deductions after the substantial increase to the standard deduction under the TCJA.

189. *See* I.R.C. §§ 21, 32 (2012).

financial duress. While that might make the bargain more beneficial for them, we can ask whether that is a choice that we, as society, want to force upon our least economically well off.

There is one final reason to discount the importance of consent in this area—the social value of privacy. Even if individuals can rationally bargain for their own privacy, they still may not make choices that are beneficial to society as a whole.[190] Many scholars recognize that privacy has social value,[191] and some have referred to privacy as a type of public good.[192] Individuals' choices regarding their own privacy thus have externalities that may not be considered in tax choices. An individual might make a completely rational, self-interested determination to trade her information for a tax deduction, for example, but that decision might be suboptimal from a societal perspective. Privacy has a social dimension, and expectation setting should not be delegated to individual, self-interested determinations without question. We should take a more deliberate look at tax privacy on a macro level rather than deferring to the collective judgment of the crowd each April 15.

2. What Is Not Private Is Not Necessarily Public

Just as it is not clear that consent should allay tax-privacy concerns, it is not clear that a public-private dichotomy should either. That dichotomy necessarily presumes that what is not private is public, but this is not entirely accurate. What I share with my wife is not public information even though it is no longer private in the sense that I alone know the information. Similarly, what I wear to teach class is not private, but it is also not known by the public at large.[193] People often share information with particular individuals or groups, but feel harm if the information is distributed further than expected.[194] What this means for current purposes is that we should not accept a theory of tax privacy that views information in binary terms. Information is not either public or private.[195] Instead, the public/private divide occurs on a spectrum.

Identifying where information falls on the public-private spectrum will

190. *See* Peppet, *supra* note 155, at 1187–88 (noting that, under some privacy conceptions, "privacy would still matter *even if* market-perfecting strategies eliminated information market failures").

191. *See id.* at 1186–88.

192. *See generally* Fairfield & Engel, *supra* note 108.

193. The Supreme Court recognizes this reality. *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 770 (1989) (noting that "the fact that 'an event is not wholly "private" does not mean that an individual has no interest in limiting disclosure or dissemination of the information'" (quoting William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 KAN. L. REV. 1, 8 (1974))).

194. In modern society, this often involves transfers of sensitive information through electronic means. *See, e.g.*, Derek E. Bambauer, *Exposed*, 98 MINN. L. REV. 2025, 2027 (2014) (discussing the "[u]nauthorized distribution of intimate images and videos").

195. *See* Solove, *Conceptualizing Privacy*, *supra* note 115, at 1132 ("Particular matters have long remained private but in different ways; they have been understood as private but because of different attributes; or they have been regarded as private for some people or groups but not for others.").

always be subjective, but I propose that it is helpful to evaluate this in terms of transaction costs[196]—specifically, the transaction costs borne by a third party who seeks to discover that information from someone other than the data subject. Under this framework, *private* information would be information for which the transaction costs of discovery (either ex ante or ex post) are prohibitively high, and *public* information would be information for which the transaction costs of discovery are incredibly low, perhaps just having our eyes open.

This way of analyzing the difference between public and private information would suggest that what occurs in our bathrooms is considered *private* because it is costly for others to obtain that information without our consent. We have put in place physical and legal boundaries to its independent discovery.[197] In contrast, our names and addresses would be considered public because they can be discovered quite easily. Between these two ends of the spectrum, we might have information like the custodial arrangements of a child whose parents have divorced. That information can be found if one knows how to access court documents or knows someone close to the child, but the information is not generally distributed to the public at large. The information is thus available, but there are transaction costs of discovery that are higher than for other information. We would thus place that information closer to the private end of the public/private spectrum.

This way of evaluating information is very helpful when analyzing tax privacy. It not only helps us to assess the private nature of certain information, but it also teaches us to be cognizant of how particular tax provisions or practices reduce the transaction costs of discovery of taxpayer information. It also suggests that it is important to evaluate how the very structure of the Tax Code has the

196. *See* Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 991, 996–98 (2012) (recognizing that a reduction in transaction costs can trigger privacy concerns). *See generally* Strahilevitz, *supra* note 124 (building a theory of privacy based on the ease at which information travels through social networks). Professor Lior Strahilevitz's work is particularly on point. He has argued that courts should look to a "social networks" theory for assistance in "determining whether an individual has a reasonable expectation of privacy in a particular fact that he has shared with one or more persons." *Id.* at 919. His application of social networks theory principally helps courts to evaluate whether a data subject should reasonably expect that others would have access to their information based on the ease at which information flows through social networks. That approach is consistent with the idea that transaction costs matter for determining when information is "private." The more quickly and widely that information travels through a network, the less private it truly is. Further, when a person distributes information in a way that causes the information to travel farther or faster, that creates privacy harm. *See id.* at 974–75 (suggesting that courts should ask whether a "defendant's actions materially affect[ed] the extent of subsequent disclosure"). The relationship between information and the social network is one of transaction costs. A social network that facilitates the flow of information lowers the transaction costs of one who wants to discover that information. Simultaneously, a less connected network increases the transaction costs imposed on an outsider seeking to obtain that information.

197. This method of evaluating costs does not necessarily look only at ex ante costs of discovery, but also the ex post legal costs of doing so illegally. In that way, it might come to be that thermal imaging can be done with cheap technology, but that the legal penalties for using it to spy on your neighbor in his bedroom would be cost prohibitive.

same effect. An IRS that is assigned more duties collects more information, and that creates an even larger bank of data for thieves to access. The complexity of the Tax Code also results in the use of third-party tax advisors, which means that taxpayer information is replicated and subject to easier access by third parties through nongovernmental sources.

In sum, keeping private information private obviously assists in protecting privacy, but we can do better than ignoring tax privacy simply because most tax information is not truly secret. We should be able to build a model of tax privacy that focuses on actions that reduce the transaction costs of discovering information. If those costs are already low with respect to certain information, we might be concerned less about tax privacy. If they are high, however, we would be more concerned. This method for prioritizing tax privacy issues is discussed further below.[198] At this point, suffice it to say that tax-privacy concerns should not be discarded with a quick reference to a public/private distinction.

3. The Status Quo Bias of Contextual Integrity

The final normative privacy theory discussed above was contextual integrity. Under that theory, tax privacy might look very limited because the existing norms of information flows in the tax system are relatively loose and stable. One significant problem with this theory, however, is that it contains a significant status quo bias. The contextual-integrity approach evaluates privacy by referencing prevailing norms of information flow, and, by doing so, it fails to question whether those norms are truly desirable. Professor Nissenbaum readily recognizes this status quo bias and refers to it as the "tyranny of the normal."[199] She notes that technological changes can "often thrust change upon people and societies without a careful evaluation of harms and benefits" and cause "perturbations in social and cultural values."[200] Expectations and norms can thus shift without careful analysis, and "[a]s long as contextual integrity is tied solely to actual practice, as long as it merely defines a heuristic for detecting effectively when novel practices deviate from entrenched norms, it can be judged an instrument of" this "tyranny of the normal."[201] This, of course, means that the concept of privacy generally ratchets only one way—it shrinks over time.[202]

This aspect of contextual integrity means that relying on it to define tax privacy only makes sense if you have reason to believe that the existing information flows in our tax system represent a normatively desirable position.[203]

198. *See infra* Part III.B.

199. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 160–61 (discussing the status quo bias of her theory of contextual integrity).

200. *Id.*

201. *Id.* at 161.

202. Solove, *Conceptualizing Privacy*, *supra* note 115, at 1142 ("If we focus simply on people's current expectations of privacy, our conception of privacy would continually shrink given the increasing surveillance in the modern world.").

203. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 164–65 (evaluating the

That seems unlikely. It is not as though we adopted the current form of the Tax Code after due consideration of the privacy implications of such an intrusive system for raising revenue. Rather, the Tax Code has grown incrementally over time from a tax that impacted only the very rich[204] to one that impacts nearly every aspect of all of our lives.

The United States collected over $1.7 trillion in personal income taxes in 2015,[205] and the Tax Code now includes exclusions, deductions, or credits for healthcare expenses;[206] education expenses;[207] certain childcare expenses;[208] employer-provided health insurance;[209] energy-efficient appliance expenses;[210] alimony;[211] start-up expenditures;[212] qualified scholarships;[213] personal injury recoveries;[214] the production of certain types of renewable energy;[215] the interest incurred to buy a primary or secondary residence;[216] and more. The Tax Code has over two million words, and there are over seven million words contained in the Treasury Regulations interpreting it.[217]

The growth in the Tax Code is notable, but has been incremental and without an appreciable pause to analyze the privacy implications of the system that has emerged. This would suggest that we should question the norms of information flows and not simply accept them. American taxpayers might have low expectations of tax privacy simply because they have never been afforded an

"conservatism" of contextual integrity and admitting that "more is needed to assess the moral standing of custom in relation to novel practices").

204. *See* AJAY K. MEHROTRA, MAKING THE MODERN AMERICAN FISCAL STATE: LAW, POLITICS, AND THE RISE OF PROGRESSIVE TAXATION, 1877–1929, at 284 (2013) (noting that the first income tax "was a class tax" that was "aimed at economic elites"). Of course, there have always been privacy concerns with the income tax. *Id.* at 277 (presenting the privacy concerns raised, and rejected, with respect to the first U.S. income tax); *see also* DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 50–51 (1978) (discussing the lessons that politicians learned from the adoption of the income tax). Individuals felt as though the income tax required a personal look into their private sphere of home. *Id.* The tax was lambasted as "inquisitorial" in nature, but it was ultimately adopted to serve the nation's needs. MEHROTRA, *supra*, at 284; SEIPP, *supra*, at 50–51.

205. *SOI Tax Stats – Collections and Refunds, by Type of Tax – IRS Data Book Table 1*, IRS, http://www.irs.gov/uac/soi-tax-stats-collections-and-refunds-by-type-of-tax-irs-data-book-table-1 [perma: http://perma.cc/M4LC-RSWX] (follow the "2015" hyperlink to download the data table) (last updated Aug. 28, 2017).

206. I.R.C. § 213 (2012).

207. Treas. Reg. § 1.162-5(a) (as amended in 1967).

208. I.R.C. § 129.

209. *Id.* § 106.

210. *Id.* § 45M.

211. *Id.* § 215.

212. *Id.* § 195.

213. *Id.* § 117.

214. *Id.* § 104.

215. *Id.* § 45.

216. *Id.* § 163(h)(2)(D).

217. Scott Greenberg, *Federal Tax Laws and Regulations Are Now over 10 Million Words Long*, TAX FOUND. (Oct. 8, 2015), http://taxfoundation.org/blog/federal-tax-laws-and-regulations-are-now-over-10-million-words-long [perma: http://perma.cc/P93Q-C7VE].

alternative option.[218] Contextual integrity therefore might not be the best approach in this area.

Ultimately, this is not the article to evaluate that question, nor is law necessarily the correct discipline to take on the inquiry, but it is important to recognize that there is a dynamic relationship involved. The tax-privacy norm that exists is not the result of some divine declaration that matters of tax are different. There is a complex interaction between how we cede legislative power to Congress and how we feel about our privacy. There is a social justice aspect.[219] There is a story of path dependency and one of agency costs. To simply say that we have low expectations of privacy in matters of tax ignores these realities. We should not ignore tax privacy, then, simply because our current system appears to be explained by contextual integrity. Instead, we should evaluate existing norms against the values that we ultimately wish to further.[220]

III. A MORE COMPLETE APPROACH TO TAX PRIVACY

The discussion contained above shows that privacy is not a universally accepted concept, which means that there are varying degrees of individual concern about privacy matters and about how we should regulate privacy. Regardless of one's personal views, though, it seems relatively clear that tax law and tax scholars have approached privacy much too narrowly. Privacy theory, and neutral conceptions of privacy specifically, show that individuals' privacy can be impacted by far more than just breaches of confidentiality.

The first step toward developing a more complete approach to tax privacy is therefore to catalogue exactly where and how the Tax Code implicates privacy interests in their broadest forms. This can be done within a context that is familiar in the privacy literature: Professor Solove's taxonomy of privacy.[221] That

218. As Professor Julie E. Cohen notes, the "self has no autonomous, precultural core, nor could it, because we are born and remain situated within social and cultural contexts. And privacy is not a fixed condition, nor could it be, because the individual's relationship to social and cultural contexts is dynamic." Cohen, *supra* note 125, at 1908. Privacy and privacy norms are shaped by the world that we are born into and the world that develops as we do. Contextual integrity operates independent of this reality.

219. *See generally* Holderness, *supra* note 34 (evaluating the privacy implications of programs aimed at low-income individuals).

220. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 32, at 166 (concluding that contextual integrity can obtain "moral legitimacy" by comparing "entrenched normative practices against novel alternatives or competing practices on the basis of how effective each is in supporting, achieving, or promoting relevant contextual values").

221. *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) [hereinafter Solove, *Taxonomy*]. Professor Gavison's original formulation of this type of neutral conception focused on secrecy, anonymity, and solitude, but Professor Solove identifies the additional harms that occur due to practices like data aggregation, even though they do not result in a loss of secrecy, anonymity, or solitude. *Compare* Gavison, *supra* note 123, at 433, *with* Solove, *Conceptualizing Privacy*, *supra* note 115, at 1105. Professor Solove's taxonomy is "neutral" because he specifically notes that identifying that particular privacy harms exist does not mean that they should be legally cognizable harms in all cases. Solove, *Taxonomy*, *supra*, at 485 ("Of course, declaring that an activity is harmful or problematic does not automatically imply that there should be legal redress, since

taxonomy identifies and organizes the privacy harms that exist under a neutral conception into four different categories—information-collection harms, information-processing harms, information-dissemination harms, and invasion harms.[222] Those categories are not mutually exclusive, and many types of privacy violations fall within multiple categories. Our tax system implicates them all.

