Articles

MICHELLE LYON DRUMBL*

#Audited: Social Media and Tax Enforcement

* Michelle Lyon Drumbl, Robert O. Bentley Professor of Law and Tax Clinic Director, Washington and Lee University School of Law. I wish to extend special thanks to the participants of the 2019 National Tax Association Annual Conference on Taxation, including Leandra Lederman, Emily Satterthwaite, Dave Williams, and Ted Afield, and to Steven Dean, Heather Field, Adam Thimmesch, Miranda Fleisher, Susan Morse, Jordan Barry, Shu-Yi Oei, Ben Leff, Emily Cauble, Brian Galle, and Darien Shanske for their comments. Thank you also to Franklin Runge, Mark Drumbl, Jeff Lyon, Leanne Scott, and Margaret Hu for early stage inspiration and brainstorming. I am incredibly grateful to Seth Kuntz, Angela Cannon, and Hunter Rush for their stellar research assistance, and to the Frances Lewis Law Center at the Washington and Lee University School of Law for support of the project.

INTRODUCTION

With budget constraints and a mission that has been expanded by Congress over time, it is not surprising that the Internal Revenue Service (IRS) is looking for new tools to maximize its enforcement efficiency. Ever-advancing technology provides new opportunities for the IRS, and in turn, new privacy concerns for taxpayers.

In December 2018, the IRS made headlines when it issued a request for information (RFI) seeking social media research tools available in

the marketplace.[1] In its RFI, the IRS referenced the limits on its own employees' abilities to engage in social media research,[2] and it stated its hope to engage a vendor-supplied tool that would allow the agency to access publicly available social media to "expedite IRS case resolution for existing compliance cases, providing a more efficient way of identifying resources and assisting with the collection of known tax deficiencies, leading to increased collection of revenue involving unfiled tax returns and other tax liabilities."[3] The RFI noted that the agency "respects taxpayer rights" and stated that "such a tool would not be used to search the internet or social media sites for purposes of identifying or initiating new tax audits" but rather to "assist with previously identified tax compliance cases."[4]

The RFI also mentions a potential benefit to taxpayers, which is that the IRS believes a social media mining tool could aid in the resolution of tax-related identity theft.[5] The RFI does not elaborate further on this potential use, though it is worth imagining how the IRS might use social media constructively rather than for enforcement.[6] The RFI concludes by noting that the IRS intends to "be mindful that frequently information posted on social media and the internet may be wrong or misleading."[7]

The RFI does not explicitly define the term "social media" or list examples of the sites the IRS is interested in reviewing. Presumably the term would encompass websites in which users create profiles and may interact with one another, such as Facebook, Twitter, Instagram, and LinkedIn.[8] Demographic studies reveal that a majority of American

---

1 Jared Gilmour, *The IRS Wants Help Scouring Social Media for Clues on Tax Cheats*, MIAMI HERALD (Dec. 28, 2018, 4:29 PM), https://www.miamiherald.com/news/nation-world/national/article223681430.html.

2 The RFI cites to IRM 11.3.21.8.1(4) as prohibiting IRS employees from logging into social media sites to carry out compliance-related work and states that "the IRS currently has no formal tool to access [] public information [used by taxpayers to advertise, promote, and sell products and services], compile social media feeds, or search multiple social media sites." DEP'T OF TREASURY, IRS, REQUEST FOR INFORMATION, SOLICITATION NO. 2032H8-RFI-MEDIA, SOCIAL MEDIA RESEARCH REQUEST (Dec. 18, 2018) [hereinafter IRS RFI].

3 *Id.*

4 *Id.*

5 *Id.*

6 *See* discussion *infra* Section II.C.6.

7 IRS RFI, *supra* note 2; *see also infra* Section II.A (discussing the seeming contradiction between the IRS's goals of efficiency and the extra cost and work that would be required for a human being to sort through misleading claims).

8 *See* Aaron Smith & Monica Anderson, *Social Media Use in 2018*, PEW RSCH. CTR. (Mar. 1, 2018), https://www.pewresearch.org/internet/2018/03/01/social-media-use

adults use Facebook and YouTube on their computer or cellphone.[9] Younger adults (age 18–24) use a wider variety of sites and do so more frequently.[10] A 2012 study showed that younger adults are more likely to use social media than older adults, and urban dwellers are significantly more likely to use social media than those who live in rural areas; however, the study did not reveal a statistically significant disparity in overall social media site use across different household income levels.[11] Interestingly, even those who abstain from social media may not be as hidden from sight as they think. Researchers report that individuals with no social media accounts themselves are likely drawn into this public sphere, with algorithms able to draw predictive and reasonably accurate[12] findings about an individual based upon postings by those of the individual's friends, family, and acquaintances who do have a social media presence.[13]

The thought of IRS employees searching through individual taxpayers' social media sites presents concerns on multiple fronts: What policies or limits might the agency adopt? Might the IRS later expand the program beyond the stated intention to use such practices only in existing compliance cases? This Article begins by considering the potential implications to taxpayer privacy rights of such an initiative, and questions whether it may conflict with the statutory notion of a taxpayer's right to privacy.[14] Speaking for myself, I bristle

---

-in-2018/ [https://perma.cc/L432-JGTW]. Smith and Anderson also define social media as including YouTube, Snapchat, Pinterest, and WhatsApp. *Id.*

9 *Id.* (noting that 68% of American adults are Facebook users, with 74% of Facebook users accessing it on a daily basis, and that a majority of American adults in all demographic groups, other than individuals 65 and older, currently use Facebook).

10 *Id.*

11 Maeve Duggan & Joanna Brenner, *The Demographics of Social Media Users — 2012*, PEW RSCH. CTR. 3 (Feb. 14, 2013), https://www.pewresearch.org/internet/2013/02/14/the-demographics-of-social-media-users-2012/ [https://perma.cc/U8AX-8NXN].

12 Jessica Baron, *Think Your Data Is Private Because You're Not on Social Media? Think Again*, FORBES (Jan. 23, 2019, 8:46 AM), https://www.forbes.com/sites/jessicabaron/2019/01/23/think-your-data-is-private-because-youre-not-on-social-media-think-again/#7ab38b814a16 [https://perma.cc/HL8C-2BQW] ("The original user's Tweets allowed them to predict future tweets with an accuracy rate of roughly 64% and the user's contacts gave them enough data to predict behavior with an accuracy rate of 61%.").

13 *Id.* Baron's article describes the work of James P. Bagrow et al., *Information Flow Reveals Prediction Limits in Online Social Activity*, 3 NAT. HUM. BEHAV. 122, 122 (2019) ("As few as 8–9 of an individual's contacts are sufficient to obtain predictability comparable to that of the individual alone.").

14 Concerns about taxpayer privacy are certainly not new. Tax scholars such as Michael Hatfield have written multiple thoughtful pieces addressing privacy in taxation, including the scope of the IRS's power to collect personal information. *See* Michael Hatfield, *Privacy in Taxation*, 44 FLA. ST. U. L. REV. 579, 581 (2017) ("[A]mong government agencies, the

at the idea of the IRS staking out an ever-more invasive footprint into the private life of any individual taxpayer. Regardless of one's views on taxpayer privacy, this Article makes a deeper inquiry: it asks not whether the IRS has the *right* to access and use this information for examination and collections purposes but whether, as a matter of social policy, it is *appropriate and desirable* for the IRS to trawl for such information, and to do so in a *civil* context as opposed to in a criminal case.

Beyond questions of privacy, a broader concern is the potential for social media mining to create disproportionate harms for low-income taxpayers. As this Article will describe, low-income taxpayers are already subject to disproportionate rates of tax enforcement relative to most other income bands. Moreover, this economically vulnerable population is also subject to intrusive and judgmental monitoring in other contexts.[15] On balance, it strikes me that to use social media mining as a tax enforcement tool is to simply add a layer of further indignity onto a population that is already subject to increased digital surveillance by virtue of lacking income or wealth.

Thus, the primary focus of this Article is to question whether, in light of the IRS's need to make the most of diminished resources,[16] it is equitable to further automate its examination and collections tactics in a way that punishes unsophisticated behavior. In particular, this Article articulates a concern that the use of social media mining may pose a greater harm to low-income taxpayers relative to other types of taxpayers, in part because it is easier for the IRS to direct automated resources at the types of issues involved in examining those returns.[17] Many low-income families rely on the tax filing system to claim critical social welfare benefits such as the earned income tax credit and child

IRS has the broadest legal authority to collect information that minimizes privacy . . . ."). Likewise, Kimberly Houser and Debra Sanders have raised concerns about how the IRS is already using social media to collect taxpayer information, asserting that the IRS is engaging in social media data mining in ways that breach taxpayer privacy. Kimberly A. Houser & Debra Sanders, *The Use of Big Data Analytics by the IRS: Efficient Solutions or the End of Privacy as We Know It?*, 19 VAND. J. ENT. & TECH. L. 817, 817 (2017).

15 *See infra* notes 30–33 and accompanying text.

16 *See, e.g.*, *IRS Oversight: Treasury Inspector General for Tax Administration: Hearing Before the Subcomm. on Fin. Servs. & Gen. Gov't of the H. Comm. on Appropriations*, 116th Cong. 86 (2019) (testimony of J. Russell George, Treasury Inspector General for Tax Administration) [hereinafter George testimony]; Robert A. Weinberger, *Budget Blues for Tax Administration*, TAX POL'Y CTR. (Jan. 13, 2020) (showing in a chart how IRS appropriations fell by 21% from 2010 to 2020), https://www.taxpolicycenter.org/taxvox/budget-blues-tax-administration [https://perma.cc/G6ML-U2UY].

17 *See infra* Section I.B.2.

tax credit. Congress has chosen this system to reward and incentivize work and to help lift working families from poverty.[18] In many cases, the working families eligible for these benefits have a zero-tax liability because they earn less than the standard deduction. While taxpayers with annual income below the standard deduction are generally not required to file an income tax return, they must file a return to claim these valuable refundable credits. Concerns about how enforcement techniques involving social media mining may disproportionately impact low-income taxpayers are especially relevant in light of data from recent years showing that the IRS audits the poor at a similar rate to the highest-earning taxpayers[19] and in light of the IRS defending that practice as justified given its available resources.[20]

To clarify, this Article does not condone tax noncompliance, and as a tax attorney, I would never advise my clients that "a little cheating is OK." While taxpayer privacy and the possibility of disparate treatment of taxpayers are the main concerns of this Article, my thoughts are tempered with realism and cost-benefit considerations. Just as the police tolerate a little bit of speeding (e.g., ignoring those who drive seventy-four miles per hour in a seventy mile per hour zone, but pursuing those who drive eighty-five miles per hour), it does not seem practical or cost efficient to pursue every perceived case of tax

---

18 *See, e.g.*, MICHELLE LYON DRUMBL, TAX CREDITS FOR THE WORKING POOR: A CALL FOR REFORM (2019) (detailing the history of the earned income tax credit and child tax credit and exploring the reasons why Congress has chosen the IRS to administer these social benefits).

19 Paul Kiel, *It's Getting Worse: The IRS Now Audits Poor Americans at About the Same Rate as the Top 1%*, PROPUBLICA (May 30, 2019, 10:16 AM), https://www.propublica.org/article/irs-now-audits-poor-americans-at-about-the-same-rate-as-the-top-1-percent [https://perma.cc/CAK2-SE25].

20 William Hoffman, *IRS Exams Focus on EITC Claims, Not Poor, Inspector General Says*, TAX NOTES TODAY (Sept. 27, 2019), https://www.taxnotes.com/tax-notes-today-federal/tax-system-administration/irs-exams-focus-eitc-claims-not-poor-inspector-general-says/2019/09/27/29zm4 [https://perma.cc/G4RK-P9WE]. Subcommittee Chair Mike Quigley asked, "So if you have fewer resources, it makes sense to audit poor people more?" In response, Treasury Inspector General J. Russell George replied, "It's somewhat more complicated than that" and explained that audit work on EITC claimants is easier than on high-income taxpayers, "especially with the work of junior IRS employees. . . . The more sophisticated the income tax, the more involved it is, the longer it takes. It really boils down to how [the IRS] allocates their resources." *Id.* (alteration in original). Hoffman reports that when asked about possible racism or bias in IRS examination policies, George replied, "None of our work has shown any evidence that bias is occurring in terms of those with money versus those with less money . . . [b]ut there is no question that more low-income people are being examined than upper-income people." *Id.*; *see also* George testimony, *supra* note 16, at 86 ("As a percentage of overall enforcement revenue collected, the amount attributable to automated [functions are] increasing . . . [while o]ther types of enforcement actions . . . are decreasing.").

noncompliance. For example, is it worth it to devote resources to having the IRS manually investigate every social media post that suggests any hint of unreported income, no matter how small in dollar amount?[21]

This Article proceeds in three parts. Part I identifies the growing trend for public agencies and private third parties to use social media, automation, and other tools of technology to monitor or collect information on individuals. It identifies concerns and tensions that arise from this trend. It then considers how a taxpayer's statutory "right to privacy" applies in the context of information made available online by the taxpayer. While the taxpayer right to privacy is not clearly defined, it appears to refer to more than just the right of confidentiality of taxpayer information. Part II frames the issue of social media mining within broader reactions to punishing (or choosing not to punish) unsophisticated behavior and raises thoughts about how social media mining is different than investigating tips from whistleblowers. Part II then makes several proposals for the IRS to consider, starting with a call for the agency to provide the public with a clearer explanation of its understanding of the taxpayer "right to privacy." Part III, proceeding under the assumption that the IRS can and will access social media for enforcement purposes,[22] provides takeaways and thoughts for those attorneys who advocate on behalf of low-income taxpayers and represent them in their controversies with the IRS.

I
TENSIONS ARISING FROM THE COLLISION OF AUTOMATION, CONVENIENCE, PRIVACY, AND EXPECTATIONS

Examples abound of federal and state agencies, as well as private third parties, using big data algorithms, automated systems, and other tools of technology (including, but not limited to, social media mining) to monitor or collect information on individuals. In some cases,

---

21 This fits within broader questions of the appropriateness of leeway in law enforcement. *See* Shu-Yi Oei & Diane Ring, *Falling Short in the Data Age* (working paper) (on file with author) ("[I]ncreasing access to data and information will change the availability and shape of informal leeway in the law.").

22 While the primary focus of this Article is the possibility that the IRS may use social media at the examination and collections level, a recent Tax Court decision reveals the first known example of IRS Counsel using a social media post as evidence contradicting the petitioner's filing position. James Creech, *Oversharing on Social Media Reaches the Tax Court*, PROCEDURALLY TAXING (Sept. 3, 2020) (citing Brzyski v. Comm'r, T.C. Summ. Op. 2020-25 (Aug. 27, 2020)), https://proceduralytaxing.com/oversharing-on-social-media-reaches-the-tax-court/ [https://perma.cc/S99C-3B48].

individuals consent knowingly as a matter of convenience. In other instances, individuals are unaware they are being surveilled. The motivations for tracking individuals and collecting such data are varied, with rationales ranging from national security to marketing of consumer products and many things in between.

Section I.A first discusses some of the ways in which government agencies other than the IRS use technology to categorize or identify behaviors, and it then provides examples of how private third parties do so, including as a service to other individuals and, in some cases, the person being surveilled. Section I.A of the Article raises questions more than it provides answers: Where are we as a society with respect to privacy norms, and what is our comfort level with technological tracking? Under what circumstances do Americans seem to find it acceptable to sacrifice privacy (whether their own or that of others) as a means to achieve law enforcement, safety, or convenience? The examples used herein are intended to set a stage for how the public at large might feel about the IRS engaging in data mining for tax enforcement purposes.

Section I.B addresses notions of tax and privacy, reflecting on how the IRS has historically used publicly available information and imagining how the use of social media mining may change or build upon that use. The RFI reveals that the IRS is currently researching third-party options for machine-driven data mining on publicly available data.[23] When asked whether the government was interested in leveraging artificial intelligence-based technology to interpret text and image-based information on social media, the IRS responded that it "is open to any viable solution that fits our needs."[24] Thus, this Article imagines a variety of possibilities that might flow once the IRS opens the Pandora's box that is social media.

A. Is Our Collective Notion of Privacy Slowly Changing? Examples Outside the Realm of Tax Administration

As technology evolves, so too do norms and expectations. Public agencies and private companies alike use artificial intelligence, or AI, for a variety of predictive purposes. In some instances, predictive screening techniques may be employed by both government agencies and private industry in pursuit of the same goals, either in partnership

23 IRS RFI, *supra* note 2.

24 IRS, REQUEST FOR INFORMATION, NO. 2032H8-RFI-MEDIA, ANSWER 31, IRS SUPPLIED RESPONSES TO VENDOR QUESTIONS (on file with author).

or in parallel. For example, both the U.S. Department of Veterans Affairs and Facebook have created predictive tools for suicide screening and prevention.[25] The use of artificial intelligence by government agencies may have different policy or privacy implications than the use by private companies, but there also may be overlap. With its RFI, the IRS signals an intention to partner with private industry. Thus, in thinking about how the IRS may use social media to mine for data, it is helpful to consider analogies drawn both from other government agencies and from private companies.