A. Accounting for Tax's Privacy Harms

1. Tax and Information-Collection Harms

The first category of privacy harm under Professor Solove's taxonomy includes the harms that occur when others intrude on our seclusion by collecting our information.[223] That type of harm is relatively straightforward, but there are two components of that category that are important to recognize for purposes of thinking about tax privacy. First, information-collection harms occur regardless of whether the information is collected through surveillance or through direct interrogation. Second, those harms also occur regardless of whether the information is collected by the government or by a private actor.[224] In either case, individuals lose a piece of their seclusion, which results in privacy loss under a neutral conception.

Information-collection harms obviously abound in the U.S. tax system.[225] The government collects tax information both through interrogation and through surveillance, and that information is extensive.[226] That is fairly obvious, and those harms are likely the first that come to mind when one thinks about tax privacy extending beyond confidentiality.[227] The IRS as a nosy neighbor is an easy picture to paint. It seems less likely, though, that we intuitively think about the privacy harms created by the amount of tax information collected by nongovernmental parties. As noted above, the complexity and structure of the

there may be valid reasons why the law should not get involved or why countervailing interests should prevail.").

222. Solove, *Taxonomy*, *supra* note 221, at 489. Professor Gavison noted many of these harms in her seminal work on neutral conceptions of privacy. *See* Gavison, *supra* note 123, at 436 (noting that her "neutral concept of privacy" includes as "invasions of privacy . . . the collection, storage, and computerization of information; the dissemination of information about individuals; peeping, following, watching, and photographing individuals; intruding or entering 'private' places; eavesdropping, wiretapping, reading of letters; drawing attention to individuals; required testing of individuals; and forced disclosure of information").

223. *See* Solove, *Taxonomy*, *supra* note 221, at 491–505.

224. *Id.* at 491–99 (discussing the range of information-collection harms created by private and public actions). The former would include wiretaps or police interrogations, and the latter would include unwelcomed gazes by a "Peeping Tom." *Id.*

225. The government's collection of taxpayer information is the focus of Professor Hatfield's recent work on taxpayer privacy. *See* Hatfield, *Privacy in Taxation*, *supra* note 5 (manuscript at 40–46) (focusing on the collection of information by the IRS in the tax collection process).

226. See *supra* Part I.A for a discussion of the information flows that exist under the current tax system.

227. Those harms are also the focus of Professor Hatfield's recent work on tax privacy. *See generally* Hatfield, *Privacy in Taxation*, *supra* note 5.

tax system means that our tax information does not flow only between taxpayers and the IRS.[228] A variety of parties become privy to that information.[229] And most of them are included by design.

Recognizing this additional aspect of tax privacy is important, and it raises the basic question of whether our need for tax revenue should result in a system that requires you to disclose your personal information to other members of your community. For example, should your local CPA be asking about the terms of your divorce, the reason for your breast augmentation,[230] or your online shopping history? The collection of that information results in privacy harm under the neutral conception, but it is not considered problematic under existing tax privacy theory. A more complete account of tax privacy should at least consider the privacy harms that result from information collection.

An awareness of the privacy harms that stem from information collection could result in a determination that certain tax provisions are not warranted or that they could be better structured to avoid invasive inquiries. Such an awareness might also suggest that we should make broader changes to how we administer the tax system—like adopting a ready-return system that eliminates the need for many taxpayers to use tax advisors.[231] Finally, this understanding of information collection might counsel against making changes to the tax system that rely on the collection of more information or the implementation of more complex requirements. A new tax based on mileage data, for example, might meet some goals of efficiency or equity, but it would also result in a new pool of data being collected by the government in the name of tax.[232] In contrast, the adoption of a "standard business deduction" for those working in the sharing economy might reduce information-collection harms and the harms that follow.[233]

Of course, once we become aware of how the Tax Code diminishes privacy in these ways, the next issue that must be considered is how one would evaluate whether those losses are normatively troubling, on balance. Not all privacy losses are equal. For example, disclosing the identity of one's children on a tax return

228. See *supra* Part I.A for a discussion of how tax information is shared with third parties.

229. *See supra* Part I.A.

230. See *supra* note 59 for a discussion of the deductibility of breast augmentation performed for cosmetic, as opposed to medical, reasons.

231. See *infra* Part III.A.5 for a summary of the issues that must be considered with regard to tax privacy.

232. Such a tax is not a mere academic fantasy. *See* Dorothy J. Glancy, *Vehicle Miles Traveled and Sustainable Communities*, 46 MCGEORGE L. REV. 23, 57–58 (2014) (discussing the potential use of GPS technology to track taxpayer miles driven); Michael Laris, *East Coast States Want to Tax Drivers' Travel, Not Their Gas*, WASH. POST (June 25, 2016), http://www.washingtonpost.com/local/trafficandcommuting/east-coast-states-want-to-tax-drivers-travel-not-their-gas/2016/06/25/9d4d1488-395c-11e6-8f7c-d4c723a2becb_story.html [perma: http://perma.cc/Y6CM-VVA9]; *States Eye Taxing Miles Driven, Not Gasoline*, NBC NEWS (Jan. 2, 2009, 5:49 PM), http://www.nbcnews.com/id/28472161/ns/us_news-life/t/states-eye-taxing-miles-driven-not-gasoline/ [perma: http://perma.cc/B9AS-L9MB].

233. *See* Kathleen DeLaney Thomas, *Taxing the Gig Economy*, 166 U. PA. L. REV. (forthcoming 2018) (manuscript at 35–37) (discussing how taxpayers might choose a standard business deduction over itemizing deductions).

results in privacy loss under a neutral conception, but it surely is not troubling enough to eliminate the child tax credit.[234] A significant component of addressing the tax privacy harms that stem from information collection will thus be prioritizing those harms. That is where the normative theories of privacy discussed above can provide guidance even if they are imperfect.

As noted previously, normative judgments regarding the value of privacy will vary by person and by context. That lack of uniformity prevents the development of a universal method for assessing privacy harms, but it does not mean that normative privacy theory tells us nothing. Instead, the factors that are often used to define privacy can be used to signal when privacy interests are more likely to be involved in a meaningful way.

Recall the two factors that privacy theorists often use to define privacy: (1) whether the information involved is public or private, and (2) whether the taxpayer has consented to its use.[235] The discussion above critiqued those factors because it is incorrect to label information as either public or private or to say that taxpayers have either consented to its disclosure or that they have not.[236] The public nature of information and the consensual nature of a taxpayer's decision are not binary in nature. They each occur on a spectrum. Placing those spectra perpendicular to one another reveals a way to visually prioritize tax's information-collection harms based on existing normative privacy theory. This is shown in Figure 1.

FIGURE 1

234. According to the Center on Budget and Policy Priorities, the child tax credit "lifted approximately 2.7 million people out of poverty in 2016, including about 1.5 million children." *Policy Basics: The Child Tax Credit*, CTR. ON BUDGET & POL'Y PRIORITIES, http://www.cbpp.org/research/federal- tax/policy-basics- the-child- tax-credit [perma: http://perma.cc/YRQ6-ZENS] (last updated Oct. 25, 2017).