1. Government Agency Use of Social Media Mining and Big Data

Federal and state government agencies engage in data mining in a variety of ways and for a whole host of purposes.[26] In their article addressing the IRS big data analytics program, Kimberly Houser and Debra Sanders reference a Senate report, noting that as of 2007 there were 52 different federal agencies using at least 199 different operating or planned data mining programs, including the IRS.[27] Many of these programs involved counterterrorism and national security but also included efforts to improve agency service or performance, analyze scientific and research information, manage human resources, and detect fraud, waste, and abuse.[28]

Government data mining fits within, or perhaps couples with, a larger trend of using automation to facilitate the administration of

---

25 Mason Marks, *Artificial Intelligence-Based Suicide Prediction*, 21 YALE J.L. & TECH. SPECIAL ISSUE 98, 102 (2019). Marks divides the types of AI tools used for suicide screening into two categories: "medical suicide prediction," which is undertaken within the healthcare system and involves the use of patient medical records, and "social suicide prediction," which refers to tech companies scrutinizing data, including social media data. *Id.* at 104–05. Medical suicide prevention is subject to various regulatory regimes that govern the healthcare industry, including but not limited to the Health Insurance Portability and Accountability Act. *Id.* at 105. Marks explains that the social suicide prevention is more controversial in that it lacks accountability and transparency. *Id.* at 109. As a government agency, Veterans Affairs is able to engage in both types of categories of suicide prevention screenings, medical and social. *Id.* at 105. Tech companies, on the other hand, do not have access to medical records due to privacy laws, and engage only in social suicide prevention screenings. *Id.* at 107.

26 As Houser and Sanders note, data mining can be predictive (meaning it analyzes and extrapolates data to make predictions about unavailable data) or descriptive (meaning it "summarizes properties of the data set"). Houser & Sanders, *supra* note 14, at 824.

27 *Id.* at 825; *Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 1 (2007).

28 U.S. GEN. ACCT. OFF., GAO 04-548, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 8 (2004).

social services to the public.[29] While efficient, automation also has identifiable downsides for individuals. In her book *Automating Inequality*, Virginia Eubanks provides alarming examples of how automated systems, ranking algorithms, and predictive risk models affect the lives of the poor and working-class communities, including individuals with respect to their use of various public services.[30] Eubanks provides three in-depth case studies in her book: automation of state welfare eligibility, an electronic registry of unhoused individuals, and a risk model created to predict which children might become victims of child abuse or neglect.[31] Eubanks notes that technologies are being integrated into social services "at a breathtaking pace, with little or no political discussion about their impacts," and she observes ways in which they "intensif[y] discrimination" and disproportionately affect low-income communities.[32] Eubanks notes that this digital trend is a modern continuation of the centuries-old ways in which the poor and working class are surveilled and stigmatized for being poor; she refers to this as the "digital poorhouse."[33]

Other scholars have identified similar concerns about the link between poverty and privacy. Using empirical data from a survey of low-income individuals, Mary Madden, Michele Gilman, Karen Levy, and Alice Marwick developed case studies of how big data tracking (including social media tracking) poses risks to the poor in the context of employment, access to higher education, and policing.[34]

These observations by Eubanks, as well as Madden and her coauthors, reinforce my concern that low-income taxpayers may find themselves under disproportionate scrutiny relative to other taxpayers. As I describe in Section I.B, the IRS's use of automated examination

---

29 For a discussion envisioning how regulators might use big data to personalize or individualize outcomes, see Jordan M. Barry, John William Hatfield & Scott Duke Kominers, *To Thine Own Self Be True? Incentive Problems in Personalized Law*, 62 WM. & MARY L. REV. (forthcoming 2021).

30 VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 9 (2018) ("Digital tracking and decision-making systems have become routine in policing, political forecasting, marketing, credit reporting, criminal sentencing, business management, finance, and the administration of public programs.").

31 *Id.* at 10.

32 *Id.* at 11–12.

33 *Id.* at 12.

34 Mary Madden, Michele Gilman, Karen Levy & Alice Marwick, *Privacy, Poverty, and Big Data: A Matrix of Vulnerability for Poor Americans*, 95 WASH. U. L. REV. 53, 54 (2017). "In each setting, low-income Americans face not only adverse inferences drawn based on their personally identifiable information (which often is erroneous), but also those drawn from their social media and demographic networks." *Id.* at 124.

techniques already disproportionately impacts the low-income taxpayer population.[35] Further exacerbating my concern, social science research has found that lower-income individuals are "comparatively unlikely to restrict their social media activity's visibility via privacy settings and are less hesitant to share sensitive information online."[36] Thus the very nature of their social media use makes them vulnerable to disproportionate scrutiny.

Inherent in concerns about the low-income populations is a concern about how these enforcement practices may impact taxpayers of different races. Scholars such as Dorothy Brown, Palma Joy Strand, Nicholas Mirkay, and Francine Lipman have identified structural ways in which income inequality and wealth inequality are racialized and how tax structures perpetuate or exacerbate these inequalities.[37] Ideally, the use of artificial intelligence and technology would be used to *reduce* inequality.[38] However, much like humans, algorithms are susceptible to bias.[39] Data privacy scholar Margaret Hu has argued that "algorithmically anchored" screening protocols are reminiscent of Jim Crow laws: the protocols may present on the front end as facially neutral while the results "may in fact have a disparate impact on traditionally protected classes."[40] Information studies scholar Safiya

---

35 I have also addressed this phenomenon in my previous scholarship. *See* Michelle Lyon Drumbl, *Those Who Know, Those Who Don't, and Those Who Know Better: Balancing Complexity, Sophistication, and Accuracy on Tax Returns*, 11 PITT. TAX REV. 113, 135 (2013) (examining and rethinking the application of the accuracy-related penalty to unsophisticated and low-income taxpayers, particularly in the context of complex provisions granting social benefits, such as the EITC).

36 Spencer Headworth, *Getting to Know You: Welfare Fraud Investigation and the Appropriation of Social Ties*, 84 AM. SOC. REV. 171, 189 (2019) (citing Madden et al., *supra* note 34).

37 DOROTHY BROWN, THE WHITENESS OF WEALTH 19–21 (2021) (describing how the persistent and widening black-white wealth gap is related to tax policy); *see also* Palma Joy Strand & Nicholas A. Mirkay, *Racialized Tax Inequity: Wealth, Racism, and the U.S. System of Taxation*, 15 NW. J.L. & SOC. POL'Y 265, 265 (2020); Francine J. Lipman, Nicholas A. Mirkay & Palma Joy Strand, *U.S. Tax Systems Need Anti-Racist Restructuring*, 168 TAX NOTES FED., Aug. 3, 2020, at 855, 856.

38 *See, e.g.*, I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1291 (2017) (positing that technology can be harnessed in ways that would deracialize policing, or at least make a "significant step in the right direction.").

39 Rumman Chowdhury & Narenda Mulani, *Auditing Algorithms for Bias*, HARV. BUS. REV., Oct. 24, 2018; *see also* Kristian Lum, *Limitations of Mitigating Judicial Bias with Machine Learning*, 1 NAT. HUM. BEHAV., No. 0141, June 26, 2017 (noting that judicial use of risk assessment tools in criminal cases are only as objective as how they are trained because machines will absorb the underlying human biases inherent in the data inputs), https://www.nature.com/articles/s41562-017-0141.pdf [https://perma.cc/5C2H-DHAZ].

40 Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 645 (2017). Hu writes,

Umoja Noble's recent book, *Algorithms of Oppression*, provides compelling examples of how algorithmic search engines discriminate against people of color, particularly women, and reinforce negative race and gender stereotypes.[41]

Privacy experts express concern over many different ways in which government agencies use cutting-edge technology and artificial intelligence—not just social media—as surveillance tools,[42] and the potential negative consequences to the public.[43] As one example, without knowledge or consent, the Federal Bureau of Investigation and the Immigration and Customs Enforcement agencies are using facial recognition software to scan state driver's license databases as a "routine investigative tool."[44] While the use of this has grown over time, a 2019 report revealed that facial recognition software

---

> Artificial intelligence and algorithms are not usually perceived as resulting in discrimination. In fact, they may appear to be equality-compliant or even equality-enhancing in that algorithmic screening and vetting can be applied equally across entire populations and subpopulations. Screening and classification systems, however, even when facially neutral and algorithmically based, can lead to profound constitutional challenges.

Id. at 650.

41 SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 17–18 (2018). As one of many examples, Noble describes her surprise when a Google search on her own computer using the term "black girls" retrieved results filled with pornography, despite the fact that her individual search history included engagement with Black feminist texts, videos, and books. *Id.*

42 Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1736, 1744 (2015) (explaining how certain government programs screen the public through big data protocols to create a class of big data blacklisted individuals) ("Specifically, [Hu's article] explains how, for example, matches and mismatches in big data systems can lead to inferential guilt that can directly or indirectly categorize individuals as administratively 'guilty until proven innocent' by virtue of digitally generated suspicion.").

43 Of airport facial scanning for security screening, technology columnist Geoffrey A. Fowler writes, "This has all the makings of a convenience trap. That's how privacy-invading technology—the stuff of China's police state—creeps into American life." Geoffrey A. Fowler, *Don't Smile for Surveillance: Why Airport Face Scans Are a Privacy Trap*, WASH. POST (June 10, 2019, 1:51 PM), https://www.washingtonpost.com/technology/2019/06/10/your-face-is-now-your-boarding-pass-thats-problem/ [https://perma.cc/B63F-MS44]; *see also* Shea Swauger, *Software That Monitors Students During Tests Perpetuates Inequality and Violates Their Privacy*, MIT TECH. REV. (Aug. 7, 2020), https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/ [https://perma.cc/R8BB-QWZC] (describing how algorithmic proctoring of online exams, which includes a facial recognition component, can result in racial and gender biases).

44 Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019, 12:54 PM), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [https://perma.cc/Z3KL-4R2V].

misidentified people of color more frequently than white people and misidentified women more frequently than men.[45] In what has been described as a first known case (and a terrifyingly dystopian one at that), a Black man in Detroit was wrongfully arrested and detained for thirty hours based on an erroneous match from a facial recognition algorithm.[46] Ironically, social media could have helped in this case: the man later realized he could have used his Instagram account to provide an alibi by showing he was elsewhere at the time the crime was committed.[47] As a result of concerns about discrimination and the potential for false positives, a handful of localities have banned the use of such technology.[48] In the wake of nationwide protests of police brutality following the killing of George Floyd, Amazon announced a one-year moratorium on the police use of Rekognition, the company's facial recognition technology,[49] and IBM announced that it "firmly opposes and will not condone" the use of such technology "for mass

45 Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019, 3:43 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ [https://perma.cc/B3CR-DM5X] ("The National Institute of Standards and Technology, the federal laboratory known as NIST that develops standards for new technology, found 'empirical evidence' that most of the facial-recognition algorithms exhibit 'demographic differentials' that can worsen their accuracy based on a person's age, gender or race."); *see also* Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html [https://perma.cc/4QB4-69FL] ("The systems falsely identified African-American and Asian faces 10 times to 100 times more than Caucasian faces . . . [a]nd falsely identified older adults up to 10 times more than middle-aged adults.").

46 Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/L9D3-TDZZ]. While referring to this as the first known case of its kind, the article quotes Clare Garvie, a lawyer from the Georgetown University Center on Privacy and Technology who has written about concerns with facial recognition technology: "I strongly suspect this is not the first case to misidentify someone to arrest them for a crime they didn't commit. This is just the first time we know about it." *Id.*

47 *Id.* In the proposals I set forth in Section II.C, I suggest the IRS might restrict its use of social media mining to constructive purposes, such as when the taxpayer requests it to resolve a dispute.

48 Harwell, *supra* note 45 (stating that San Francisco and Oakland in California, and Somerville and Brookline in Massachusetts, passed bans in 2019 on facial recognition use by public officials, and the State of California banned the software's use in police body cameras).

49 Jay Greene, *Amazon Bans Police Use of Its Facial-Recognition Technology for a Year*, WASH. POST (June 10, 2020, 5:31 PM), https://www.washingtonpost.com/technology/2020/06/10/amazon-rekognition-police/ [https://perma.cc/S38P-A2K8].

surveillance, racial profiling, [or] violations of basic human rights and freedoms."[50]

As to the appropriateness of government agencies using big data mining techniques, one might also draw a logistical distinction between civil and criminal investigations. One might more readily support the use of artificial intelligence, social media mining, and digital surveillance to investigate a crime, and I address this distinction in Section I.B. In some cases, a warrant may be required as a procedural safeguard prior to a search, but Fourth Amendment protections generally do not extend to government agents gathering information on social media.[51] In this regard, social media use is similar to the countless ways in which we are all being monitored daily without a warrant: by security cameras in stores, by red-light cameras,[52] and by email providers and internet servers.

In many respects, we consensually (if unthinkingly) sacrifice our own privacy any time we leave the house.[53] How, then, can anyone reasonably expect to have privacy rights in any of the information they post on Twitter, Instagram, or Facebook? It is true that those platforms offer a sliding continuum of privacy options; for example, one can choose to share Facebook posts only with those they have "friended" on Facebook. That said, we obviously lose control of information the instant we publish it even to a limited audience; for example, most people are cognizant that a private email or text sent to a friend, or a screenshot thereof, can be easily forwarded to an unlimited number of

---

50 BBC News, *IBM Abandons 'Biased' Facial Recognition Tech*, BBC (June 9, 2020), https://www.bbc.com/news/technology-52978191 [https://perma.cc/6QZ6-K75R].

51 *See, e.g.*, United States v. Gatson, No. 13-705, 2014 WL 7182275, at *22 (D.N.J. Dec. 16, 2014) (holding that an undercover operation in which law enforcement created an undercover Instagram account and "friended" the suspect in order to view photos and other information that he posted to his account did not require a warrant). For a comprehensive discussion of privacy rights and social media posts, including a summary of *Gatson* and other relevant caselaw, see Brian Mund, *Social Media Searches and the Reasonable Expectation of Privacy*, 19 YALE J.L. & TECH. 238, 240 (2018) ("An exploration of the extant case law shows that social media users have no reasonable expectation of privacy in their social media postings—even if users communicate their information behind password-protected pages.").

52 I. Bennett Capers cites red-light cameras and other technological innovations, coupled with access to big data, as other possible ways to make "policing more transparent, accountable, and egalitarian." I. Bennet Capers, *Techno-Policing*, 15 OHIO ST. J. CRIM. L. 495, 499 (2018).

53 *See* Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 248 (2008) ("[For example,] a person would have to be a hermit to be able to function in our society without voluntarily disclosing a vast amount of personal information to a vast array of public and private demanders.").

other people. And people, even those not on social media themselves, have no control at all over what others may post about them.

In comparing the IRS to other government agencies, perhaps the most useful analogy would be to those agencies that administer social welfare benefits, such as the Social Security Administration and state departments of social services. I draw upon these examples in particular because Congress has chosen to use the IRS, and the tax filing process, to administer and deliver a number of social benefits to the public.[54] Most notable of these benefits is the earned income tax credit (EITC), a refundable tax credit paid to approximately 25 million low-income families each year as part of their income tax refund.[55] Lawrence Zelenak has aptly described the EITC as "a welfare program that happens to be administered through the tax system"[56] while also suggesting that because it is housed in the Internal Revenue Code, there is a higher tolerance for EITC overpayments than for general welfare overpayments.[57]

Unlike the EITC, for which claimants self-certify, more traditional welfare benefits such as the Supplemental Nutrition Assistance Program (SNAP),[58] Temporary Assistance for Needy Families (TANF), and Social Security Disability Insurance (SSDI) are subject to verification procedures before the benefits are awarded. In addition, recipients of these benefits are also subject to investigation if fraud is suspected during or after receipt of the benefit.[59]

This use of social media mining for investigating welfare fraud appears to be widespread among state and local agencies, in particular

---

54 Over time, these benefits have included income-based refundable credits to working families, as well as expenditure-based refundable credits such as the First-Time Homebuyer Credit, the Adoption Tax Credit, the Premium Tax Credit, and a variety of education credits. Drumbl, *Those Who Know*, *supra* note 35, at 119–39.

55 *EITC Fast Facts*, IRS, https://www.eitc.irs.gov/partner-toolkit/basic-marketing-communication-materials/eitc-fast-facts/eitc-fast-facts [https://perma.cc/MC72-CADU].

56 Lawrence Zelenak, *Tax or Welfare? The Administration of the Earned Income Credit*, 52 UCLA L. REV. 1867, 1869 (2005). Zelenak distinguishes the EITC from other welfare programs, such as SNAP and TANF, because the EITC is predicated on earned income.

57 *Id.* at 1874.

58 SNAP is the program formerly known as Food Stamps. U.S. GOV'T ACCT. OFF., GAO 14-641, SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM: ENHANCED DETECTION TOOLS AND REPORTING COULD IMPROVE EFFORTS TO COMBAT RECIPIENT FRAUD, at 3 (2014) [hereinafter SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM].

59 *See* Headworth, *supra* note 36, at 171 ("[F]ederal law requires state governments to maintain dedicated fraud control units . . . . These units are busy [and] primarily focus [on SNAP.]").

for enforcement of SNAP eligibility.[60] The Social Security Administration also has publicly acknowledged that its adjudicators use social media in evaluating cases and has stated it will consider expanding such use.[61]

Sociologist Spencer Headworth describes how SNAP investigators manually search social media by viewing publicly available posts to gather information about household circumstances, such as who lives in the household, relationship status, and vacation photos.[62] Some fraud investigations arise from social media posts that are less subtle: Washington State Department of Social and Health Services fraud investigators came across a social media post offering to trade "great organic marijuana" for an EBT card, leading to an arrest of an individual on both food benefit trafficking and drug charges.[63] In other cases, social media leads originate from outside the agency: in Pennsylvania, a woman who offered on Facebook to trade her EBT card for cash was arrested after a member of the public tipped off the state's fraud unit.[64]

---

60 *See, e.g.*, SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM, *supra* note 58 (reviewing fraud detection tools used in eleven states, including both automated and manual monitoring of social media).

61 SOC. SEC. ADMIN., BUDGET ESTIMATES AND RELATED INFORMATION: FY 2020, https://www.ssa.gov/budget/FY20Files/2020BO_1.pdf [https://perma.cc/UH24-TCDY]. The Budget Overview states,

> Currently, agency adjudicators use social media information to evaluate a beneficiary's symptoms when there is a [Cooperative Disability Investigation] unit's Report of Investigation that contains social media data corroborating the investigative findings. In FY 2019, we are evaluating how social media could be used by disability adjudicators in assessing the consistency and supportability of evidence in a claimant's case file.

Id. at 26; *see also* Sarah Min, *Social Security May Use Your Facebook and Instagram Photos to Nix Disability Claims*, CBS NEWS (Mar. 21, 2019, 8:46 AM), https://www.cbsnews.com/news/social-security-disability-benefits-your-facebook-instagram-posts-could-affect-your-social-security-disability-claim/ [https://perma.cc/R34V-6VFJ].

62 Headworth, *supra* note 36, at 187–88. Of his interviews with fraud enforcement workers, "[s]ome investigators described Facebook as their most valuable tool, and some saw it as much less useful." *Id.* at 188.

63 Press Release, *Want to Trade EBT Card for Marijuana?*, WASH. ST. DEP'T OF SOC. & HEALTH SERVS. (Feb. 6, 2017), https://www.dshs.wa.gov/sesa/office-communications/media-release/want-trade-ebt-card-marijuana [https://perma.cc/55U5-U8N4]. Journalist Kalena Thomhave took note of the way in which this specific press release "celebrated the arrest" and how the press release "began ominously, 'Note to would-be food benefits traffickers. You're being watched.'" Kalena Thomhave, *Another Way to Police the Poor*, AM. PROSPECT (Mar. 11, 2019), https://prospect.org/economy/another-way-police-poor/ [https://perma.cc/RZV9-RCFV].

64 Press Release, *OIG Charges Williamsport Woman with SNAP Trafficking for Selling Her Food Stamp Benefits on Facebook. She Exchanged Benefits for Heroin*, PA. OFF. OF

Some state agencies have tried using software programs as an automated tool for social media mining, with mixed results. The Department of Agriculture Food and Nutrition Service (FNS) provided guidance to state agencies that wanted to set up such software to detect benefit trafficking on social media sites.[65] A U.S. Government Accountability Office review of eleven states that experimented with that approach reported that only one state found the automated approach effective; the other states found the automated tools impractical (either because of technical difficulties or because of the high false positive rate) and preferred to devote their resources to manual searches.[66]

As public policy student and freelance writer Kalena Thomhave explains, social media investigations are a modern-day continuation of the type of invasion of privacy endemic in welfare fraud investigations.[67] Thomhave attributes this to the "dichotomy between those who are *deserving* and *undeserving* of public benefits, with the government as arbiter, [which] lies at the foundation of the American social safety net."[68] Though Thomhave's remarks are directed at other agencies that administer social benefits and do not mention the IRS, one cannot ignore the fact that the EITC is part of the social safety net for working families and the fact that the IRS has identified the EITC as a targeted area of enforcement.[69] This underscores my concern that the IRS may set its social media sights on EITC recipients, a concern I address in more detail in Section I.B.

INSPECTOR GEN. (Mar. 24, 2017), https://www.media.pa.gov/Pages/inspector-general-Details.aspx?newsid=35 [https://perma.cc/U93P-EXDC]. In Section II.B, I discuss the IRS Whistleblower program, and I raise the question of whether the IRS should encourage the public to report tax-related social media posts to the agency.

65 SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM, *supra* note 58, at 23.

66 *Id.* at 17 ("Our testing found the recommended e-commerce monitoring tool less effective than manual searches in detecting postings indicative of potential trafficking, and we found the tool for monitoring social media to be impractical for states due to the volume of irrelevant data.").

67 Thomhave, *supra* note 63 ("[I]n the 1960s, welfare officials would regularly make unannounced home visits (sometimes even 'midnight raids') to women receiving traditional cash benefits to see if they lived in accordance with welfare eligibility rules."). While not referring specifically to social media mining, sociologist Spencer Headworth comments on loss of privacy: "Making their lives transparent and legible to state agencies is one way the poor pay for public assistance." Headworth, *supra* note 36, at 172.

68 Thomhave, *supra* note 63 (emphasis in original).

69 *See generally* Michelle Lyon Drumbl, *Beyond Polemics: Poverty, Taxes, and Noncompliance*, 14 EJOURNAL OF TAX RSCH. 253, 254 (2016) (identifying the high rate of improper payments as one explanation of the high audit rate of EITC returns).

2. Private Actor Use of Social Media Mining and Big Data

As noted, the use of artificial intelligence to screen individuals extends beyond government agencies to the private sector, and some companies are using social media algorithms as a screening tool, just as the IRS seeks to do. One such online service company, Predictim, ceased operation after it faced backlash for its methods.[70] Predictim had used AI to scan social media posts to assess babysitters' personalities.[71] This cyber-sleuthing service apparently appealed to some anxious parents worried about leaving their child with an unknown person; the company asserted that its algorithm could predict such things as a sitter's risk of drug use, tendency to bully, or even a "bad attitude."[72] Predictim provided parents a risk rating based on the results of the algorithm, but the company did not explain how the algorithm arrived at that risk rating, and the results were not shared with the potential babysitter.[73]

Though Predictim no longer offers this service, technology reporter Drew Harwell observes that this type of technology is increasingly used by companies in other types of hiring.[74] Harwell notes that companies use such methods in recruiting, hiring, and reviewing their workers, "offering employers an unrivaled look at job candidates through a new wave of invasive psychological assessment and surveillance."[75]

Insurance companies are another class of private actor eager to utilize information from social media, whether as a tool to determine risk (and therefore premium rates) or to detect fraud.[76] One

---

70 Predictim halted its service after backlash from media publicity, including a Washington Post article, and after it was blocked by Facebook, Twitter, and Instagram. Drew Harwell, *AI Start-Up That Scanned Babysitters Halts Launch Following Post Report*, WASH. POST (Dec. 14, 2018, 8:44 AM), https://www.washingtonpost.com/technology/2018/12/14/ai-start-up-that-scanned-babysitters-halts-launch-following-post-report/ [https://perma.cc/TN2K-3EDD].

71 Drew Harwell, *Wanted: The 'Perfect Babysitter.' Must Pass AI Scan for Respect and Attitude*, WASH. POST (Nov. 23, 2018, 8:50 AM), https://www.washingtonpost.com/technology/2018/11/16/wanted-perfect-babysitter-must-pass-ai-scan-respect-attitude/ [https://perma.cc/WTB2-N7GQ] ("[Predictim uses] language-processing algorithms and an image-recognition software known as 'computer vision' to assess babysitters' Facebook, Twitter and Instagram posts for clues about their offline life.").

72 *Id.*

73 *Id.*

74 *Id.* ("[Tech firms sell to employers] artificial-intelligence systems that analyze a person's speech, facial expressions and online history with promises of revealing the hidden aspects of their private lives.").

75 *Id.*

76 Jessica Baron, *Life Insurers Can Use Social Media Posts to Determine Premiums, as Long as They Don't Discriminate*, FORBES (Feb. 4, 2019, 1:26 PM), https://www.forbes

commentator's concern about insurance companies' use of this practice could be generalized as an overarching concern that any type of social media mining can be potentially misleading.[77] "If you've given up smoking but have old photos with cigarette in hand (or repost one of those popular Facebook Memories) how can a computer (or even an underwriter with a lot of work to do) properly assess the context of a photo?"[78] Moreover, the image social media users cultivate online often does not portray real life. In turn, this can limit the value of the information obtained on social media and create time-consuming false positives for the agency or company engaging in the search.[79]

People seem willing to tolerate and consent to privacy losses coupled with technology (often in connection with their smartphone) for a host of reasons, ranging from convenience to reassurance to rewards. Consider also the example of summer sleep-away camps offering a facial-recognition service, with an app sending the camper's parents a notification the moment their child's photograph is uploaded to its site.[80] In 2019, the University of Alabama offered its students an incentive to opt into cell phone–based location tracking because football coach Nick Saban did not like that students were leaving the stadium before games ended.[81] The school created an app that students could download on their smartphone to verify that they attended and stayed at games for the full four quarters of the contest; those who did so accumulated reward points, which would be used to provide preferred access to tickets for championship games.[82] During the first

.com/sites/jessicabaron/2019/02/04/life-insurers-can-use-social-media-posts-to-determine-premiums/#7e18b19f23ce [https://perma.cc/SZW6-AFGW].

77 *Id.*

78 *Id.* In the context of life insurance, a cigarette represents a health risk for actuarial purposes, as would certain hobbies such as skydiving or motorcycle riding. As other scholars have noted, surveillance of poor people may focus on the use of cigarettes and alcohol, or perhaps gambling. *See* EUBANKS, *supra* note 30, at 114 (discussing the example of Maine Governor Paul LePage).

79 *See* discussion *infra* Section II.A.

80 Drew Harwell, *As Summer Camps Turn on Facial Recognition, Parents Demand: More Smiles, Please*, WASH. POST (Aug. 8, 2019, 1:26 PM), https://www.washingtonpost.com/technology/2019/08/08/summer-camps-turn-facial-recognition-parents-demand-more-smiles-please/?hpid=hp_hp-top-table-main_facecamp-815pm%3Ahomepage%2Fstory-ans [https://perma.cc/UA47-7K3X].

81 Alex Scarborough, *Bama Tracking Students to Check 4-Quarter Stays*, ESPN (Sept. 13, 2019), https://www.espn.com/college-football/story/_/id/27608647/bama-tracking-students-check-4-quarter-stays [https://perma.cc/9NPQ-RYXZ].

82 Billy Witz, *Orwellabama? Crimson Tide Track Locations to Keep Students at Games*, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/09/12/sports/alabama-tracking-app.html [https://perma.cc/KM9X-AAS6] ("Greg Byrne, Alabama's athletic director,

game the incentive was available, so many students opted in that the stadium's network servers went down.[83]

For better or for worse, these sorts of commercial uses of data mining and surveillance may have the effect of desensitizing people, especially younger generations, to the loss of privacy. But what is it that we should actually expect of our revenue agency, or of our federal government? The next section explores the taxpayer "right to privacy" and examines these issues through a tax-specific lens.

B. What Is a Taxpayer's Right to Privacy?

In 2015, Congress codified a Taxpayer Bill of Rights (TBOR), which the Taxpayer Advocate refers to as a list of ten fundamental rights that taxpayers should be aware of when dealing with the IRS.[84] Internal Revenue Code (the Code) § 7803(a)(3) provides, "In discharging his duties, the Commissioner shall ensure that employees of the Internal Revenue Service are familiar with and act in accord with taxpayer rights as afforded by other provisions of this title," and lists the ten rights. Number seven on the list is "the right to privacy."[85] There is a separately enumerated taxpayer right to confidentiality (number eight on the list), which addresses how and with whom the IRS can share taxpayer information.[86] By statutory implication, this means the right to privacy is more than just a right to have one's tax information kept private from the public.

In his literature review of contemporary scholarship on tax and privacy, Michael Hatfield categorizes the common characteristics that frame the scholarly conversation about privacy.[87] With one notable exception that relates to low-income taxpayers and the privacy sacrifices they make in exchange for refundable tax credits,[88] Hatfield

---

said privacy concerns rarely came up when the program was being discussed with other departments and student groups.").

83 *Id.* Though not an Alabama fan or college student, my own teenage son told me he would gladly consent to such tracking in order to secure College Football Playoff tickets.

84 I.R.C. § 7803; *Taxpayer Bill of Rights*, IRS (Nov. 25, 2020), https://www.irs.gov/taxpayer-bill-of-rights [https://perma.cc/UH33-R82A].

85 I.R.C. § 7803(a)(3)(G). I.R.C. § 6103 provides a detailed set of limitations on how and when the agency may disclose taxpayer information.

86 I.R.C. § 7803(a)(3)(H).

87 Hatfield, *supra* note 14, at 604–10.

88 *See* Hayes Holderness, *Taxing Privacy*, 21 GEO. J. POVERTY L. & POL'Y 1, 30–32 (2013) (expressing concern that the EITC, like other social welfare programs, imposes a privacy burden on its recipients). As I discuss in the next section, this privacy burden

finds that "privacy" scholarship focuses on protection from the *disclosure* of information (i.e., what the IRS can do with information it collects) rather than how we conceive of privacy limitations on the *collection* of information.[89] Hatfield describes the Code's privacy protections as "aim[ing] to maintain the confidentiality of taxpayer information"[90] while noting that the IRS has authority "to collect any information relevant to the 145,000,000 individual income tax returns filed each year."[91]

If privacy and confidentiality are distinct rights and disclosure rules primarily protect confidentiality, then what exactly is meant by the "right to privacy?"[92] At the time of this writing, there is no case law interpreting § 7803(a)(3)(G),[93] nor are there Treasury Regulations providing formal administrative guidance on the various taxpayer rights.[94] Adam Thimmesch, a tax scholar who has written about

---

intersects with the fact that low-income taxpayers are disproportionately selected for audit when they claim the EITC.

89 Hatfield, *supra* note 14, at 606; *see also* Adam B. Thimmesch, *Tax Privacy?*, 90 TEMP. L. REV. 375, 375 (2018) ("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.").

90 Hatfield, *supra* note 14, at 596. Hatfield points to § 6103, which generally provides that tax return information shall be kept confidential. *Id.* at 598. Hatfield notes that the IRS can collect any relevant information about taxpayers without probable cause of a crime or suspicion of a misstatement or understatement of any kind. *Id.* at 580.

91 *Id.* at 580 (describing examples of cases in which the IRS reviewed medical records, love letters, family dynamics, reading habits, and other details of people's private lives). Hatfield argues that tax scholarship "has not addressed the risks of excessive information collection." *Id.* at 610.

92 *See* Joshua P. Law, *Balancing Efficient IRS Administration and Taxpayer Rights*, 43 SETON HALL LEGIS. J. 337, 348 (2019) (presenting a brief synopsis of the right to privacy in a note that was published after Hatfield's literature review) ("The [taxpayer's] right to privacy is ostensibly meant to guarantee taxpayers assurance that information about their financial situation will not be intruded upon without due cause; however, the IRS currently remains far from full compliance with this right.").

93 Courts have stated that the Taxpayer Bill of Rights does not create any *new* rights. *See* Moya v. Comm., 152 T.C. 182, 192 (2019) ("We think that the history of the IRS TBOR makes clear that it accords taxpayers no rights they did not already possess."); Facebook v. IRS, No. 17-cv-06490-LB, 2018 WL 2215743, at *13 (N.D. Cal., May 14, 2018) ("The statutory TBOR enacted as part of the 2015 PATH Act did not grant new enforceable rights."); Atl. Pac. Mgmt. Grp. v. Comm'r, 152 T.C. 330, 336 (2019) ("[S]ection 7803(a)(3) itself does not confer any new rights on taxpayers; it merely lists 'taxpayer rights as afforded by other provisions of the Code.").

94 Whether taxpayer rights are even enforceable is also an open question. *See* Alice G. Abreu & Richard K. Greenstein, *The U.S. Taxpayer Bill of Rights: Window Dressing or Expression of Justice?*, 4 J. TAX ADMIN. 25, 27 (2018); Leandra Lederman, *Is the Taxpayer Bill of Rights Enforceable?* (Ind. Univ. Maurer Sch. of L., Working Paper No. 404, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3365777 [https://perma.cc/WCE9

privacy, refers to the TBOR's statutory right to privacy as "aspirational," insofar as the standard is loose and subjective, and there is no apparent remedy.[95]

The IRS defines the right to privacy as follows: "Taxpayers have the 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 respect all due process rights, including search and seizure protections, and will provide, where applicable, a collection due process hearing."[96] The IRS elaborates on the examination process as follows:

> The process of selecting a return for examination usually begins in one of two ways. First, we use computer programs to identify returns that may have incorrect amounts. These programs may be based on information returns, such as Forms 1099 and W-2, on studies of past examinations, or on certain issues identified by compliance projects. Second, we use information from outside sources that indicates that a return may have incorrect amounts. These sources may include newspapers, public records, and individuals. If we determine that the information is accurate and reliable, we may use it to select a return for examination.[97]

As a starting point, then, query whether the IRS looking at public social media accounts or other publicly available online information would constitute a violation of a taxpayer's right to privacy. It seems intuitive that if an individual makes information about him or herself

---

-3PJ7]. *But see* T. Keith Fogg, *Can the Taxpayer Bill of Rights Assist Your Clients?*, 91 TEMP. L. REV. 705, 729 (2019) (arguing that the taxpayer's right to privacy has a role in examination cases with respect to a revenue agent seeking information from third parties, and in collection cases with respect to the loss of privacy that results from the filing of a notice of federal tax lien).

95 Thimmesch, *supra* note 89, at 392–93. Thimmesch observes that tax design must weigh privacy interests, whether those are described in neutral or normative terms, against potential information-collection harms (among other potential harms). *Id.* at 414. Building on the work of Daniel Solove, Thimmesch notes that "information-collection harms occur regardless of whether the information is collected through surveillance or through direct interrogation" and "regardless of whether the information is collected by the government or by a private actor." *Id.* at 412 (citing Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 491–92 (2006)).

96 IRS, PUBL'N NO. 1, YOUR RIGHTS AS A TAXPAYER (Sept. 2017) (emphasis added), https://www.irs.gov/pub/irs-pdf/p1.pdf [https://perma.cc/E7WQ-EG5C]. The right to confidentiality is described distinctly: "Taxpayers have the right to expect that any information they provide to the IRS will not be disclosed unless authorized by the taxpayer or by law." *Id.*

97 *Id.*

publicly available on such accounts, that individual has no reasonable expectation of privacy with respect to what has been posted.[98]

To reiterate, the primary concern of this Article is not whether the IRS looking at social media violates the taxpayer's right to privacy or whether the IRS has the right to access and use this information for enforcement purposes. I think the better question is whether, as a matter of social policy, it is appropriate and desirable, or even cost-effective, for the IRS to mine social media for civil enforcement purposes. As the prior section explained, other government agencies can and do access social media to investigate various types of benefits fraud. But most tax noncompliance does not constitute "fraud."