235. See *supra* Part II.C for a discussion of these factors as elements of normative privacy theories.

236. See *supra* Parts II.E.1 and II.E.2 for a critique of the consent and public/private factors of privacy theory.

Using this approach, items that fall within the upper-right quadrant are relatively more worrisome than those that occur in the others. Those situations might include disclosures of private information made under financial duress or those made in aggressive enforcement actions.[237] In contrast, a deduction for property-tax payments might be in the lower-left quadrant. The information is both available at low cost and it is an elective deduction generally taken by high-income taxpayers.

This method of evaluating tax privacy gives due accord to the privacy losses identified by neutral conceptions but shows how the public-private distinction and the consensual nature of an information flow impact our responses. This should help guide efforts to address the most pressing of privacy issues. It is not perfect, though. Ultimately, decisions on prioritization must still include personal normative judgments. This method just helps to answer whether doing so in a particular situation is likely worth the effort.

2. Tax and Information-Processing Harms

Privacy harms also occur after information is collected, and those include harms that stem from the processing of the collected information. Professor Solove identifies five different harmful actions of this type: aggregation, identification, insecurity, secondary use, and exclusion.[238] The aggregation of information creates privacy harm because information has much more value and danger when it exists as part of a dataset than when it exists in isolation.[239] "Identification" refers to the connecting of information to particular individuals, and it creates privacy harm by saddling individuals with "informational baggage" that might be otherwise unknown or might be incorrect.[240] "Insecurity" manifests itself most clearly in the problems associated with identity theft, but it

237. This could include information submitted to claim an EITC or the disclosure of extensive credit card records during an audit, for example.

238. Solove, *Taxonomy*, *supra* note 221, at 505–06.

239. *See id.* at 507–08. Aggregation can create great value, but it can also create great harm or great risk of harm. *See* Fairfield & Engel, *supra* note 108, at 427–29 (discussing the developing recognition of an increased risk of harm as a legally cognizable harm itself).

240. Solove, *Taxonomy*, *supra* note 221, at 511–13. The use of a grocery store loyalty card might identify an individual as one who has a particular medical condition. *See id.* at 513 (explaining how identification documents could reveal someone's surgical history, just in the course of being used in "the many occasions in daily life where it was necessary to prove the existence and amount of one's income (taking a lease, opening a bank account, applying for credit, etc.)" (quoting B. v. France, 232 Eur. Ct. H.R. 33, 52 (1992))). Other data collection practices might create a digital record of a person's status as a transgender individual or as a person with a criminal history. *See id.* at 513–14. Professor Gavison retells an anecdote about a priest who discloses a damning fact about his "first confessor" to a group at a party. Gavison, *supra* note 123, at 430–31. An individual later approaches the same group and identifies himself as the priest's first confessor, which would be innocuous but for the priest's earlier disclosure. *See id.* at 431. The collection of information results in these types of harms to privacy even when each individual datum seems unimportant or harmless. This can be particularly troubling if the information is used to quell particular activities or to otherwise target particular individuals in undesirable ways. Identifying those who have a particular trait or mindset or who belong to a particular group is an important step in discouraging that particular activity. *See* Solove, *Taxonomy*, *supra* note 221, at 514–16.

occurs with more basic security lapses and illicit uses of personal information as well.[241] The fourth component of information processing, secondary use, refers to how information that is collected for one purpose can be used for another—using tax information for a nontax criminal prosecution, perhaps.[242] Finally, the category of "exclusion" focuses on the relationship between a person and her own information. "Exclusion" is the "failure to provide individuals with notice and input about their records."[243]

All of these potential harms exist within the tax system. Obviously, the tax system aggregates significant personal information from a variety of sources. A tax return involves information about your financial, social, romantic, political, and religious life. It compiles information from your employer, your bank, your state, your place of worship, and the charities that you support. The IRS, by its design, serves as a central repository of much of your life's information. Information-processing harms abound.

Recognizing these harms in the tax system might suggest that several reforms are warranted. For example, the aggregation harms inherent in our tax system might provide another reason for Congress to stop using the IRS to administer new government programs. Any new program that gives the IRS more administrative responsibilities also results in the IRS aggregating more taxpayer information, with the attendant harms to privacy.[244] Scholarship bemoaning the use of the Tax Code and the IRS to handle social programs would thus benefit from recognizing the privacy dangers of that practice as well.

The government's aggregation of taxpayer information can result in the privacy losses attributable to identification, insecurity, secondary use, and exclusion as well.[245] Taxpayer records might identify taxpayers as having particular medical conditions, political leanings, or family dynamics. That information can be used inappropriately, and it can be used for purposes other than tax administration.[246] Section 6103 significantly limits the secondary use of

241. Solove, *Taxonomy*, *supra* note 221, at 516–20. One of the great harms of insecurity is that it exposes people to potential future harm. *Id.* at 519–20 ("[I]nsecurity is the injury of being placed in a weakened state, of being made more vulnerable to a range of future harms.").

242. Philosopher Jeroen van den Hoven discusses secondary use in the context of "informational injustice." Jeroen van den Hoven, *Privacy and the Varieties of Informational Wrongdoing*, *in* READINGS IN CYBERETHICS 488, 493–95 (Richard A. Spinello & Herman T. Tavani eds., 2d ed. 2004). Solove notes that secondary use can create "dignitary harm" by undermining individuals' expectations of how their information will be used. Solove, *Taxonomy*, *supra* note 221, at 521–22. For example, a woman might not choose to disclose her fingerprint to the military if she knows that it will be incorporated into the FBI's criminal fingerprint database or might not disclose her location to MapMyRun if she knew that it would be given to her parole officer. *See id.* Secondary use can also result in "a sense of powerlessness and vulnerability." *Id.* at 522.

243. Solove, *Taxonomy*, *supra* note 221, at 523. Exclusion can harm individuals by reducing the accountability of those with the information and by preventing individuals from having input on, or knowledge of, the use of their information. *Id.*

244. *See id.* at 506–11 (discussing the privacy harms that stem from aggregation).

245. But see *supra* Part I.B.1 for a discussion on the limitations on the IRS's secondary use of taxpayer information.

246. As discussed above, § 6103 allows many nontax uses of tax return information. See *supra*

taxpayer information, but it contains many exceptions, especially for governmental uses.[247] Evaluating the privacy impacts of those practices more purposefully might suggest that those exclusions are too permissive, or perhaps too narrow.