1. IRS Use of Data Analytics—Past and Future

The IRS has been using data analytics to address noncompliance since long before Facebook and Instagram. Since the 1960s, the agency has used something called Discriminant Function (DIF) scoring to select returns for audit.[99] The DIF score is a three-digit score assigned by a series of algorithms and models, the contents of which are not known outside the IRS.[100] According to the IRS, the DIF "score rates the potential for [tax liability] change, based on past IRS experience with similar returns"—with a higher score more likely to be selected for examination.[101] The DIF is used as a screening tool, and a return identified by a DIF score is manually classified by an "experienced [IRS] examiner" in order to screen for significant issues "worthy of exam."[102]

The examination selection process has evolved over time through the use of technology and automation, and over time these methods have increased the efficiency of audits by using data to identify returns

---

98 Stacey Vanek Smith, *When the IRS 'Likes' Your Facebook Update*, MARKETPLACE (Apr. 14, 2014) https://www.marketplace.org/2014/04/14/when-irs-likes-your-facebook-update/ [https://perma.cc/KJQ9-UT38]. As tax scholar Edward Zelinsky remarked, "It's hard to believe that anybody who puts anything on Facebook has any legitimate expectation of privacy." *Id.*

99 *See* Carina Federico & Travis Thompson, *Do IRS Computers Dream About Tax Cheats? Artificial Intelligence and Big Data in Tax Enforcement and Compliance*, J. TAX PRAC. & PROC., Feb.–Mar. 2019, at 43, 45; TOM GREENAWAY & ALEXANDRA DESANTIS, *Taking the Mystery Out of Examinations—the Audit Process*, *in* 1 EFFECTIVELY REPRESENTING YOUR CLIENT BEFORE THE IRS 3-3 (Keith Fogg ed., 7th ed. 2018).

100 GREENAWAY & DESANTIS, *supra* note 99, at 5; *see also* IRM 4.1.5.3.3.1(1) (Sept. 21, 2020).

101 I.R.S. Fact Sheet FS-2006-10 (Jan. 2006).

102 IRM 4.1.5.3.3.1 (Sept. 21, 2020) ("Classifiers must use their skills, technical expertise, local knowledge, and experience to identify hidden, as well as obvious, issues.").

more likely to be noncompliant.[103] Other examples include the IRS automated underreporter program that matches returns with third-party reporting and the requirement implemented in 1987 to list identification numbers of dependents.[104] The IRS also screens individual income tax returns using databases external to the agency to detect errors and noncompliance. For example, returns claiming the EITC are screened against the Dependent Database, which includes information from external sources.[105] These returns are scored according to certain indicators, with a higher score suggesting a greater probability that a taxpayer may not meet the credit's residency, relationship, or age eligibility requirements.[106]

While the public does not know how DIF scores are calculated, or exactly what information is entered into the Dependent Database and from which sources, it stands to reason that the possibilities of social media data mining extend far beyond the traditional tools used for return screening.

In their 2017 article, Kimberly Houser and Debra Sanders detail how the IRS is already engaging in data mining of public and commercial data pools, including social media sites such as Facebook, Instagram, and Twitter, and using that information to run predictive algorithms.[107] In addition to raising procedural and due process concerns about this practice,[108] Houser and Sanders also express a concern that the IRS's use of such algorithms may result in discrimination.[109]

---

103 *See generally* Houser & Sanders, *supra* note 14, at 828–33.

104 *Id.* at 829; *see also* James Alm et al., *New Technologies and the Evolution of Tax Compliance*, 39 VA. TAX REV. 287, 312–13.

105 *See* NAT'L TAXPAYER ADVOC., THE EARNED INCOME CREDIT, 3 SPECIAL REPORT TO CONGRESS 2020, at 5 n.26. ("The [Dependent Database] is a rule-based system incorporating data within the IRS and information from external sources such as the Department of Health and Human Services and the Social Security Administration."); *see also* IRM 4.19.14.1.1 (Dec. 7, 2017) ("Exam receives the majority of its EITC work from the Dependent Database [] and Electronic Fraud Detection System.").

106 NAT'L TAXPAYER ADVOC., *supra* note 105, at 27. The Dependent Database is referenced in IRM 4.19.14.8 (Apr. 4, 2019), but most of the details are redacted.

107 Houser & Sanders, *supra* note 14, at 819–20. Houser and Sanders also detail other types of privacy breaches not discussed in this Article, including how the ACLU has found that the IRS purchased cell phone tracking technology and also discovered in 2013 that the IRS policy permitted the reading of private emails without a warrant (it has since agreed to stop doing so). *Id.* at 822–23.

108 *Id.* at 843 (identifying ways in which the IRS data collection and analytics practices may violate the Administrative Procedures Act and/or due process protections).

109 *Id.* at 848–50 ("[Algorithms] may result in targeting certain groups based on the associations created as the algorithm learns . . . . [And t]he New York Police Department came under fire for its use of predictive analytics to focus its policing on certain communities."). *But see generally* I. Bennett Capers, *Race, Policing, and Technology*,

My greatest concern, which Houser and Sanders do not specifically raise, is that data mining of social media sources will disproportionately impact low-income taxpayers. As I[110] and others[111] have highlighted elsewhere, low-income taxpayers are already disproportionately in the examination spotlight: in fiscal year 2018, the audit rate for all individual taxpayers was 0.59%; when broken down by level of adjusted gross income (AGI), a higher percentage of taxpayers with AGI between $1 and $25,000 were audited (0.69%) than those with AGI between $25,000 and $499,000.[112] As the next section addresses, audits of low-income taxpayers are typically time-consuming, burdensome, and stressful. Taxpayers are asked to provide documentation substantiating fact-intensive questions, such as who lives in their household, what their relationship to those individuals is, and how much support the taxpayer provides to those individuals.[113] For low-income taxpayers, audits can pose an economic hardship for those cases in which the IRS freezes the valuable refundable credit portion of the refund until the audit is resolved.[114]

---

95 N.C. L. REV. 1241 (2017) (advocating for the harnessing of surveillance technology to deracialize policing and describing the necessary redistribution of privacy).

110 *See* MICHELLE LYON DRUMBL, TAX CREDITS FOR THE WORKING POOR (2019).

111 Kiel, *supra* note 19 ("[A]udits of the rich continue to plunge while those of the poor hold steady, and the two audit rates are converging . . . . [EITC recipients] are audited at a higher rate than all but the richest taxpayers.").

112 I.R.S., PUB. NO. 55B, DATA BOOK: 2018, at 27 (May 2019). At AGI levels above $500,000, the audit rate is higher, and the tiny number of the taxpayers at the highest end are subject to a sharply higher rate: the audit rate of taxpayers with AGI between $500,000 and $1 million was 1.1%; taxpayers with AGI between $1 million and $5 million had an audit rate of 2.21%; taxpayers with AGI between $5 million and $10 million faced an audit rate of 4.21%, and 6.66% of taxpayers with AGI above $10 million were audited. *Id.* Note that taxpayers who reported no AGI were also subject to a higher than average audit rate (2.04%); this includes returns with losses, and a taxpayer with no AGI cannot claim EITC. *Id.*

113 *See* I.R.C. §§ 2(b), 7703(b), 24, 32, 151 and accompanying Treasury Regulations (setting forth the eligibility requirements for head of household filing status, marital status, the child tax credit, the EITC, and the dependent exemption). These various eligibility requirements overlap imperfectly and can be particularly complicated to apply to multigenerational households and shared child custody situations. Examiners ask taxpayers to prove residence of individuals through the use of such documents as school records, medical or social service records, and court orders, if applicable. *See, e.g.*, I.R.S. Form 886-H-EIC (Oct. 2019), https://www.irs.gov/pub/irs-pdf/f886he.pdf [https://perma.cc/Y2LN-YAKZ].

114 *See infra* text accompanying note 120.

2. Disproportionate Enforcement on Lower-Income Taxpayers, and Implications for Taxpayer Privacy

The higher audit rate of these low-income taxpayers, relative to the moderate-income taxpayers, is due in part to the fact that the IRS prioritizes audits of returns claiming the EITC. In recent years, more than one in three individual income tax returns selected for examination involved an EITC claim.[115] The EITC remains an enforcement priority for the IRS even as other types of examinations have declined and even though the overall number of returns with EITC claims has not increased in recent years.[116] The IRS has been subject to criticism for shining the spotlight on the poor rather than the rich, as well as for the demographic consequences of this enforcement strategy.[117] A former IRS economist who analyzed exam coverage data and estimated how it breaks down by county and state reported that taxpayers in the rural south are being audited at disproportionately high rates; according to his estimates, the ten most-heavily audited counties in the United States are disproportionately rural, low-income, and nonwhite.[118]

---

115 In 2018, 37% of audited returns were selected on the basis of an EITC claim. I.R.S., PUB. NO. 55B, *supra* note 112, at 23–26. Table 9a shows that 150,043,227 individual income tax returns were filed; of this total, 892,187 were selected for audit, representing an overall individual income tax audit rate of 0.59% for FY 2018. *Id.* Of the 892,187 returns selected for audit, footnote 5 specifies that 330,359 (37%) were selected for audit on the basis of an EITC claim. *Id.* at 126 n.5. *See also* Paul Kiel & Jesse Eisinger, *Who's More Likely to Be Audited: A Person Making $20,000—or $400,000?*, PROPUBLICA (Dec. 12, 2018, 5:00 AM), http://www.propublica.org/article/earned-income-tax-credit-irs-audit-working-poor [https://perma.cc/HMP7-DDVR] (describing how EITC audits have increased as a proportion of audits over a period of time in which IRS resources have been reduced) ("[In FY 2016], the IRS audited 381,000 recipients of the EITC. That was 36 percent of all audits the IRS conducted, up from 33 percent in 2011, when the budget cuts began.").

116 *See, e.g.*, TREASURY INSPECTOR GEN. FOR TAX ADMIN., NO. 2019-30-063, TRENDS IN COMPLIANCE ACTIVITIES THROUGH FISCAL YEAR 2018, at 15 (Sept. 9, 2019) ("Overall, the number of tax returns claiming the [EITC] have not increased over the past five years. At the same time, the number of examinations conducted by the [Wage & Investment] Division for returns claiming the [EITC] have increased by 17 percent, from 282,665 in FY 2014 to 330,886 in FY 2018."); *see also* George testimony, *supra* note 16, at 10 (noting that the IRS added 290 additional tax examiner positions, that tax examiners were the only position the IRS increased in 2018 and that correspondence examinations were the only types of examinations that the IRS increased in 2018. In contrast, the IRS has decreased the number of revenue agent positions; revenue agents conduct more complex examinations in the field).

117 *See, e.g.*, Paul Kiel & Hannah Fresques, *Where in the U.S. Are You Most Likely to Be Audited by the IRS?*, PROPUBLICA (Apr. 1, 2019), https://projects.propublica.org/graphics/eitc-audit [https://perma.cc/JZ7F-EJLL].

118 Kim M. Bloomquist, *Regional Bias in IRS Audit Selection*, 162 TAX NOTES 987 (Mar. 4, 2019) (discussing regional bias in audits for tax years 2012–2015 and highlighting

The majority of all examinations, and EITC examinations in particular, are correspondence examinations rather than in-person audits.[119] Correspondence examinations, as the name suggests, are conducted through the mail. These examinations are highly automated and are not overseen by one specific employee from start to finish. In other words, the IRS uses an inefficient process to audit low-income taxpayers on an issue with fact-intensive and complex eligibility requirements. These audits are time-consuming to resolve, with the result that refunds of thousands of dollars are often delayed for months or longer.[120] Further, these audits are often burdensome for taxpayers.[121] Yet the IRS has justified this disproportionate focus on EITC claimants, citing resource constraints.[122] At the same time, the IRS has faced criticism for not doing more to pursue high-income individuals who fail to file a tax return, even though pursuing nonfilers is also cost-efficient because of automation and the use of third-party information reporting.[123]

---

that rural Humphreys County, Mississippi, with a median annual household income of just $26,000, had the highest rate of audit intensity, while also noting that the ten most heavily audited counties are all in the rural south and that in 2017 the population of these ten counties was 79% nonwhite (primarily African-American) according to the U.S. Census Bureau).

119 Seventy-one percent of examinations conducted in FY 2017 were correspondence examinations, which is fairly typical. NAT'L TAXPAYER ADVOC., ANNUAL REPORT TO CONGRESS 126 (2018), http://www.TaxpayerAdvocate.irs.gov/2018AnnualReport [https://perma.cc/PWB6-Z3LM]. In the same year, approximately 72% of correspondence exams in the Wage & Income Division were EITC exams. *Id.* at 128.

120 Most EITC exams occur prior to the issuance of the refund, with the result that the refund is frozen and the taxpayer does not receive the EITC until the audit is concluded in the taxpayer's favor. *Id.* at 130, fig.1.8.3. Depending on household composition and income level, these refunds are often thousands of dollars, making them significant relative to the annual earned income of the household; low-income households rely on these refunds as a critical anti-poverty safety net. *See* CONG. RSCH. SERV. REP., THE EARNED INCOME TAX CREDIT (EITC): HOW IT WORKS AND WHO RECEIVES IT, R43805 (Jan. 12, 2021), https://fas.org/sgp/crs/misc/R43805.pdf [https://perma.cc/33EY-LTPX].

121 *Id.* at 133 (citing lower education levels, reliance on tax return preparers, and language barriers as some of the challenges faced by EITC claimants upon audit).

122 Describing how the IRS audits approximately 300,000 EITC returns a year, the agency's website states, "EITC correspondence audits are the most efficient use of available IRS examination resources with the average time to complete the audit of 5 hours per return." I.R.S. Update on Audits (Sept. 24, 2020), https://www.irs.gov/newsroom/irs-update-on-audits [https://perma.cc/WL6P-VLB4].

123 TREASURY INSPECTOR GEN. FOR TAX ADMIN., NO. 2020-30-015, HIGH-INCOME NONFILERS OWING BILLIONS OF DOLLARS ARE NOT BEING WORKED BY THE INTERNAL REVENUE SERVICE (May 29, 2020) [hereinafter TREASURY INSPECTOR REPORT]. As the TIGTA report notes, the intentional failure to file federal income tax returns is a crime. *Id.* at 1. *But see* I.R.S. News Release IR-2020-34 (Feb. 19, 2020) (announcing that revenue officers would increase in-person visits to taxpayers with income of more than $100,000 who did not file returns in 2018 or previous years). IRS Commissioner Charles Rettig

It should be noted that while EITC claimants are disproportionately in the IRS enforcement spotlight, recipients of this social benefit are in many respects perceived to be treated with more dignity than recipients of traditional welfare.[124] Tax scholar Hayes Holderness describes the EITC as "far less privacy-invasive than either TANF or SNAP," as both of those social benefit programs require precertification whereas the EITC does not.[125] Moreover, as Zelenak describes, it is rare for the IRS to make a criminal referral for an individual EITC claimant; individuals who wrongfully claim the EITC usually face only civil sanctions.[126]

3. Differing Policy Implications for the IRS Examination and Collection Functions

The IRS RFI explicitly mentions the agency's interest in using social media research tools for "existing compliance cases" and mentions collections as an end goal.[127] Though it does not explicitly mention the potential use in examinations, it is not implausible that the IRS would consider using such tools to access social media in the context of both examinations and collections.

While social media is a relatively new phenomenon, the IRS has long navigated criticism and limitations on the appropriate balance between taxpayer privacy and tax enforcement, including in examinations. In the early 1990s, the IRS acknowledged it had expanded the use of its "economic reality" investigations; whereas the indirect method technique was previously used only in criminal cases involving unfiled returns, the IRS extended its use of these so-called

---

emphasized this initiative as a priority in testimony before the Senate Finance Committee in June 2020: "We continue working towards the goal of having a presence in every neighborhood, on each type of tax issue and at every level of income, to ensure fairness for all taxpayers." *2020 Filing Season and COVID-19 Recovery: Before the S. Fin. Comm.*, 116th Cong. (June 30, 2020) (Testimony of Charles P. Rettig, Commissioner, Internal Revenue Service), https://www.finance.senate.gov/hearings/2020-filing-season-and-irs-covid-19-recovery [https://perma.cc/T6GR-VS8G].

124 *See generally* SARAH HALPERN-MEEKIN ET AL., IT'S NOT LIKE I'M POOR (2015) (recounting interviews with EITC recipients who speak to their perceptions); *see also* Sara Sternberg Greene, *The Broken Safety Net: A Study of Earned Income Tax Credit Recipients and a Proposal for Repair*, 88 N.Y.U. L. REV. 515 (2013).

125 Hayes Holderness, *Taxing Privacy*, 21 GEO. J. ON POVERTY L. & POL'Y 1, 30 (2013).

126 To the extent that the IRS makes criminal referrals in connection with the EITC, it is most commonly in the context of tax return preparer fraud and promoters of fraudulent schemes, rather than individual claimants. Zelenak, *supra* note 56, at 1891–92. One might analogize return preparer fraud to social benefit trafficking.

127 IRS RFI, *supra* note 2.

lifestyle audits to civil cases.[128] Agents were trained to look for economic signs that taxpayers were living beyond their means, signaling possible unreported income.[129] Tax professionals complained that the audits were arbitrary, blurred the lines between civil examinations and criminal investigations, and involved intrusions into taxpayer privacy.[130] Congress subsequently enacted § 7602(e), which limited the circumstances under which the IRS could use this technique.[131] While § 7602(e) seemingly gave taxpayers a new defense and even an opportunity to invoke a due process right, the statute provides only that the IRS must show it had a "reasonable indication" of a "likelihood" of unreported income. The relatively thin caselaw on § 7602(e) suggests that the IRS has had little trouble in meeting this standard to justify its use of lifestyle audits when challenged by taxpayers.[132] In its internal legal advice interpreting § 7602(e), the Office of Chief Counsel advised IRS revenue agents that they may drive by a taxpayer's house, or may conduct a Lexis search to ascertain if the taxpayer purchased real estate in a year at issue, prior to having a reasonable indication that there is a likelihood of unreported income.[133]

All this raises the question: If the IRS decides to pursue the use of social media in both examinations and collections, should it develop different policies and guidelines for the use of social media by these distinct functions?

---

128 Albert B. Crenshaw, *Tax Cheats Beware: The IRS Will Now Audit Lifestyles*, WASH. POST (Nov. 6, 1994), https://www.washingtonpost.com/archive/business/1994/11/06/tax-cheats-beware-the-irs-will-now-audit-lifestyles/1c220596-4ee3-4ec3-80cb-b06a0e443c32/ [https://perma.cc/T6GR-VS8G].

129 *See, e.g.*, Philip R. Fink & Charles Gibson, *Less Reason to Be Afraid?*, CPA J. (June 1999), http://archives.cpajournal.com/1999/0699/features/f46699.html [https://perma.cc/6NC9-UU2E].

130 *Id.*; Barbara Whitaker, *Spending It; When the I.R.S. Agent Peeks Under the Mattress*, N.Y. TIMES (July 28, 1996), https://www.nytimes.com/1996/07/28/business/spending-it-when-the-irs-agent-peeks-under-the-mattress.html [https://perma.cc/J648-GH74].

131 I.R.C. § 7602(e) ("The Secretary shall not use financial status or economic reality examination techniques to determine the existence of unreported income of any taxpayer unless the Secretary has a reasonable indication that there is a likelihood of such unreported income.").

132 *See, e.g.*, Hsu v. United States, No. 17-cv-06656 NC, 2018 WL 2234439 (N.D. Cal. May 16, 2018); Mortland v. IRS, No. A-03-CA-115-SS, 2003 WL 21791249 (W.D. Tex. June 24, 2003); United States v. Abramson-Schmeiler, No. 09-cr-00359-REB, 2010 WL 11537887 (D. Colo. Oct. 14, 2010); Chapin v. IRS Agent, No. 2:14-cv-538-EJL-REB, 2016 WL 383135 (D. Idaho Jan. 8, 2016).

133 I.R.S. Assoc. Chief Couns. Mem. 200101030 (Oct. 25, 2000) (concluding that these specific practices would not constitute "an intrusion on a taxpayer").

The IRS examination function and the IRS collection function each play a role in enforcement. As there are slight distinctions in their mission, each function's use of social media mining and big data algorithms might have different implications.[134] IRS policy states that, in selecting returns for examination,

> [t]he primary objective . . . is to promote the highest degree of voluntary compliance on the part of taxpayers. This requires the exercise of professional judgment in selecting sufficient returns of all classes of returns in order to assure all taxpayers of equitable consideration, in utilizing available experience and statistics indicating the probability of substantial error, and in making the most efficient use of examination staffing and other resources.[135]

The IRS has a separately stated set of policy considerations for collections, which also emphasizes that "enforcement is a necessary component of a voluntary assessment system."[136] Unlike in the examination context, taxpayers have additional rights and protections in the collections context, some of which are statutory[137] and some of which are a function of IRS policy.[138] For example—and of critical importance to low-income individuals—the IRS cannot pursue forced collections through levy if doing so will create an economic hardship for the taxpayer.[139] In addition to statutory notice and due process requirements, there are additional checks and balances in the collection process. For example, by statute, the IRS cannot seize the taxpayer's principal residence without the approval of a U.S. district court judge or magistrate.[140]

---

134 Recall that the RFI references using social media mining tools only with respect to collections and explicitly mentions that it would limit the use to open cases. *See supra* note 2. I include both examination and collections in this discussion in light of Houser and Sanders' concerns about how the IRS is using its big data database. *See* Houser & Sanders, *supra* note 14, at 870.

135 IRM 1.2.1.5.10 (June 1, 1974).

136 IRM 1.2.1.6.1 (August 18, 1994).

137 See I.R.C. §§ 6300–44, which includes notice and demand requirements and collection due process rights related to the imposition of liens and levies.

138 *See, e.g.*, IRM 5.11.7.2.1.1(2)(e) (Sept. 23, 2016); I.R.S., Dir. of Collection Inventory Delivery and Selection Mem. SBSE-05-1015-0067 (Oct. 7, 2015) (notifying IRS Field Collection agents of a policy decision to exclude social security disability insurance payments from the automated levy program, even though § 6331(h) provides the IRS the statutory authority to levy those benefits).

139 I.R.C. § 6343(a); Treas. Reg. § 301.6343-1(b)(4) (as amended in 2005) (defining economic hardship as a taxpayer being unable to pay reasonable basic living expenses).

140 I.R.C. § 6334(e). Section 6334(a)(13) additionally provides that any real property used as the taxpayer's residence is exempt if the amount of the levy does not exceed $5,000. *See also* Treas. Reg. § 301.6334-1(d).

The IRS Policy Statement on "Fairness and Integrity in Enforcement and Collection" states three primary goals: (1) to ensure fairness to the taxpaying public; (2) to ensure an equitable process for all taxpayers; and (3) to ensure fairness to each taxpayer.[141] The policy further describes how it aims to ensure an equitable process: "[F]airness and integrity are built into the foundation of our enforcement selection processes. These processes operate under a comprehensive set of checks and balances and safeguards to identify the highest potential noncompliance, using scoring mechanisms, data driven algorithms, third party information, whistleblowers and information provided by the taxpayer."[142] We should expect the IRS to pursue collection where necessary to promote compliance, but it must take measures to avoid undue hardship to the taxpayer.[143]

As one way of balancing these enforcement goals with taxpayer rights, Section II.C proposes that the IRS clarify its conception of the taxpayer right to privacy to the public. The agency should be transparent to the public about its use (if any) of social media, so that taxpayers are on notice that the IRS is watching. It is hard, if not impossible, to predict what compliance impact would result from taxpayers knowing that the IRS is monitoring their social media.[144] However, putting taxpayers on notice of this intention affords them dignity.[145]

---

141 I.R.S. Policy Statement 1-236 (Oct. 24, 2016).

142 *Id.*

143 *See, e.g.*, IRM 1.2.1.6.5 (July 10, 1959); IRM 1.2.1.6.14 (Nov. 19, 1980).

144 There is a rich literature on theories of tax compliance. *See, e.g.*, Marjorie E. Kornhauser, *Normative and Cognitive Aspects of Tax Compliance: Literature Review and Recommendations for the IRS Regarding Individual Taxpayers*, *in* NAT'L TAXPAYER ADVOC., 2 ANN. REP. TO CONG. 138 (2007). One theory of tax compliance is economic deterrence, which is the idea that taxpayers who perceive that the IRS is likely to catch tax cheats will be deterred from cheating. However, studies suggest that deterrence is not the strongest driver of tax compliance: other compliance motivations include social norms, tax morale, trust in government, convenience, and reliance on tax preparers. *Id.*

145 Arguably, it also affords taxpayers who engage in noncompliance a warning to cultivate their social media in a way that does not publicly tip off the IRS while continuing to engage in such noncompliance. On the other hand, if everyone on social media cultivates their online image with this in mind, with the effect that no one on social media brags about cheating on their taxes, might this boost tax morale? These questions are worthy of research, but beyond the scope of this Article.

4. Differing Policy Implications for Civil Tax Enforcement and Criminal Tax Enforcement

Just as there ought to be different considerations for examination and collections, there should be different considerations in place for civil proceedings and criminal investigations. As a policy matter, it may be more justifiable for the IRS to engage in social media mining (along with other use of artificial intelligence) to determine whether a criminal act has been committed.[146] The IRS Criminal Investigations unit has far fewer employees than the civil enforcement side,[147] and its smaller workforce has a broader scope that includes not just tax fraud but also money laundering and narcotics-related and counterterrorism-related financial crimes.[148] Don Fort, chief of the IRS Criminal Investigations unit, has spoken publicly about how his office is using "advanced data analytics to spot suspicious behavior," specifically mentioning his office was using data analytics to investigate noncompliance with payroll tax laws.[149] The need for this stems in part from the agency's decrease in staffing.[150] Fort has also made public remarks about unreported capital gains related to cryptocurrencies as an emerging area of focus and said that there are whistleblower cases they are actively working; he cited cryptocurrencies as an area of concern because of the lack of transparency and visibility in those transactions.[151]

---

146 *See generally* Alm et al., *supra* note 104 (discussing ways that technology may both improve and subvert tax compliance, including in the criminal tax context).

147 In fiscal year 2018, examinations and collections had 30,876 full-time equivalent positions. IRS, DATA BOOK 2018 at 67, tbl.30 (2018). In contrast, there were 2,019 special agent positions in the Criminal Investigations unit in fiscal year 2018. IRS, IRS: CRIMINAL INVESTIGATION ANNUAL REPORT 7 (2018), https://www.irs.gov/pub/irs-utl/2018_irs_criminal_investigation_annual_report.pdf [https://perma.cc/GR3W-K5PA].

148 IRS, IRS: CRIMINAL INVESTIGATION ANNUAL REPORT 6 (2018).

149 Kristin Broughton, *Tax Crime Enforcement Unit Relying More on Analytics to Spot Crime*, WALL ST. J. (June 12, 2019, 5:14 PM), https://www.wsj.com/articles/tax-crime-enforcement-unit-relying-more-on-analytics-to-spot-crime-11560363826 [https://perma.cc/JC7V-KHTW].

150 *Id.* (noting that the IRS Inspector General reports the IRS has 26% fewer special agents than it did in 2012); *see also* Michael Cohn, *IRS Criminal Investigation Leveraging More Data Analytics*, ACCT. TODAY (Nov. 14, 2018, 12:29 PM), https://www.accountingtoday.com/news/irs-criminal-investigation-leveraging-more-data-analytics-to-probe-tax-fraud [https://perma.cc/PW5S-B6VU] ("One reason why the division needed to rely so much on data analytics was to make up for the shortage of special agents, while helping IRS agents identify the cases that would have the most impact.").

151 Broughton, *supra* note 149. The IRS Criminal Investigation unit is devoting significant resources to cryptocurrency investigations. *See* Federico & Thompson, *supra* note 99.

Perhaps it is inevitable that the IRS will increasingly utilize artificial intelligence techniques in criminal investigations, and perhaps the public at large will not find the use of such techniques objectionable in this context. If we embrace this as acceptable, where might this ultimately take us? Will the IRS use facial recognition techniques to track where taxpayers are going and to monitor their cash purchases?[152] Where, as a society, do we want this to end? And do we want this technology to be applied to all taxpayers and to all potential tax-related issues, both big and small?[153]

II
PUNISHING THE UNSOPHISTICATED: PONDERING BRAGGADOCIO, WHISTLEBLOWERS, AND THE QUEST TO CLOSE THE TAX GAP

This Article is not meant to deny or undermine the importance of tax compliance or IRS enforcement efforts. The IRS estimates there is a relatively high and steady rate of voluntary tax compliance, most recently estimated at approximately 83.6%.[154] The term "tax gap" refers to the amount of tax *not* paid voluntarily and timely and refers to three distinct types of noncompliance: nonfiling, underreporting, and underpayment.[155] The IRS uses noncompliance estimates and research programs to inform its enforcement strategies. For example, there is a well-established correlation between information reporting and compliance, and there is a well-known compliance gap correlating with the cash economy due to the lack of information reporting. Underlying the goal of reducing the tax gap (as well as underlying the RFI) are

---

152 EUBANKS, *supra* note 30, at 7 (citing the example of Maine Governor Paul LePage having his administration mine data and publicly release information about welfare recipients who withdrew cash from ATMs in smoke shops, liquor stores, and out-of-state locations).

153 According to TIGTA, "[i]n the past, the Internal Revenue Service (IRS) has focused on the tax compliance of high-income individuals because their noncompliance can have a significant corrosive effect on tax administration." TREASURY INSPECTOR REPORT, *supra* note 123, at 1. This is not to argue that the IRS should ignore small indiscretions, but given the agency's high focus on EITC enforcement, it ought to use technology to increase its efforts at reducing high-dollar noncompliance. To see the proposal I set forth for this, see my discussion in Section II.C.5.

154 IRS, PUBLICATION 1415, FEDERAL TAX COMPLIANCE RESEARCH: TAX GAP ESTIMATES FOR TAX YEARS 2011–2013, at 1 (2019). This figure is the voluntary compliance rate, which is a measurement of the gross tax gap; the net compliance rate, which includes amounts that are eventually paid, including through enforcement and collection measures, is a slightly higher figure (85.8% in latest report).

155 *Id.* at 4.

questions about how to most efficiently allocate limited resources in maximizing tax compliance.

For some, it may be easy to shrug off a call to protect the privacy of people who voluntarily make public the intimate (and often mundane) details of their private life. Section II.A addresses that temptation and raises examples of when and why it might be unfair, unwise, or inefficient to incorporate social media mining for tax enforcement. A distinction can and should be made between blatant public admissions of fraudulent behavior, on the one hand, and subtleties perceived by possibly discriminatory algorithms that may lead to significant false positives. As to blatant admissions, Section II.B explores the question of whistleblowers and whether the IRS should expressly encourage third parties to report potential fraud based on social media postings.

This part then concludes in Section II.C with several suggested policy proposals for the IRS, including a call for the IRS to clarify its understanding of a taxpayer's "right to privacy" for the public.

A. The Temptation to Disregard Individual Privacy Concerns

One response to this Article can be couched in the words of the fictional character Forrest Gump: "Momma says stupid is as stupid does."[156] In other words, people may intuitively respond to the IRS RFI with a shoulder shrug: if taxpayers are foolish enough to get caught doing something wrong, why is that necessarily bad? And if they are bragging about illegal behavior publicly on the internet, why do they deserve sympathy or leniency?[157]

As one unsympathetic example of internet braggadocio, consider John McAfee, the British American businessman who founded the McAfee Associates software company. McAfee, a self-described Libertarian who unsuccessfully ran for President in 2016, is a multimillionaire who has publicly stated that he is a nonfiler.[158] I would be surprised if this fact had been previously unknown to the IRS—presumably at least some of his income is subject to third-party

---

156 FORREST GUMP (Paramount Pictures 1994).

157 Note that this dovetails with one of the major critiques of privacy rights: that "those with nothing to hide have no reason to be concerned for privacy." Hatfield, *supra* note 14, at 591 (evoking arguments made by Judge Richard Posner and Catherine MacKinnon). Several people I have spoken to about this Article had that reaction as well.

158 Brooker Crothers, *John McAfee Is Running from U.S. Authorities – and Running for President. On a Boat.*, FOX NEWS (Jan. 24, 2019), https://www.foxnews.com/tech/john-mcafee-is-running-from-u-s-authorities-and-running-for-president-on-a-boat [https://perma.cc/WQ7D-LGQZ].

information reporting,[159] and the IRS would easily determine if no return had been filed in a given year. Of course, it is the height of hubris to brag about this publicly on Twitter, as McAfee did:[160]

> I have not filed a tax return for 8 years. Why? 1: taxation is illegal. 2: I paid tens of millions already and received Jack Shit in services. 3. I'm done making money. I live off of cash from McAfee Inc. My net income is negative. But i [sic] am a prime target for the IRS. Here I am.

According to McAfee, he has told the IRS, "I am not filing a return, I have no intention of doing so, come and find me."[161] Though the IRS has not publicly confirmed this, McAfee claims that in January 2019 the IRS convened a grand jury to charge him, his wife, and four campaign workers "with unspecified IRS crimes."[162]

Another unsympathetic example of such public bluster is Rashia Wilson, the self-declared "First Lady" and "Queen of Tax Fraud."[163] Wilson pleaded guilty to one count of wire fraud and one count of aggravated identity theft in connection with charges that she filed false federal income tax returns using fraudulently obtained social security numbers.[164] According to news reports, Wilson "taunted police by posting photos of herself flashing stacks of cash"[165] and posted inflammatory statements online, including: "*I'M RASHIA, THE QUEEN OF IRS TAX FRAUD . . . I'm a millionaire for the record, so if U think indicting me will B easy it won't, I promise you!"*[166]

---

159 The Internal Revenue Code imposes an information reporting requirement on certain third-party payors. *See* I.R.C. § 6031. The list is voluminous and includes payors of rents, royalties, wages, and sales or redemptions of securities. IRS research analysts have consistently found a relationship between third-party information reporting and tax compliance. *See* IRS, PUBLICATION 1415, *supra* note 154, at 13.

160 John McAfee (@officialmcafee), TWITTER (Jan. 3, 2019, 2:24 PM), https://twitter.com/officialmcafee/status/1080953136985133062?s=21.

161 Crothers, *supra* note 158.

162 *Id.*

163 Press Release, U.S. Att'y's Off., Middle Dist. of Florida, "Queen of Tax Fraud" Resentenced to 21 Years in Prison (Mar. 6, 2015), https://www.justice.gov/usao-mdfl/pr/queen-tax-fraud-resentenced-21-years-prison [https://perma.cc/E3CL-6RBA].

164 Wilson's federal indictment included fifty-seven counts. *See* U.S. v. Wilson, 593 F. App'x 942 (11th Cir. 2014), *aff'd in part, remanded in part*, 649 F. App'x 827 (11th Cir. 2016), *cert. denied*, 137 S. Ct. 1064 (2017).

165 Susan Taylor Martin, *From the 'Tax Fraud Queen' to the $980,000 Refund, Tampa Bay Is a Hotbed of Tax Scammers*, TAMPA BAY TIMES (Feb. 22, 2019), https://www.tampabay.com/business/from-the-tax-fraud-queen-to-the-980000-refund-tampa-bay-is-a-hotbed-of-tax-scammers-20190222/ [https://perma.cc/QXM9-RYPD].