The secondary use of tax information is also an issue that has manifested itself in a number of ways over the past few years. For example, leaks of taxpayer information have shown how taxpayers have used international tax rules and complicated structures to avoid taxation.[248] This has resulted in global efforts to increase transfers of taxpayer information to prevent or detect those abuses.[249] As this type of arrangement becomes more common, it will be useful to think about the privacy implications of those exchanges. How do foreign governments protect taxpayer information, and how will taxpayers respond to the potential transfer of their information to those governments?[250] The privacy tradeoffs in this area could be immense.[251]

Access to tax information—the cure for exclusion harms—is also a considerable issue in today's world. For example, U.S. taxpayers generally have access to their tax information that is held by the IRS through a request for a tax transcript, but the recent IRS data breach has made accessing that information more difficult.[252] Similarly, the IRS recently disabled an online tool that allowed

Part I.B.1 for a discussion of the exceptions that exist to the general rule of confidentiality under § 6103.

247. *See supra* Part I.B.1.

248. *See* Press Release, U.S. Dep't of Justice, UBS Enters into Deferred Prosecution Agreement (Feb. 18, 2009), http://www.justice.gov/opa/pr/ubs-enters-deferred-prosecution-agreement [perma: http://perma.cc/T5G8-PT5B] (discussing UBS's actions that were intended to help U.S. taxpayers avoid U.S. taxation); Greg Farrell & David Kocieniewski, *UBS, HSBC Offshore Dealings Thrust into Panama Papers Spotlight*, BLOOMBERG (Apr. 5, 2016, 10:26 AM), http://www.bloomberg.com/news/articles/2016-04-05/ubs-hsbc-offshore-dealings-thrust-into-panama-papers-spotlight [perma: http://perma.cc/FGY7-D9G2] (discussing the UBS and Panama Papers scandals). *See generally* Omri Marian, *Is Something Rotten in the Grand Duchy of Luxembourg?*, 84 TAX NOTES INT'L 281 (2016) (discussing the so-called "LuxLeaks"); Shu-Yi Oei & Diane M. Ring, *Leak Driven Law*, 65 UCLA L. REV. (forthcoming 2018).

249. *See* Farrell & Kocieniewski, *supra* note 248 (discussing how banks vet accounts and monitor activity by means of "due diligence, 'Know Your Customer,' source of wealth, and tax transparency checks" in order to prevent abuses); *Automatic Exchange of Information*, OECD, http://www.oecd.org/tax/transparency/automaticexchangeofinformation.htm [perma: http://perma.cc/V4CC-PV9D] (last visited May 14, 2018) (discussing the efforts of tax authorities around the globe to share information to reduce the possibility of tax evasion).

250. Senator Rand Paul, for example, has previously opposed the passage of tax treaties due to their privacy implications. *See* Bernie Becker, *Libertarian Lawmaker Blocks International Tax Treaties, Making Strange Bedfellows*, THEHILL (May 5, 2013, 11:20 AM), http://thehill.com/policy/finance/297741-libertarian-lawmaker-blocks-international-tax-treaties [perma: http://perma.cc/7VJQ-THQP]; Bernie Becker, *The Obama-Rand Tax Treaty Soap Opera*, POLITICO (May 9, 2016, 10:00 AM), http://www.politico.com/tipsheets/morning-tax/2016/05/the-obama-rand-tax-treaty-soap-opera-214182 [perma: http://perma.cc/HU2V-G94H].

251. Professor Arthur J. Cockfield has written several pieces that discuss the privacy aspects of this practice. *See supra* note 6.

252. 1 NAT'L TAXPAYER ADVOCATE, *supra* note 66, at 132–34 (discussing the challenges that taxpayers have had accessing the new IRS system).

taxpayers to easily transfer their tax information to the FAFSA form.[253] The IRS did that after a breach of that tool may have compromised over 100,000 taxpayers' personal information.[254] The IRS is thus in a tough spot. Its efforts to be more accessible to taxpayers can result in data theft if it lacks adequate security protocols, but those privacy-protecting protocols can limit taxpayers' access to their own information. This will be a significant tax-privacy issue to handle as the IRS moves more services online.

Finally, researchers might also use taxpayer data in positive ways if they were allowed to use anonymized information for statistical purposes. The government does allow this to some degree, but the restrictions on that access are very burdensome.[255] The IRS Statistics of Income division has also recently suggested that it would like to increase the ability of researchers to utilize taxpayer data in their studies, but it is cognizant of taxpayer privacy interests.[256] Those privacy interests are real, but researchers can mine a great deal of important information from the existing pool of taxpayer data, and we should seek to maximize the social value that could be gleaned from that information.[257] Part of the cost of paying taxes is money, but part of the cost is information. It only makes sense that we explore how best to use that information for the public good. Scholars should thus evaluate the ways that modern data science could be utilized to protect taxpayer privacy while still maximizing the returns from this national asset.[258]

3. Tax and Information-Dissemination Harms

The third category in Professor Solove's framework includes the harms that stem from the dissemination of information. Those include harms that occur

253. Richard Rubin & Douglas Belkin, *IRS Data on Up to 100,000 Taxpayers Compromised in Breach of College Financial-Aid Tool*, WALL ST. J. (Apr. 7, 2017, 12:25 AM), http://www.wsj.com/articles/irs-data-on-up-to-100-000-taxpayers-compromised-in-breach-of-college-financial-aid-tool-1491498254 [perma: http://perma.cc/965W-WQGK].

254. *Id.*

255. *See* Jeffrey Mervis, *How Two Economists Got Direct Access to IRS Tax Records*, SCIENCE (May 22, 2014, 2:00 PM), http://www.sciencemag.org/news/2014/05/how-two-economists-got-direct-access-irs-tax-records [perma: http://perma.cc/CQ4T-Y3UA] (discussing the process imposed before two economists obtained access to IRS data).

256. *See* Zoe Sagalow, *SOI, at Centennial, Balancing Research with Taxpayer Privacy*, TAX ANALYSTS (Jan. 18, 2017), http://www.taxanalysts.org/content/soi-centennial-balancing-research-taxpayer-privacy [perma: http://perma.cc/X3TZ-SUPJ].

257. *See* Blank, *Reconsidering Corporate Tax Privacy*, *supra* note 14, at 71–72 (discussing researchers' complaints regarding the limitations on available taxpayer data and the potential benefits from greater access).

258. The Statistics of Income (SOI) division generally does tax-data analysis for the IRS, and nongovernmental researchers can access that information in limited situations, but access is very strictly controlled. *See* STATISTICS OF INCOME DIV., IRS, 5-YEAR BUSINESS PLAN: FY2016–FY2017, at 6–7 (2016), http://www.irs.gov/pub/irs-soi/16rpsoi5yearplan.pdf [perma: http://perma.cc/4PAG-FMPW] (discussing the vision, mission, core values, and guiding principles of the SOI); *see also* Mervis, *supra* note 255 (discussing the difficulty of accessing IRS data and one example of a study that resulted when to researchers were granted that access); Sagalow, *supra* note 256 (discussing the balancing of data analysis and taxpayer privacy at the SOI).

from breaches of confidentiality,[259] disclosure,[260] exposure,[261] increased accessibility,[262] blackmail,[263] appropriation,[264] and distortion.[265] In the tax realm, the most relevant of these categories are breaches of confidentiality and increased accessibility. Breaches of confidentiality are the type of privacy violations that the tax literature and our tax laws recognize and should be familiar to most readers of legal literature.[266] Increased accessibility is different.