166 Robert W. Wood, *Queen of Tax Fraud Gets 21 Year Prison Term — for the Second Time*, FORBES (Mar. 6, 2015, 1:26 AM), https://www.forbes.com/sites/robertwood/2015/03

Neither McAfee nor Wilson is a low-income taxpayer who engaged in a small amount of cheating or made a small mistake. Wilson was sentenced to twenty-one years in her plea bargain and was ordered to forfeit over $2,000,000 in stolen proceeds.[167] McAfee was indicted in October 2020 for tax evasion and willful failure to file tax returns.[168]

It is understandable that some would take a just deserts approach: the idea that those who (like McAfee and Wilson) post things publicly are inviting scrutiny and deserve what they get. Indeed, Americans seem to enjoy stories of stupid criminals and human folly.[169] These stories proliferate on blogs, in news media, and in books.[170] It stands to reason, therefore, that people may enjoy stories of taxpayers "dumb" enough to tip their tax hand to the IRS on social media.[171] In my view, our government agencies should resist the apparently very human urge to laugh at human misjudgment. Our revenue agency ought to direct its resources toward serious and systemic tax evasion and toward reducing the tax gap.

I do not find McAfee or Wilson to be sympathetic examples either; while both cases involve social media bragging, they run much deeper than that. My privacy concerns do not extend to those who choose to use social media to openly taunt the IRS or encourage the shirking of

---

/06/queen-of-tax-fraud-teasing-i-cant-be-caught-gets-21-years-prison-for-the-second-time/#791bcc0a4d15 [https://perma.cc/PDD5-2ZZY].

167 Press Release, U.S. Att'y's Off., *supra* note 163.

168 Press Release, U.S. Dep't of Just., John McAfee Indicted for Tax Evasion (Oct. 5, 2020), https://www.justice.gov/opa/pr/john-mcafee-indicted-tax-evasion [https://perma.cc/6GWA-AFEB]. McAfee was arrested in Barcelona, Spain, as he was getting ready to board a flight to Istanbul. Following his arrest, McAfee tweeted from prison: "I am charged with tax fraud but my only crime is refusing to file returns - a misdemeanor. Fraud is lying on your tax returns. How could I have lied if I have said nothing?" John McAfee (@officialmcafee), TWITTER (Oct. 10, 2020, 12:00 PM), https://twitter.com/officialmcafee/status/1315004213638897665.

169 *See, e.g.*, DARWIN AWARDS, http://darwinawards.com/rules/ [https://perma.cc/333W-5QK9]. The Darwin Awards is a "humor" site and a community effort published by Wendy Northcutt, who has compiled the stories into a book series titled "The Darwin Awards" (Dutton Books). *Id.* At the time of this writing, there were four books in the series. The Darwin Awards website states, "One should not be ashamed of laughing over the misfortune of others." *Id.*

170 *See, e.g.*, TOM NICK COCOTOS, WEIRD BUT TRUE! STUPID CRIMINALS: 150 BRAINLESS BADDIES BUSTED, PLUS WACKY FACTS (2012); Andy Simmons & Priscilla Torres, *The Fifteen Unluckiest Dumb Criminals Ever*, READER'S DIG. (Sept. 18, 2019), http://www.rd.com/funny-stuff/dumb-criminals-unlucky/ [https://perma.cc/8BES-ZVDJ].

171 Similarly, the state of Washington made an example of the individual who publicly posted an offer to trade marijuana for EBT cards. WASH. ST. DEP'T OF SOC. & HEALTH SERVS., *supra* note 63. All three of these examples (McAfee, Wilson, and the EBT trader) involve criminal acts rather than civil infractions.

tax obligations. The IRS would ignore this behavior at its own peril, as researchers find a strong link between tax compliance and tax morale.[172] If taxpayers view tax evasion taunts on social media and believe that those individuals are "getting away with it," that undermines goals of tax compliance.[173]

Moreover, any criminal investigations of these two individuals likely did not emanate from the internet bragging—rather, the bragging (or taunting) seems to have come after the individuals were under scrutiny by the authorities. My concerns are with much more subtle social media users. For example, ordinary photos scanned by an algorithm might prompt an audit; the algorithm might predict that, based on these photos, an individual earns more money than he or she reported, or that a child does not live in the taxpayer's house for the period required in connection with a particular credit that he or she claimed.

In addition to my concern that the use of social media mining might disproportionately harm low-income taxpayers, I wonder if the agency's choice to engage in social media mining might impact certain personality types of taxpayers more than others. For example, it seems that social media mining would likely locate individuals who engage in bluster, targeting for scrutiny those who are loud, flashy, or indiscreet, even though those individuals' tax compliance may be no better or worse than quiet individuals. Another concern is that it might punish those who are cultivating a false image of themselves online.[174] In a survey of 2000 British social media users, more than 75% of people admitted to lying about themselves on Twitter and Facebook.[175] There is a rich body of social science literature examining how and why

---

[172] *See* Kornhauser, *supra* note 144, at 139 ("Higher tax morale correlates with higher tax compliance."). Kornhauser's article provides an extensive bibliography of tax compliance literature.

[173] Kornhauser notes that "[n]on-compliance among other taxpayers can decrease an individual's own tax morale and compliance." *Id.* at 139–40 (citing Bruno S. Frey & Benno Torgler, *Tax Morale and Conditional Cooperation*, 35 J. COMP. ECON. 136 (2007)).

[174] Houser and Sanders address the problem of potentially false data in their article. *See* Houser & Sanders, *supra* note 14, at 841–42 (citing Minas Michikyan, Jessica Dennis & Kaveri Subrahmanyam, *Can You Guess Who I Am? Real, Ideal, and False Self-Presentation on Facebook Among Emerging Adults*¸ 3 EMERGING ADULTHOOD 55, 60 (2015)).

[175] Lisa Vaas, *Over 75% of People Lie on Social Media*, NAKED SECURITY: SOPHOS (Apr. 7, 2016), https://nakedsecurity.sophos.com/2016/04/07/over-75-of-people-lie-on-social-media/ [https://perma.cc/QB3T-T8EM] (finding men more likely to lie on social media than women, with 43% of men polled admitting to fabricating facts about themselves); *see also* Cortney S. Warren, *How Honest Are People on Social Media*?, PSYCH. TODAY (July 30, 2018), https://www.psychologytoday.com/us/blog/naked-truth/201807/how-honest-are-people-social-media [https://perma.cc/WL8W-KFBC] (describing the same British survey).

people lie online, as well as perceptions of how often other people lie.[176]

This tendency for people to lie or exaggerate surely spans all ages, but there appears to be a generational element to it as well. Social scientists have found that young adults "with a less coherent sense of the self and lower self-esteem reported presenting their false self on Facebook to a greater extent."[177] Whether young or old, people may have a wide variety of incentives and motivations to cultivate a false online image. They may post pictures of someone else's expensive car. In some cases, a photo may not tell the full story. For example, a low-income individual may post photos of a vacation at an expensive resort, which might suggest to the IRS that the individual has significant disposable income—but perhaps this individual's parents paid for the entire trip. Do we want an algorithm to point the IRS in these directions, forcing individual taxpayers to prove that someone else took them someplace expensive and paid their way?

In this regard, it is likely data mining will pick up false hits and minor indiscretions that will direct the IRS down a path that is either negligible (in the case of a low-income taxpayer who has committed a relatively minor tax indiscretion, either intentionally or unintentionally) or useless (in the case of those presenting a false image or those posts that the algorithm misinterprets).[178] Other government agencies that engage in social media investigations have cited this as a downside of using automated tools.[179] Thus, it is foreseeable that the IRS's use of automated mining may necessitate the resource-intensive manual review of many accounts that turn out to be false hits or not worth pursuing; in that regard, it is possible that automation may not be as cost-saving as one would assume. Kimberly Houser and Debra Sanders raised similar concerns about the accuracy of IRS data mining, noting, "big data results are based on correlation, not causation, and it is inappropriate to judge people based on correlation; just because

---

176 *See, e.g.*, Michelle Drouin et al., *Why Do People Lie Online? "Because Everyone Lies on the Internet*," 64 COMPUTS. HUM. BEHAV. 134 (2016) (examining online deception across four different online venues, including social media).

177 Michikyan et al., *supra* note 174, at 55.

178 The IRS RFI mentions this possibility, though does not elaborate on how it would prevent it: "the IRS will also be mindful that frequently information posted on social media and the internet may be wrong or misleading." IRS RFI, *supra* note 2.

179 *See* SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM, *supra* note 58, at 23 ("[O]fficials in one state noted that the automated tools have placed an excessive demand on staff because they had to sift through the many false-positive leads that were generated.").

people share characteristics or interests does not mean that they will have similar tax compliance behavior."[180]

Returning to the example of Predictim, the now-defunct online service that used artificial intelligence screening to create a predictive profile of potential babysitters, computer-generated scans sometimes produce ambiguous results. "When one babysitter's scan was flagged for possible bullying behavior, the unnerved mother who requested it said she couldn't tell whether the software had spotted an old movie quote, song lyric or other phrase as opposed to actual bullying language."[181] Similarly, Facebook has worked to fine-tune its social suicide prediction screening: Mason Marks cites the example of how in its early efforts Facebook picked up false positives from likely benign social media posts such as "Ugh, I have so much homework I just wanna kill myself."[182]

At the same time, the IRS's use of social media data mining presumably would spare those who are quiet—those who are sophisticated enough to maintain online privacy, who know what not to post, those who are so down-and-out that they lack access to the internet, or those who lack the instinct to post about their lives on social media. A sophisticated individual will follow the advice of privacy law scholar Joshua Fairfield, who advises that one way for a device user to protect one's privacy is to "provide false information where possible, to make the algorithms less sure."[183]

I can imagine instances in which an algorithm might also target those who maintain a social media presence but are silent as to certain aspects of their lives. Imagine a taxpayer who has qualifying children she claims for the EITC and child tax credit. What if she maintains an active Facebook page but never posts pictures of her children? This is not a farfetched scenario: many people choose not to post photos of their children due to privacy concerns or simply because their children ask them not to do so. Based on the absence of photos, would an algorithm suggest that the IRS select this taxpayer's return for examination and require substantiation for the qualifying child claims, even if the existing databases (e.g., the Dependent Database) had not prompted it?

---

180 Houser & Sanders, *supra* note 14, at 871.

181 Harwell, *supra* note 71.

182 Marks, *supra* note 25, at 109.

183 Joshua Fairfield, *7 Things I Teach My Kids About Privacy*, MEDIUM (Sept. 9, 2020), https://medium.com/@fairfieldj/7-things-i-teach-my-kids-about-privacy-24372552cde0 [https://perma.cc/5DTP-42T4] (explaining that, as device users, we lack the ability to protect our data but can take certain steps to protect our privacy).

Another concern is the proliferation of fake social media accounts, including for nefarious purposes.[184] There have been publicized cases of criminals impersonating individuals on Facebook in order to scam unsuspecting individuals.[185] Would this affect the social media mining algorithm, leading to time-consuming false positives?

These are but a few suggestions of how social media algorithms might create red herrings for the IRS in many directions, directing scarce resources to dead ends rather than prioritizing human analytical work toward larger dollar cases. Are there other, more effective ways to use social media as a tax compliance tool? Returning to the extreme examples of internet braggadocio, the IRS Whistleblower Program provides an example that might be instructive to draw upon in this regard.

B. Whistleblowers: Should the IRS Encourage Social Media Snitching, and Under What Circumstances?

Recall the story of the woman in Pennsylvania who brazenly posted an offer on Facebook to trade her SNAP card for cash.[186] Social media was her downfall, but she wasn't caught by an algorithm or even by an agency employee conducting a manual search.[187] Something old-fashioned happened: someone snitched on her.[188] A member of the public saw the post, recognized the illegal nature of it, and contacted the agency to report it.[189] This example underscores something about human nature: if people are morally outraged by something, they will speak up. Thus, it is possible that social media will serve as a tool for

---

184 *See* Arun Vishwanath, *Habitual Facebook Use and Its Impact on Getting Deceived on Social Media*, 20 J. COMPUTER-MEDIATED COMM. 83 (2015) (describing how habitual Facebook use may increase the user's vulnerability to phishing attacks on social media sites).

185 *See, e.g.*, Jack Nicas, *Facebook Connected Her to a Tattooed Soldier in Iraq. Or So She Thought*, N.Y. TIMES (July 28, 2019), https://www.nytimes.com/2019/07/28/technology/facebook-military-scam.html [https://perma.cc/UR8E-PVWR] ("[There are] two sides of a fraud that has flourished on Facebook and Instagram, where scammers impersonate real American service members to cheat vulnerable and lonely women out of their money.").

186 Following the tip from a member of the public, investigators arrested Tanya Keenan Mac after she traded her EBT card for heroin. Kristina Papa, *Food Stamp Facebook Post Leads to Another Arrest*, WNEP (Apr. 4, 2017, 5:50 PM), https://www.wnep.com/article/news/local/lycoming-county/food-stamp-facebook-post-leads-to-another-arrest/523-8c2dcca-b352-42bb-9e37-4eafa4fdf6d9 [https://perma.cc/Y49Y-972U].

187 *Id.*

188 *Id.*

189 *Id.*

enforcement whether the IRS chooses to mine it or not. Not every instance of internet braggadocio is as outrageous as the examples of John McAfee and Rashia Wilson or even as overt as that of the woman in Pennsylvania. Most social media leads will be subtler and may be useful only in conjunction with other information known to the viewer.

In his 1996 article suggesting ways to improve public perceptions of the tax system, Joshua Rosenberg proposed ways to encourage and even financially incentivize the public to report tax avoidance to the authorities, arguing that fostering communication (rather than polarization) with the IRS may improve attitudes toward tax compliance.[190] Along those lines, perhaps it might be more appropriate to leave social media monitoring to the public and not have the IRS initiate it. In that framework, the IRS is not doing the frontline social media mining, which eliminates the unwelcome "Big Brother" feeling of the government monitoring your posts.

The IRS already has some mechanisms in place for members of the public to report tax noncompliance. Anyone can report a "suspected tax law violation" on IRS Form 3949-A, which can be submitted anonymously.[191] The form provides a place to report the name of the alleged wrongdoer, and the informant can tick one or more of twenty boxes to describe the alleged violations. These boxes range from very common types of civil noncompliance (failure to file a return, failure to pay tax, EITC, unreported income) to more serious criminal allegations (narcotics income, kickback, organized crime, corruption).

In addition to this information referral form, which anyone can use to report a variety of suspected misconduct, the IRS has a statutory whistleblower program. Internal Revenue Code § 7623, as originally enacted, was an informant claim program authorizing the Secretary of Treasury to pay financial awards as necessary for "(1) detecting underpayments of tax," or "(2) detecting and bringing to trial and punishment persons guilty of violating the internal revenue laws or

---

190 Joshua D. Rosenberg, *The Psychology of Taxes: Why They Drive Us Crazy, and How We Can Make Them Sane*, 16 VA. TAX REV. 155 (1996).

191 IRS, FORM 3949-A, INFORMATION REFERRAL (2016). IRS procedures for screening these forms are described in the Internal Revenue Manual, though parts are redacted. IRM 3.28.2 (Aug. 1, 2020).

conniving at the same."[192] Section 7623(b), added in 2006,[193] created a formalized whistleblower program, providing that a whistleblower shall "receive as an award at least 15 percent but not more than 30 percent of the proceeds collected as a result of the action . . . or from any settlement in response to such action," with the amount of the award determined based upon "the extent to which the individual substantially contributed to such action."[194] The 2006 amendment also mandated the creation of an IRS Whistleblower Office to implement the program.[195]

Under the IRS Whistleblower Program, an award applies only in cases in which (1) an individual taxpayer's gross income exceeds $200,000 in the year at issue; or (2) the proceeds in dispute exceed $2,000,000.[196] Thus, Congress designed the program to incentivize tips or reports of significant evasion or of evasion by taxpayers with significant income.

Notably, the award is decreased in cases "based principally on information disclosed in certain public sources . . . ."[197] This limitation

---

192 I.R.C. § 7623(a). Internal revenue informant laws have been in effect since 1867, but the significant revisions that created the whistleblower program were enacted in 2006. *See* IRS, *History of the Whistleblower/Informant Program* (June 18, 2020), https://www.irs.gov/compliance/history-of-the-whistleblower-informant-program [https://perma.cc/8HF3-HUY2].

193 Tax Relief and Health Care Act of 2006, Pub. L. No. 109-432, div. A, tit. IV, § 406, 120 Stat. 2958.

194 I.R.C. § 7623(b).

195 Tax Relief and Health Care Act of 2006 § 406(b).

196 I.R.C. § 7623(b)(5). The most prominent IRS whistleblower is Bradley Birkenfeld, the UBS banker who divulged information to the IRS about Swiss banking schemes that amounted to criminal tax evasion. David Kocieniewski, *Whistle-Blower Awarded $104 Million by I.R.S.*, N.Y. TIMES (Sept. 11, 2012), https://www.nytimes.com/2012/09/12/business/whistle-blower-awarded-104-million-by-irs.html [https://perma.cc/Q37C-6GAB]. Birkenfeld, himself a subject of the criminal investigation and who served two and a half years in prison for his role in the scheme, made use of the IRS Whistleblower Program and received the largest ever award, $104 million. *Id.* The information he provided to the IRS yielded a lot of fruit: thousands of names of U.S. offshore bank account owners were provided to the IRS, and thousands of other offshore bank account holders voluntarily disclosed their accounts as part of an amnesty program that resulted. *Id.* The IRS estimated that Birkenfeld's information "helped recover more than $5 billion in unpaid taxes."As the article notes, whistleblower awards constitute gross income, so the IRS ultimately receives part of the award back in tax revenue. *Id.*

197 IRS, PUBLICATION 5241, WHISTLEBLOWER PROGRAM FISCAL YEAR 2018 ANNUAL REPORT TO CONGRESS 4 (2019), https://www.irs.gov/pub/irs-prior/p5241--2019.pdf [https://perma.cc/3HSB-N2AE]; *see also* I.R.C. § 7623(b)(2). The award is also decreased when the whistleblower "planned and initiated the actions" that led to the tax law violations. I.R.C. § 7623(b)(3).

is likely to become relevant if a whistleblower's basis for the claim is information he or she saw on a taxpayer's Facebook or Twitter page.