Increased accessibility differs from the other categories of information-dissemination harms because it refers not to the damages that stem from an actual disclosure of information but to the increased *likelihood* of such a disclosure and to the increased harms created when one occurs.[267] That type of harm is especially associated with the Internet era. Data, once collected, can obviously be disclosed, and it can readily be used for secondary purposes.[268] The magnitude of the information available also creates greater risk—both because of the simple cumulative loss that stems from more information being disclosed and because information is more valuable and worth accessing when it is aggregated.

That the tax system creates these harms should again be very clear. The IRS collects massive amounts of taxpayer information, and its ability to secure that information is questionable.[269] Even if the IRS abides by § 6103 and respects taxpayer confidentiality, a tax system that makes taxpayer information easier to access is problematic. As noted above, the IRS is under constant attack from hackers, and it seems unlikely that the problem is going to get any better in the near term.[270] The broad centralization of governmental programs within the IRS thus comes at another privacy cost.

Finally, as noted above, data security is also an issue for every person involved in the tax-filing process. Data thieves are targeting employers,

259. Solove, *Taxonomy*, *supra* note 221, at 526–27.

260. *Id.* at 530–31. Disclosure is the most general of these types of dissemination and involves the revelation of true information about a person that can harm that person's reputation regardless of the relationship between the disclosing party and the party about whom the information relates. *Id.* at 531.

261. *Id.* at 535–36. Exposure involves intimately private information, perhaps involving bodily functions, medical conditions, or our private physical characteristics. *Id.* at 536.

262. *Id.* at 539–40.

263. *Id.* at 541–43.

264. *Id.* at 545–46. Appropriation involves the self-interested and generally commercial use of another person's identity or personality. *Id.* at 546.

265. *Id.* at 549–50. Distortion involves statements of falsehoods that injure a person's reputation, and includes the torts of libel, slander, and false light. *Id.* Distortion is very similar to Professor Solove's "disclosure" category, but it involves false information. *Id.* at 550.

266. See *supra* Part I.B.3 for a discussion of the existing legal literature on tax confidentiality.

267. Solove, *Taxonomy*, *supra* note 221, at 539–40.

268. *See id.* at 540.

269. See *supra* notes 73–77 and accompanying text for examples of breaches of taxpayer information.

270. *See supra* notes 72–77 and accompanying text.

taxpayers, and tax-return preparers in addition to the IRS.[271] Any time that taxpayer data is replicated, there is the potential for someone to steal it. The potential privacy issues that stem from a lack of data security are thus widely dispersed.[272]

4. Tax and Invasion Harms

The final major category of privacy harm in Professor Solove's taxonomy is "invasion," which includes the subcategories of "intrusion" and "decisional interference."[273] "Intrusion" refers to actions that infringe upon some protected element of a person's daily activities, alter her routine, destroy her solitude, or make her uncomfortable.[274] Invasion is incredibly similar to a number of Solove's other categories. It resembles surveillance because it can involve "gazes" that can become intrusive or disturbing.[275] It resembles interrogation because extensive questioning on certain matters can be viewed as an intrusion.[276] It differs from the other categories, however, because of its impact. It goes beyond mere discomfort or some minor social sanction. An invasion is characterized by an interference with a broader sense of solitude or one's ability to be left alone.[277]

The second category of invasion harms, termed "decisional interference," involves a governmental intrusion on one's ability to make decisions regarding important matters in one's life.[278] It is reflected in the concept of decisional privacy in constitutional law.[279] *Griswold v. Connecticut*[280] recognized a privacy right related to individuals' usage of birth control.[281] *Roe v. Wade*[282] involved a privacy right related to a woman's choice of whether to terminate a pregnancy.[283] *Lawrence v. Texas*[284] involved a privacy right in consensual sexual activities within one's own home.[285] Decisional interference relates to many of Solove's other categories, but applies to a limited subset of highly private matters—the

271. *See* Bambauer, *Privacy Versus Security*, *supra* note 29, at 668–69.

272. Fortunately, the IRS is well aware of this aspect of tax privacy and "has joined with representatives of the software industry, tax preparation firms, payroll and tax financial product processors and state tax administrators to combat identity theft refund fraud to protect the nation's taxpayers." *Security Summit*, IRS, http://www.irs.gov/privacy-disclosure/security-summit [perma: http://perma.cc/X334-HF7R] (last updated Feb. 9, 2018).

273. Solove, *Taxonomy*, *supra* note 221, at 552.

274. *Id.* at 553.

275. *Id.*

276. *Id.*

277. *Id.* at 554.

278. *Id.* at 557.

279. *Id.* at 557–58.

280. 381 U.S. 479 (1965).

281. *Griswold*, 381 U.S. at 484.

282. 410 U.S. 113 (1973).

283. *Roe*, 410 U.S. at 120.

284. 539 U.S. 558 (2003).

285. *Lawrence*, 539 U.S. at 562–64.

self, the body, and sexuality.[286]

These categories of harm can occur in the tax system, not necessarily because of any particular tax provision but because of the system as a whole. For example, we generally do not have tax deductions that apply based on highly sensitive matters like the number or type of a taxpayer's sexual encounters. What the Tax Code does do, however, is play an integral role in decisionmaking, and it involves a degree of intrusion that, in the aggregate, could be considered an invasion. The Tax Code can impact a spouse's decision to seek work outside the home.[287] It can impact the decision of whether to have another child. It can impact whether one can quit her job or move residences. These are important matters that affect self-actualization, and it is worth assessing whether the Tax Code should have such a broad impact on our lives.

5. Summary

The sum of this material is that those considering the privacy implications of tax-design choices or administrative practices should consider a broad range of potential privacy harms. These harms occur at different stages of the tax-collection process, occur in a variety of ways, and are cumulative.[288] Privacy is not a monolithic concept and should not be discussed without reference to where and how it is implicated. Solove's taxonomy thus provides a useful structure to help refine tax-privacy analyses.

This approach should not only guide and discipline tax-privacy analyses, but it should also help to prevent them from becoming too narrow. Take, for example, a privacy analysis of the Tax Filing Simplification Act of 2016 (TFSA), which would allow some taxpayers the option of having the IRS prepopulate a tax return on their behalf.[289] Under that proposed legislation, taxpayers would be mailed a pro forma tax return that was completed by the IRS, and they could accept the return as prepared or make changes and submit the modified form.[290]

286. Solove, *Taxonomy*, *supra* note 221, at 559.

287. *See generally* Grace Blumberg, *Sexism in the Code: A Comparative Study of Income Taxation of Working Wives and Mothers*, *in* CRITICAL TAX THEORY: AN INTRODUCTION 3 (Anthony C. Infanti & Bridget J. Crawford eds., 2009).

288. A tax proposal that requires the disclosure of taxpayer information not only results in information-collection harms, but it creates potential issues with respect to information processing and information dissemination as well. The potential cumulative harm from a simple tax change might counsel against action. That can get lost if privacy is discussed as an abstract concept in tax policy analyses.