While most tips from social media would be unlikely to meet the criteria of the formalized whistleblower program, the IRS has fixed a general framework for individuals to report noncompliant taxpayers. Instead of pursuing a third-party tool for social media mining, the IRS could simply leave the online snooping to the public, and the agency can follow its existing procedures in pursuing any social media-related tips that are reported on Form 3949-A or whistleblower claims.

C. Proposals for Setting IRS Policies on Social Media Mining: Balancing Modern Enforcement Techniques with a Taxpayer Right to Privacy

1. The IRS Should Clarify Its Understanding of the Taxpayer "Right to Privacy"

As a starting point, the IRS ought to define more clearly its interpretation of a taxpayer's right to privacy. Michael Hatfield's scholarship provides examples illustrating the breadth of personal information that may be tax relevant.[198] Hatfield warned that technological advances, including the use of big data mining, would undo the privacy protection previously afforded to individuals when the IRS faced a structural inability to review all the information available to it.[199]

Notions of privacy are rapidly changing. Perhaps it is not even possible for the IRS to define its conceptualization of taxpayer privacy. That would be a legitimate position—if that is the case, it ought to say so explicitly. In part parroting the statutory language of § 7602(e), the IRS website explanation of the taxpayer right to privacy states the agency "should not seek intrusive and extraneous information about your lifestyle during an audit if there is no reasonable sign that you

---

[198] Hatfield, *supra* note 14, at 631 (referencing the potential tax relevance of sleeping arrangements, marital discord, therapy sessions, and health and social club memberships, among other things); *see also* Michael Hatfield, *Taxation and Surveillance: An Agenda*, 17 YALE J.L. & TECH. 319, 321 (2015) (describing instances of how the IRS is entitled to collect information about individuals' hobbies, reading preferences, religious affiliation, travel plans, weight and doctor's recommendations about it, abortion, sterilization, or gender identity disorder).

[199] Hatfield, *supra* note 14, at 631–32 ("[G]iven how much personal information will be covered by the coming technology and how much personal information is potentially tax relevant, it is hard to have anything but a dystopian vision of this future . . . .").

have unreported income."[200] However, most of what is posted on social media is extraneous to one's income situation. If the IRS is routinely surveilling social media at large (even if by algorithm as opposed to manually), rather than making targeted searches after finding signs of unreported income, then it is seemingly violating its own principle.

2. Increase Transparency of Audit Techniques

Relatedly, if the IRS does not believe that taxpayers have a right to privacy in their social media posts, and if it intends to use automated techniques to trawl all forms of social media for possible enforcement leads, it ought to state that intention clearly and explicitly. At least then the public will be on explicit notice that the IRS is watching their social media. Just as posted signs warn motorists of traffic cameras on roads or notify the public of security cameras at tourist sites and stores, taxpayers should be on notice that the IRS is monitoring their social media activity. Further, the IRS ought also to provide specifics as to its methods: whether the mining is manual or automated; whether the agency is searching indiscriminately or only with cause; whether it is doing so in civil cases or only for criminal investigations; and whether it is doing so in connection with examinations, collections, or both.

This information ought to be prominently displayed on the IRS website. The IRS could undertake a public relations campaign to this effect, using social media as its own tool for spreading the word to taxpayers. If it wishes, it might even openly encourage people to report one another when they see incriminating information on other people's social media. Imagine such a tweet from the IRS: "Do your patriotic duty: retweet suspected tax noncompliance! #TaxGap @IRStaxpros #taxcompliance." If that is how the IRS wishes to operate, it should make that known to the public so that people can proceed accordingly.

3. Limit Social Media Investigations to Manual Searches Rather than Automated, and Define Limits in the Internal Revenue Manual

If the IRS pursues social media mining as part of its enforcement strategy, it will face decision points in setting the contours. A critical first question is to what extent the mining should be done by humans as opposed to by algorithms. If the mining is done by algorithms, a

---

200 *Taxpayer Bill of Rights 7: The Right to Privacy*, IRS (Jan. 22, 2021), https://www.irs.gov/newsroom/taxpayer-bill-of-rights-7-the-right-to-privacy-0 [https://perma.cc/2CH5-KR7D].

second question is whether mining should be limited only to current investigations or used more widely to cast the broadest possible net.

Software programs for data mining produce false positives and are potentially discriminatory. Of course, the same risks are inherent in humans performing manual searches on social media. But humans can play a role in procedural protections, especially if trained in how to conduct searches in a way that minimizes false positives. In the context of whether the Social Security Administration should explore greater use of social media in its investigatory work, Social Security Commissioner Michael J. Astrue told members of Congress that, in his view, professionally trained fraud investigators should be the ones evaluating circumstantial evidence of fraud, not administrative law judges or other employees: "Social media sites are not exactly clear and reliable evidence . . . Facebook puts up phony websites under my name all the time."[201]

Additionally, humans face constraints that computers do not: for one, they have only a limited number of work hours in the week. Humans do not have time to engage in widespread social media mining on a random basis, nor would it be cost efficient for them to do so. Thus, it would be logical to limit employee use of manual searches to the context of existing enforcement cases. This would be most consistent with the limits imposed by § 7602(e), providing that the IRS should not engage in broad fishing expeditions based solely on signs of financial status but can conduct lifestyle audits once the agency finds "a reasonable indication that there is a likelihood of such unreported income."[202]

Authorizing specially trained employees to undertake manual searches of social media in preexisting enforcement cases would be the least harmful alternative. There is a humanity to manuality that is not inherent in automated searches: it opens the door to mercy and

---

[201] Robert Pear, *On Disability and on Facebook? Uncle Sam Wants to Watch What You Post*, N.Y. TIMES (Mar. 10, 2019), https://www.nytimes.com/2019/03/10/us/politics/social-security-disability-trump-facebook.html [https://perma.cc/BM7V-FA9D]. Pear quotes Astrue's remarks in the 2019 article; the remarks were made in 2012 while Astrue was serving as Social Security Commissioner. In his testimony at the hearing, Astrue articulated the possibility that angry ex-spouses may post false information on Facebook. *The Social Security Administration: Is It Meeting Its Responsibilities to Save Taxpayer Dollars and Serve the Public?: S. Hearing 112-751 Hearing Before the Comm. on Fin.*, 112th Cong. (2012) (statement of Hon. Michael J. Astrue, Commissioner, Social Security Administration). He also expressed a concern that "[i]f you allow broad social media access on government time, I think that becomes an enormous suck on productivity." *Id.*

[202] I.R.C. § 7602(e).

discretion in the taxpayer's favor. There is, however, still the risk of employee bias with manual searches. If the IRS were to adopt this technique, it ought to develop policies on when social media investigations are appropriate and what types of evidence might be probative. The IRS can incorporate these policies into the Internal Revenue Manual. Most importantly, these tools ought not to be used to unduly scrutinize poor people.

For example, with respect to collection enforcement, it may be appropriate for an Offer Specialist to manually search social media while verifying the financial statements that were made by the applicant under penalties of perjury. Perhaps an Offer Specialist's findings should weigh adversely only if a material misrepresentation is found and documented in writing in the file, and after the applicant has had a chance to respond to specific questions about the information viewed online. Imagine a manual social media search that appears to uncover an asset of significant value not reported on the Offer in Compromise financial statement: the Offer Specialist should be allowed to make further inquiries and document the findings and the applicant's response as part of the administrative record. For example, if the Specialist sees a photograph of the taxpayer wearing a very expensive wristwatch that was not reported on the asset section of the financial statement, it is reasonable that the Specialist be permitted to ask the taxpayer about this. On the other hand, the Specialist should not be permitted to make value-laden inquiries as to the applicant's expenses. For example, taxpayers submitting an Offer in Compromise are permitted to use a standard expense dollar amount to account for food, clothing, and certain other household items based on the size of the household; the IRS policy is to permit the standard figure without questioning the amount actually spent, and the taxpayer is not required to substantiate the allowable standard figure.[203] Therefore, if the taxpayer has claimed the standard figure, the Offer Specialist should be barred from asking the taxpayer to increase the offer's dollar amount on the basis that the taxpayer has been spotted on social media smoking cigarettes, eating steak, or wearing designer-brand clothes.

---

[203] *See Collection Financial Standards*, IRS (Nov. 19. 2020), https://www.irs.gov/businesses/small-businesses-self-employed/collection-financial-standards [https://perma.cc/3TGE-JS9B].

4. If Automated Social Media Mining Is Used, Implement Use of Pre-Examination Soft Letters to Nudge Taxpayers Detected by the Algorithm

If the IRS proceeds with using social media mining, it should do so as part of an announced compliance campaign. Rather than moving straight to opening examinations based on results, as a first step, the IRS should send selected taxpayers a "soft letter" as a nudge to improve compliance. The idea behind such an initiative is to let taxpayers know that the IRS is undertaking a new enforcement technique or enhancing enforcement of a particular type. The IRS refers to these as "educational letters," and there is precedent for broad use of these letters in targeted areas of suspected noncompliance. In recent years, the IRS has sent soft letters to cryptocurrency holders,[204] offshore account holders,[205] and taxpayers known to have engaged in specific types of transactions that the IRS suspects might be abusive.[206]

The Taxpayer Advocate Service conducted a study in which it sent educational letters to taxpayers whose returns were not selected for examination, but nonetheless appeared to have erroneously claimed the EITC on their 2014 tax return.[207] The study found that the letters were effective in improving compliance the following year in some particular contexts, with taxpayers not making the same mistake the next year.[208] During her time as National Taxpayer Advocate, Nina

---

204 *See, e.g.*, I.R.S. News Release IR-2019-132 (July 26, 2019). Taxpayer Advocate Erin Collins recently criticized the scope of these letters, calling it "disturbing" that these letters imposed "unreasonable burdens on [taxpayers] outside the protection of an examination." NAT'L TAXPAYER ADVOC., OBJECTIVES REPORT TO CONGRESS FISCAL YEAR 2021, at 80 (2020).

205 *See, e.g.*, Kelly Phillips Erb, *IRS to Target S Corporations, Foreign Disclosures in New Campaigns*, FORBES (July 24, 2019, 2:15 PM), https://www.forbes.com/sites/kellyphillipserb/2019/07/24/irs-to-target-s-corporations-foreign-disclosures-in-new-campaigns/#78f1f4313a38 [https://perma.cc/CE98-9U2H].

206 *See, e.g.*, Jay Adkisson, *IRS Sends Second Wave of Soft Letter Warnings to Certain Captive Owners for Abusive Microcaptive Transactions*, FORBES (Aug. 8, 2020, 9:48 PM), https://www.forbes.com/sites/jayadkisson/2020/08/08/irs-sends-second-wave-of-soft-letter-warnings-to-certain-captive-owners-for-abusive-microcaptive-transactions/#7b14cd8713ee [https://perma.cc/6746-857W].

207 *See* NAT'L TAXPAYER ADVOC., STUDY OF SUBSEQUENT FILING BEHAVIOR OF TAXPAYERS WHO CLAIMED EARNED INCOME TAX CREDITS (EITC) APPARENTLY IN ERROR AND WERE SENT AN EDUCATIONAL LETTER FROM THE NATIONAL TAXPAYER ADVOCATE, 2 ANNUAL REPORT TO CONGRESS 32, 33 (2016).

208 *Id.* The study found the educational letters were particularly effective with respect to educating taxpayers on the relationship requirement of the EITC but less effective with respect to taxpayers who claimed a child that was also claimed by another taxpayer. Extrapolating from the study, some types of noncompliance may be more easily corrected by an educational letter than others. *See also* NTA Blog, *EITC – How a Simple Educational*

Olson emphasized that, in order to be salient and effective, IRS letters or notices should be specific in content and tailored to the most relevant issues to the taxpayers.[209] To be most effective, an educational letter in the social media context should address the specific mistake that is suspected, rather than be framed as a general reminder to comply with taxes.

While I do not wish to see the IRS engage in widescale automated social media mining, sending educational letters to taxpayers based upon suspicious findings is a more reasonable first step than immediately opening an examination. The letter should specifically reference social media. Sending such a letter serves the goal of transparency, as it puts the taxpayer on notice that the IRS is surveilling their online activity and, ideally, will nudge the taxpayer to correct his or her behavior.[210]

5. Sharply Define the Social Media Mining Criteria, Using It to Target Only the Most Egregious Noncompliance

I find social media mining in tax enforcement cringeworthy at any income level, and my first preference is to keep the IRS out of this realm. However, if the IRS proceeds with this initiative, my alternative preference is for the agency to set its sights either on the most egregious types of tax noncompliance (regardless of income level) or on the highest earners, who have been the subject of a declining audit rate in the last decade.[211]

Letter Can Help Avert Noncompliance, TAXPAYER ADVOC. SERV. (Feb. 28, 2018), https://www.taxpayeradvocate.irs.gov/news/ntablog-eitc-how-a-simple-educational-letter-can-help-avert-noncompliance/ [https://perma.cc/BGA9-KAVM].

209 NTA Blog, *The IRS Should Redesign Its Notices Using Psychological, Cognitive, and Behavioral Science Insights to Protect Taxpayer Rights, Enhance Taxpayer Understanding, and Reduce Taxpayer Burden*, TAXPAYER ADVOC. SERV. (April 3, 2019), https://www.taxpayeradvocate.irs.gov/news/ntablog-the-irs-should-redesign-its-notices-using-psychological-cognitive-and-behavioral-science-insights-to-protect-taxpayer-rights-enhance-taxpayer-understanding-and-reduce-taxpayer-burden/ [https://perma.cc/W97B-UFFF] (referring to notices in general, not educational letters in particular).

210 As governments in many other countries have done, the IRS has borrowed upon behavioral science, psychology, and cognitive science in connection with its tax compliance research; the IRS can use insights gleaned from its studies to design a social media soft letter and determine which taxpayers should receive it. *See* TAXPAYER ADVOC. SERV., LITERATURE REVIEW: IMPROVING NOTICES USING PSYCHOLOGICAL, COGNITIVE, AND BEHAVIORAL SCIENCE INSIGHTS, 2 ANNUAL REPORT TO CONGRESS 194 (2018).

211 *See, e.g.*, Keith Fogg, *IRS Large Case Examination Rate Collapses*, PROCEDURALLY TAXING (July 13, 2020), https://proceduralytaxing.com/irs-large-case-examination-rate-collapses/ [https://perma.cc/VTL2-ECTD] (citing statistics from IRS 2019 Databook).

For example, could the IRS use social media mining to screen for potential tax protestors? It could set its data mining algorithm to search for social media posts that repeat or promote frivolous tax arguments, such as those compiled by the IRS on its website.[212]

With respect to pursuing wealthy tax cheats, the IRS might wish to look to the examples of state revenue agencies and foreign revenue agencies using high-tech methods in enforcement. The New York State Department of Taxation is well known for using invasive methods (including social media) to track individuals who have ties to New York but claim to reside in lower-tax states on their tax filings.[213] These residency audits are aimed, strategically, at the wealthy as a means of maximizing the state's revenue base.[214] Greece made headlines when it used police helicopters and satellite images from Google Earth to locate home swimming pools as part of a large-scale crackdown on tax evasion and unreported income.[215]

From a cost-benefit perspective, it makes sense to aim these initiatives at the wealthy if the revenue recouped from the positive results will offset the costs of chasing false leads. To some, these initiatives may create "feel-good" stories with the hope that such stories will boost tax morale (and thus boost individual compliance) among the larger public.[216] Personally, I do not like the idea of the IRS tracking any class of individuals' movements electronically—normatively, this is more privacy than I wish for the public to sacrifice in the name of revenue collection[217]—so I do not favor this approach

---

212 *The Truth About Frivolous Tax Arguments*, IRS (May 1, 2020), https://www.irs.gov/privacy-disclosure/the-truth-about-frivolous-tax-arguments-introduction [https://perma.cc/958W-MGGX].

213 *See, e.g.*, Robert Frank, *Tax Collectors Chase Rich New Yorkers Moving to Low-Tax States. Auditors Inspect Cell Records, Even Your Dog's Vet Bills*, CNBC (Mar. 8, 2019, 7:05 AM), https://www.cnbc.com/2019/03/08/tax-collectors-chase-rich-new-yorkers-moving-to-low-tax-states.html [https://perma.cc/2EHE-ECL4].

214 *Id.* ("New York can't afford to lose many millionaires or billionaires. The top 1 percent of earners pays 46 percent of the state's income taxes . . . .").

215 Daniel Steinvorth, *Finding Swimming Pools with Google Earth*: *Greek Government Hauls in Billions in Back Taxes*, SPIEGEL INT'L (Aug. 2, 2010, 2:48 PM), https://www.spiegel.de/international/europe/finding-swimming-pools-with-google-earth-greek-government-hauls-in-billions-in-back-taxes-a-709703.html [https://perma.cc/NCA5-V553] (describing how these tactics revealed that the suburbs of Athens had 16,974 swimming pools, rather than the 324 that had been reported).

216 Studies suggest that taxpayer compliance is directly correlated to perceived compliance of others. *See, e.g.*, Alm et al., *supra* note 104, at 297.