289. *See* Tax Filing Simplification Act of 2016, S. 2789, 114th Cong. § 3 (2016); *see also* ELIZABETH WARREN, THE TAX FILING SIMPLIFICATION ACT OF 2016, at 1 (2016), http://www.warren.senate.gov/files/documents/Tax_Filing_Simplification_Act_Fact_Sheet.pdf [perma: http://perma.cc/9LMH-NL3E] (last visited May 14, 2018) (noting that, among the benefits, the proposal would allow "eligible taxpayers with simple tax situations to choose a new return-free option, which provides a pre-prepared tax return with income tax liability or refund amount already calculated").

290. *See* Joseph Bankman & James Edward Maule, *Perspectives on Two Proposals for Tax Filing Simplification*, ABA TAX TIMES, Aug. 2016, at 9, 9. This is modeled on the efforts of Professor Joseph Bankman in California. *See generally* Joseph Bankman, *Using Technology to Simplify*

That legislation implicates many privacy interests, both positively and negatively. Some have argued that the bill would endanger privacy because the prepopulated returns could be sent to incorrect addresses.[291] A narrow focus on data security and the IRS data protection challenges could thus result in a case being made against the ready-return proposal on privacy grounds.

Recognizing the breadth of privacy interests at stake, however, shows the error of this approach. The ready-return system would surely present the noted privacy challenges related to data security, and thus diminish privacy in a neutral sense. But it might also *protect* privacy by obviating the need for many taxpayers to disclose personal information to a tax-return preparer. The basic premise on which the ready-return system is based is that many taxpayers have no need for return preparers. Their income is all reported on Form W-2 and they take the standard deduction.[292] Notwithstanding the relative simplicity of their returns, though, many feel ill-equipped to file on their own. As a result, they disclose their personal information to a tax-return preparer each spring. This results in information disclosures that expose them to information-processing and dissemination harms as well. It could also result in unnecessary return errors that might result in audits, which have their own privacy costs. These privacy impacts should be recognized, too. The privacy story with respect to the TFSA is more complicated than an initial assessment might suggest.

B. The Top Priorities in Tax Privacy

Theory aside, it seems likely that the indeterminate nature of privacy and the pressing need for tax revenue will cause the scales to tip heavily in favor of information collection over protecting taxpayer privacy in the near future. If that is the case, then the immediate focus in this area should be on limiting the privacy harms that occur after that stage of the tax process.[293] That would include protecting against the harms that stem from the secondary use of taxpayer information and from a lack of data security. The identification of these categories of harm notably stems not only from the difficulty of addressing tax privacy at an earlier stage,[294] but also from the accumulated lessons of the different tax-privacy conceptions noted above.

From a context-dependent standpoint, attention to the secondary use of taxpayer information and data security is particularly warranted because those

Individual Tax Filing, 61 NAT'L TAX J. 773 (2008).

291. *See, e.g.*, *Should We Trust the IRS to Prepare Our Tax Returns*, AM. COALITION FOR TAXPAYER RTS., http://www.americancoalitionfortaxpayerrights.org/facts/should-we-trust-the-irs-to-prepare-our-tax-returns/ [perma: http://perma.cc/55KM-V3E6] (last visited May 14, 2018) (raising concerns about pro forma returns being mailed to incorrect addresses); *see also* Bankman & Maule, *supra* note 290, at 14 (noting concerns about IRS data security).

292. Bankman & Maule, *supra* note 290, at 10 ("[N]on-itemizers . . . only have to keep track of a few pieces of information (such as their W-2s).").

293. See *supra* Part I.A for a discussion of the different stages of the tax process.

294. To be sure, it will take time to develop more privacy-protective tax structures given the underlying debates about the meaning of privacy and whether disclosures to the IRS are really worth worrying about.

flows of information are becoming increasingly common and push the boundaries of how tax information has been used historically. They thus challenge settled expectations and privacy norms in the tax area. This is true even if one disagrees that the underlying information is particularly sensitive or should be kept from the government in the first place.

These flows of information are also problematic under a normative framework that relies on taxpayer consent.[295] The secondary use of information by the IRS and the use of information by data thieves involve flows of information over which taxpayers have very little control and involve the use of taxpayer information for purposes other than tax administration or the provision of benefits through the tax system. As a consequence, they create tradeoffs that go beyond those generally implicated in tax-policy choices and that might escape individual analysis.[296] Few taxpayers have the ability (financially or cognitively) to fully weigh the likelihood and cost of their information being used for nontax purposes against the immediate benefit of a tax deduction, credit, or exclusion from gross income. Using taxpayer consent to classify these flows of information as nonproblematic seems questionable.

Finally, these transfers of information occur after tax information is collected and aggregated, which means that the privacy harms are magnified.[297] This, again, is one of the insights that we can glean from viewing tax privacy through a neutral lens and looking at all stages of the tax process. It is very clear that information spreads widely once it is introduced into the tax system. That means that the privacy harms that could stem from an initial disclosure or use of tax information are cumulative. This basic reality should change how we view the initial disclosure of information to the IRS but, at the very least, requires a significant focus on how we handle tax information after it is collected. It might be that taxpayers are comfortable with the IRS knowing their sensitive information because they assume that it will be used only for tax purposes. They could feel very differently, however, if they knew that the IRS would share that information or if they understood the risk that their CPA or the IRS could fail to keep their information secure. A lax approach to tax privacy on the front end of the tax process makes protecting information on the back end even more critical and a failure to do so even more problematic. This means that attention must be paid to ensuring that tax data is used correctly and that it is adequately protected. The following subsections discuss those goals in more detail.

1. Monitoring the Secondary Use of Taxpayer Information

Tax scholars and policymakers should be especially mindful of expansions to the use of taxpayer information after it is collected. Those expansions are occurring in various ways, including the expansive use of tax information

295. See *supra* Part II.C for a discussion of the role of consent in normative privacy theory.

296. See *supra* Part II.E for a discussion of the factors that prevent individuals from optimally managing tax privacy.

297. See *supra* notes 244–47 and accompanying text for an explanation of aggregation harms.

internationally.[298] They are also occurring domestically. One example is the use of tax information by tax-return preparers. For instance, H&R Block recently implemented a program using IBM's Watson to help it analyze tax information and suggest potential tax benefits for clients.[299] Other tax preparers are using taxpayer information to market financial products, and this use of tax data is funding free filing programs.[300] These uses of taxpayer information go beyond helping clients to file their returns and should be carefully scrutinized, especially since the data exchanged and potential risks may not be salient to consumers.

The other end of the spectrum requires ensuring that tax data is used as effectively as possible without harming tax privacy. As noted above, the government limits access to taxpayer data for research purposes.[301] That protects taxpayer information from secondary use and other data processing harms, but it also results in data not being used for socially productive purposes. Evaluating how to better utilize tax data in this way should be a priority of tax and privacy scholars.

Finally, scholars should use the discussions regarding the disclosure of President Trump's tax returns to invite a more serious discussion regarding tax privacy. This public debate invites an explicit weighing of taxpayer privacy rights against other public interests, and it could provide a good forum for introducing greater attention to tax privacy. If individuals profess a lack of concern for tax privacy, would tax confidentiality even be needed? If privacy is truly dead, we might look differently at § 6103, which places significant restrictions on the government and restricts valuable uses of data.[302] This merits conversation.

2. Ensuring the Security of Taxpayer Information

Regardless of one's personal beliefs about the likelihood of a governmental expansion of the use of taxpayer information or the scope of taxpayers' privacy interests, there is at least one thing on which nearly everyone should agree—data security is critically important. A theft of information results in privacy harm under every modern conception of privacy, and it harms taxpayer privacy in an unacceptable way. It is obviously a loss of seclusion under a neutral conception. It similarly results in the nonconsensual disclosure of quasi-private information

298. *See supra* Part III.A.2.

299. *See H&R Block with IBM Watson Reinventing Tax Preparation*, IBM (Feb. 1, 2017), http://www-03.ibm.com/press/us/en/pressrelease/51505.wss [perma: http://perma.cc/D5KA-V7YS]. IBM's "Watson" refers to the company's bundle of artificial intelligence techniques and related applications. Will Knight, *IBM's Watson Is Everywhere—But What Is It?*, MIT TECH. REV. (Oct. 27, 2016), http://www.technologyreview.com/s/602744/ibms-watson-is-everywhere-but-what-is-it/ [perma: http://perma.cc/YK6J-L3D8].

300. *See* Peter Rudegeair & Laura Saunders, *The Real Reason Everyone Offered You Free Tax Prep This Year*, WALL ST. J. (Apr. 7, 2017, 2:17 PM), http://www.wsj.com/articles/the-real-reason-everyone-offered-you-free-tax-prep-this-year-1491557402 [perma: http://perma.cc/BXK8-QUVY] (reporting on how tax preparation companies use taxpayer information to sell them other products).

301. See *supra* notes 255–57 and accompanying text for an explanation of the governmental limits on taxpayer information for research purposes.

302. See *supra* Part I.B.1 for a discussion of § 6103.

and it violates existing informational norms. If one trusts the normative basis for determining that information should be private, then there is no normative justification for data theft.[303] It represents only gain to the thief at the expense of others.

Tax scholars and policymakers should thus make data security their top tax-privacy priority. This is especially true as the IRS continues its push toward a more fully automated tax administration. Tax scholarship should make use of data security literature, which provides robust lessons for how we structure and administer the Tax Code.[304] In short, we must assume that perfect security is a fool's errand. Taxpayer information will be lost. It will be lost by taxpayers, employers, tax advisors, and the IRS.[305] Whether through technical superiority or through human error, thieves will find a way.

What this means is that we need to structure the tax system in a way that both (1) reduces the likelihood of those occurrences, and (2) anticipates them. This might mean reducing the information required for certain tax benefits or removing or decentralizing the provision of those benefits. It might mean providing statutory recourse for victims of data theft in an effort to socialize the cost of data breaches. Perhaps it means committing to more secure options for taxpayer interaction with the IRS. But something must be done.

This concern is especially important given the IRS's focus on its Future State Initiative.[306] The goal of that initiative is to give taxpayers more opportunities to interact with the IRS online, and the IRS has already reduced its in-person tax services.[307] There are obvious first-order financial advantages to the IRS of replacing human representatives with computer servers, but there are equally obvious privacy problems. Every point of data access is a point for data theft.

In this vein, it will be important to evaluate the development of the privacy literature regarding the harms that stem from data breaches. A taxpayer lawsuit against the IRS in connection with the Get Transcript data breach was dismissed,

303. *See* Bambauer, *Privacy Versus Security*, *supra* note 29, at 679–82 (explaining that data theft "destroy[s] utility").

304. Among the best practices noted by data security experts that are particularly relevant in the tax context are (1) collecting only the information that is needed, (2) keeping that information only as long as it is relevant, and (3) compartmentalizing information. *See* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 367–69 (2000) (discussing the value of compartmentalization); FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 1–2 (2015), http://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [perma: http://perma.cc/AN82-HUL9]; NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 16 (2014), http://www.nist.gov/document-3766 [perma: http://perma.cc/T7N2-NGV4]. The use of the IRS as a central repository of information regarding every aspect of taxpayers' lives is problematic under these principles.

305. *See* SCHNEIER, *supra* note 304, at 255–69 (discussing the "human factor" in data security).

306. *See Future State Initiative*, IRS, http://www.irs.gov/uac/newsroom/future-state-initiative [perma: http://perma.cc/YFT3-WDVJ] (last updated Jan. 12, 2018).

307. *See id.*; *see also* 1 NAT'L TAXPAYER ADVOCATE, *supra* note 66, at 121–37 (comprehensively discussing and critiquing the IRS's efforts to provide more taxpayer services online).

in part, because the taxpayers could not show actual damages.[308] That is similar to the problems faced by the plaintiff in *Spokeo, Inc. v. Robins*,[309] a case heard by the Supreme Court in its 2015 term.[310] Privacy scholars Daniel Solove and Danielle Citron have, however, recently proposed a new approach for capturing the harms that stem from data breaches.[311] They argue that courts should recognize risk and anxiety as privacy harms that stem from those breaches.[312] Their analysis and approach should be considered in the tax arena. A better understanding of the harms that stem from a data breach might better inform courts as to the individual harms caused by the lack of IRS security and should provide insight into why we, as a society, might want to take this issue more seriously.

CONCLUSION

The current view of tax privacy essentially amounts to a policy of "Don't worry, we won't tell." A more complete view of tax privacy recognizes that this amounts to a limited form of confidentiality, but not privacy. Privacy is a concept and value that is generally much broader. It is not monolithic, though, so those advocating for greater taxpayer protections will be required to articulate precisely what privacy interest is at stake and why privacy values should override other policy goals.

The analysis of this Article should provide a roadmap for how to evaluate and protect tax privacy going forward. Those interested in tax design can be mindful of the potential information-collection, information-processing, information-dissemination, and invasion harms that could occur. Privacy may be an "essentially contested concept,"[313] but it can be a value that is considered more intentionally in tax design.

308. *See* Welborn v. IRS, 218 F. Supp. 3d 64, 82–83 (D.D.C. 2016), *appeal dismissed mem.*, No. 16-5365, 2017 WL 2373044 (D.C. Cir. Apr. 18, 2017).

309. 136 S. Ct. 1540 (2016).

310. *Spokeo*, 136 S. Ct. at 1540.

311. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 745–47 (2018); *see also* Daniel Solove, *When Do Data Breaches Cause Harm?*, TEACHPRIVACY: PRIVACY + SECURITY BLOG (Dec. 28, 2016), http://teachprivacy.com/when-do-data-breaches-cause-harm/ [perma: http://perma.cc/M36T-NRPW].

312. Solove & Citron, *supra* note 311, at 756– 74.

313. *See* Mulligan et al., *supra* note 115, at 1.