217 Recall that the IRS states that taxpayers have the right to expect enforcement action will be "no more intrusive than necessary." In my opinion, using data mining and technological surveillance to track the personal lives of taxpayers without a specific

even if targeted to the wealthy. But to the extent the IRS wishes to adopt these methods, I prefer targeting tax protestors, or the wealthy, to the idea of training an algorithm to tease out whether a poor person earns a little bit of extra cash on the side or whether a person in a $25 per month installment agreement could afford to pay a slightly higher amount but for the fact that she is smoking a pack of cigarettes a day. Targeting specific groups other than the poor would also serve as a counterweight to the fact that the lowest-income taxpayers are already subject to such a high audit rate. If nothing else, the agency's enforcement efforts would be spread among a larger group of taxpayers (instead of increasing the focus on the poorest).

6. Use Social Media Mining Only at Taxpayer's Request, as a Method of Dispute Resolution

As mentioned in the introduction, the RFI also raises the prospect of using a social media tool to *protect* taxpayers. While I do not favor the IRS searching individual taxpayers' social media in any capacity, I would be curious to see how the IRS might use it to protect taxpayers: trading off taxpayer privacy only for good, rather than for enforcement.[218] Recall the example of the man in Detroit who was wrongfully arrested and could have invoked social media in his alibi—are there similar analogies to be envisioned for taxpayers?[219]

Imagine if taxpayers could turn social media in their favor, electing at their option to use it as a defense or to substantiate their claims in disputes. For example, IRS underreporter notices are sometimes the first clue to taxpayers that they are victims of identity theft; because the notice lists all tax information reported by third parties, the taxpayer will see if income is wrongly reported by an unknown person who is working under the taxpayer's social security number. In those cases, the taxpayer must contact the IRS and establish that the income listed on the notice does not belong to the taxpayer. Perhaps in some cases a taxpayer could use social media posts to demonstrate to the IRS that they had only one place of employment or that they had no connection

---

suspicion of tax noncompliance is far more intrusive than tracking wages and financial transactions, the latter of which are justifiable for a revenue agency.

218 Relatedly, though not specific to social media, see W. Edward Afield, *Moving Tax Disputes Online Without Leaving Taxpayer Rights Behind*, 74 TAX LAW. 1 (2020) (imagining how the IRS can deploy technology to resolve tax disputes in ways that are pro-taxpayer rights).

219 *See supra* note 47 and accompanying text.

to the geographic location where the income was reported under their number.

Perhaps social media could be used (again, I would propose it be allowed only at the taxpayer's election) to substantiate an EITC claim upon examination. The IRS could institute a policy that the agency may consider a taxpayer's social media evidence within its discretion; to protect taxpayers, it could further adopt a policy that no negative inference can be drawn from the social media sources.

Some individuals have turned to technology (and opted to sacrifice a bit of their own privacy) as a method of tax planning: as a response to state residency tax audits, tax-specific compliance tools have become commercially available. Monaeo sells a so-called personal and audit defense system, which consists of an app and web interface that enable users to track and log their days in and out of a state, ensuring that they do not trip into residency status.[220]

In discussing compliance burdens and how cultural norms around technology and privacy have changed and will continue to evolve, Michael Hatfield imagines a future in which taxpayers could choose between two systems depending on their privacy preference.[221] One option Hatfield sets forth would be to voluntarily sacrifice privacy (by consenting to data surveillance) and in exchange receive certain tax benefits; the other option would be to opt out of surveillance and as a result give up the tax benefit.[222] At least such a regime would put the taxpayer in control.

III
BROADER IMPLICATIONS FOR REPRESENTING LOW-INCOME TAXPAYERS IN THE #TMI ERA

In light of the IRS social media request for information, as well as broader trends signaling the loss of individual privacy, how should tax practitioners advise their clients? As the director of a low-income taxpayer clinic, I am most concerned with this vulnerable population of clients who receive our legal services on a pro bono basis.

---

220 Frank, *supra* note 213. The article states that Monaeo said use of its "Personal Edition" app is up fifty-one percent in 2018 over 2017. *See also* MONAEO, https://monaeo.com/personal [https://perma.cc/RL64-9USL].

221 Hatfield, *supra* note 198.

222 *Id.* at 352. Hatfield emphasizes the need for research as to taxpayer preferences, and he recognizes that "the tax law of 2040 should be fundamentally different than that of 2015 if revolutionary technologies are to be integrated into its administration." *Id.* at 366.

Increasingly, I see social media usage addressed in a variety of ways as a continuing legal education (CLE) topic. One such seminar advised lawyers how to use the internet as an investigative tool; the promotional flyer included agenda items such as "[f]ind out 'secret' ways to ferret out information from social media profiles" and suggested social media site navigation as a method to obtain background information about adverse parties, lawyers, judges, and current and potential clients.[223] The CLE flyer suggests other uses for lawyers to navigate social media sites, including to (1) "[F]ind information to attack a party or witness's credibility"; (2) "uncover fraud"; and (3) "seek out the smoking gun."[224]

Other CLE programs include discussion of how the profession's ethical rules apply to social media. For example, may an attorney representing the defendant in a products liability case check the plaintiff's social media sites without the plaintiff's lawyer's consent?[225] C. Simon Davidson of law firm McGuire Woods posed this hypothetical and concluded yes, so long as there is no "communication" with the party or witness.[226] Davidson cautions, however, that some state professional regulations "would prohibit arguably deceptive conduct designed to gain access" to those social media sites; presumably this would include setting up a fictional account to "friend" the party on Facebook or "follow" the party on Twitter.[227]

If lawyers are regularly using social media as a tool for opposition research, what advice are they giving their own clients about how to manage social media without pitfalls? The obvious advice would be for clients to simply go dark: no Facebook, no Twitter, no Instagram. However, that might not be viable advice in the twenty-first century, or clients may not take it seriously. But it does not hurt to remind clients that the government may be mining their social media. I have seen posts by some of my own Facebook friends about how they want to borrow

---

223 Carole A. Levitt & Mark E. Rosch, *Social Media as Investigative Research*, GA. LAWS. CLE, https://georgialawyersclewebinars.ce21.com/item/social-media-investigative-research-evidence-309411#tabDescription [https://perma.cc/78NN-FW37] (coauthors of THE CYBERSLEUTH'S GUIDE TO THE INTERNET (14th ed. 2017)).

224 *Id.*

225 C. SIMON DAVIDSON, THE ETHICS OF EMAIL AND SOCIAL MEDIA: A TOP TEN LIST 302 (2017), https://www.tba.org/sites/default/files/davidson_hypotheticals_and_analysis.pdf [https://perma.cc/QB8A-WCF2] (providing several examples of cases in which a party's or witness's postings on social media sites were a useful source of evidence).

226 *Id.*

227 *Id.*

someone else's child for their tax return, and I have seen a compilation of tweets along the same line.[228] I presumed at least certain of these were jokes, though sometimes it is hard to be sure. Can a data algorithm perceive a joke?

Criminal defense attorneys advise their clients that social media is fair game for police investigators.[229] In the civil context, divorce lawyers routinely advise clients to be careful about what they post on social media, cautioning that content posted can be used for a variety of purposes.[230] Personal injury lawyers have a different set of best practices regarding social media posts depending on whether their client is the plaintiff or defendant.[231] A concern cited by one plaintiffs' attorney firm is the tendency of social media posts to broadcast one's good news and downplay or ignore bad news, with the unintended consequence that "defendants looking to escape liability may point to such photos and posts as evidence that you are not really injured."[232] For this reason, the law firm advises plaintiffs to refrain from social media posts following an injury.[233] Harkening back to the analogy of

---

228 *See* Drumbl, *supra* note 69.

229 Tom Petersen, *If You Are a Defendant in a Criminal Case — Be Careful What You Post on Social Media*, PETERSEN CRIM. DEF. L. (Sept. 7, 2018), https://www.criminaldefensene.com/if-you-are-a-defendant-in-a-criminal-case-be-careful-what-you-post-on-social-media/ [https://perma.cc/XG77-S4CV].

230 *See, e.g.*, Jaliz Maldonado, *Family Law: Social Media Evidence in Divorce Cases*, THE NAT'L L. REV. (Feb. 14, 2019), https://www.natlawreview.com/article/family-law-social-media-evidence-divorce-cases [https://perma.cc/Y2UJ-PFL8]; Larry Upshaw, *Contemplating Divorce? 10 Critical Social Media "Don'ts" You Need to Know*, CONNATSER FAM. L., https://connatserfamilylaw.com/contemplating-divorce-10-critical-social-media-donts-you-need-to-know/ [https://perma.cc/3YWS-332S] (last visited Jan. 24, 2021).

231 *See, e.g.*, Frances Crockett Carpenter et al., *Social Media Admissions in Personal Injury Cases: Mitigating Risk for Plaintiffs, Securing Admissions from Defendants*, STRAFFORD PUBL'NS (May 10, 2017), https://www.straffordpub.com/products/social-media-admissions-in-personal-injury-cases-mitigating-risk-for-plaintiffs-securing-admissions-from-defendants-2017-05-10 [https://perma.cc/6WCP-YZ7K] ("This CLE webinar will provide guidance to personal injury litigators for mitigating the risks that social media posts pose for their clients, as well as tips for tracking down admissions by defendants on social media.").

232 Amalia Lucero, *Social Media Being Used as Evidence in Personal Injury Cases*, CURTIS & CO. ATT'YS, https://www.curtislawfirm.org/articles/social-media-being-used-as-evidence-in-personal-injury-cases/ [https://perma.cc/U9F3-DNAU].

233 *Id.* Similar advice is found on other personal injury firm websites. *See, e.g.*, Adam S. Kutner, *How Social Media Can Impact Your Personal Injury Case*, https://www.askadamskutner.com/personal-injury/social-media-can-impact-personal-injury-case/ [https://perma.cc/U4VK-DFGZ] ("[I]f you're claiming that you have a broken arm, but you post on social media that you're going bowling, the defense is going to challenge your injuries.").

other agencies that administer social benefits, an attorney representing Social Security disability claimants states that he cautions new clients, "There is a little bitty chance that Social Security may be snooping on your Facebook or your Twitter account . . . . You don't want anything on there that shows you out playing Frisbee."[234]

What about in the tax context? Tax attorneys Carina Federico and Travis Thompson observe, "It is imperative that modern tax practitioners develop a full understanding of a client's digital footprint," advising that "[c]lient intake questions should include inquiries about social media usage and online sales through digital marketplaces, at a minimum."[235] Federico and Thompson further suggest "practitioners should advise clients to be mindful about what they post on social media. For instance, a taxpayer should not tell the IRS that they do not have any money, but then post pictures of himself on Instagram with expensive cars or on an extravagant vacation."[236] In the litigation context, tax attorney James Creech advises lawyers to conduct due diligence of a client's social media if the case "relies heavily on the petitioner's credibility on the witness stand" and warns of the ethical consequences that may arise if a lawyer finds contradictory evidence on social media.[237]

Should low-income taxpayer clinics adopt similar routine counseling tactics? Should our clients be counseled differently depending on whether the case involves an examination or a collections issue?

Beyond just the litigation context that Creech discusses, tax attorneys should consider the wide range of their due diligence obligations. Our clients sign financial forms such as a Collection Information Statement or an Offer in Compromise under penalties of perjury. The professional regulations governing practice before the IRS impose upon tax practitioners an affirmative duty to exercise due

---

234 Pear, *supra* note 201.

235 Federico & Thompson, *supra* note 99, at 46.

236 *Id.*

237 Creech, *supra* note 22. Referring to Federal Rule of Evidence 803(3), Creech argues that social media posts can be a useful indicator of mindset: "The low threshold for publication and our cultural habit of oversharing and introspection mean that [social media posts] are probably a fairly accurate indicator of the declarant's mental state." *Id.* While I agree with Creech's advice as to due diligence, it is important to remember that social media posts are not always an accurate depiction of one's life. *See* Houser & Sanders, *supra* note 14, at 841 (citing Minas Michikyan et al., *Can You Guess Who I Am? Real, Ideal, and False Self-Preservation on Facebook Among Emerging Adults*, 3 EMERGING ADULTHOOD 55, 60 (2015)).

diligence when preparing, assisting with, or approving tax returns and other documents relating to tax matters, as well as due diligence in determining the correctness of oral and written representations made by the practitioner.[238] Before submitting such financial forms and statements to the IRS, it would be prudent to also perform online searches of our clients to look for inconsistencies, the way that we might look for inconsistencies in a bank statement that supports such a form. In the bankruptcy context, there are multiple examples of debtors who failed to disclose assets or income and later ran into trouble because of social media posts.[239]

Elaborating on the point made by Federico and Thompson, I can envision a number of similarly problematic tax scenarios, particularly in the collection context. What if social media reveals a side cash business, even one that is relatively low dollar? For our clients, that could have an impact on the "ability to pay" calculation, and it could materially change an Offer in Compromise. Even if the side business is fledgling or operating at a net loss, the failure to disclose it reflects poorly on the taxpayer's honesty elsewhere on the form. Imagine a client's Facebook page posting photos of puppies for sale or advertising to mow lawns or babysit. For low-income taxpayers in collections cases, even one or two hundred dollars a month of unreported income can create issues with collections alternatives, making them ineligible for financial hardship status or forcing a higher minimum payment in an installment agreement. This is an important conversation to have with clients and one that can complicate calculation of monthly income due to the unpredictability of an income stream from such sources. It prompts a broader question as well: Should tax professionals surveil their clients' social media sites looking for any hint of unreported income in connection with preparation of a routine individual income tax return?

Another vulnerable category of taxpayers is those requesting innocent spouse relief. In these cases, a taxpayer who has filed a joint income tax return with his or her spouse in the past is asking for relief from the joint liability, either because the IRS examined the return and

---

238 Treasury Circular No. 230, 31 C.F.R. § 10.22 (2021).

239 *See, e.g.*, Carolyn S. Toto & Kimberly Buffington, *50 Cent Breaks the Golden Rule of Social Media Posting*, PILLSBURY INTERNET & SOC. MEDIA L. BLOG (Feb. 29, 2016), https://www.internetandtechnologylaw.com/50-cent-breaks-the-golden-rule-of-social-media-posting/ [https://perma.cc/55XW-HUD4]; *Debtors Beware: Social Media Knows Where Your Assets Are Buried*, PILLSBURY INTERNET & SOC. MEDIA L. BLOG (Feb. 20, 2018), https://www.internetandtechnologylaw.com/debtors-social-media-assets-bankruptcy/ [https://perma.cc/3ADK-4PTA].

found an understatement of tax or because the return showed a balance due that was not paid.[240] These cases are directed to a centralized unit of the IRS, where an individual makes a determination using a number of factors, including the following: whether the requesting spouse had knowledge, or reason to know, of the understatement of tax when the return was filed; whether the requesting spouse received a significant benefit from the understatement or underpayment; and whether under all the facts and circumstances it would be unfair to hold the requesting spouse liable for the tax owed.[241] When a taxpayer requests innocent spouse relief, the IRS sends a letter and questionnaire to that taxpayer's spouse or ex-spouse (the "nonrequesting spouse") and uses that response to evaluate the requesting spouse's claim.[242] If the requesting spouse appeals the determination in Tax Court, the nonrequesting spouse has a right to intervene in the case.[243] Thus, it would be prudent for a requesting spouse to be particularly careful about what he or she posts to social media—both the IRS and the nonrequesting spouse may be looking at those posts. Of course, if the requesting spouse is in the middle of divorce proceedings, his or her divorce lawyer may already have advised him or her to shut down social media sites. But a significant number of innocent spouse claimants are unrepresented by counsel,[244] particularly low-income claimants, and therefore they are not privy to such advice.

To reiterate, I am not advising tax attorneys to help their clients engage in tax fraud, evasion, or any kind of noncompliance. My concerns are with broader systemic fairness. For example, will the use of social media mining increase the likelihood that IRS employees will make moral judgments of the poor? As Eubanks referenced in her work, we have seen examples in other contexts in which the behavior

---

240 I.R.C. § 6015.

241 *See* I.R.C. § 6015; Rev. Proc. 2013-34, 2013-34 I.R.B. 397; I.R.S. Pub. 971 (Oct. 20, 2014).

242 Treas. Reg. § 1.6015-6(a)(1); *see also* IRM 25.15.3.4 (Dec. 12, 2016) ("The [nonrequesting spouse] must receive notice of, and an opportunity to participate in, any proceeding with respect to an innocent spouse relief request.").

243 *See* King v. Comm'r, 115 T.C. 118 (2000).

244 *See generally* Stephanie Hunter McMahon, *An Empirical Study of Innocent Spouse Relief: Do Courts Implement Congress's Legislative Intent?*, 12 FLA. TAX REV. 629, 668 (2012) (highlighting the high number of pro se petitioners appealing the outcome of their innocent spouse determination in court, but also remarking that "representation does not appear to be a critical matter for determining whether a spouse wins"). Because McMahon's study draws upon data from cases litigated in federal courts, her statistics reflect only requesting spouses who appealed the denial of their request in court, as opposed to the broader universe of all requesting spouses who submit a request. *Id.* at 648.

of poor people is scrutinized, with officials publicly shaming the behavior as part of a broader policy conversation.[245] I can envision a situation in which politicians question the IRS allowance of a standard household expense figure by citing examples of individuals who were granted financial hardship status appearing on social media smoking a cigarette, drinking a six-pack of beer, or sporting a tattoo. The underlying expense of any of those things could unfortunately yet easily become the subject of moral judgment, such as the judgment that the taxpayer could have allocated that money to rent or food.[246]

Regardless of whether the IRS chooses to move forward with social media mining, or whether and how it publicly defines a taxpayer's right to privacy, it seems wise to err on the side of assuming that all electronic transactions, actions outside one's home, internet activity, and social media posts may be subject to various levels of scrutiny and observation.[247] As lawyers, whether one is a tax lawyer, a criminal defense attorney, or a family law specialist, it is prudent to remind our clients of this twenty-first century technological reality.

CONCLUSION

As I stated at the beginning, this Article is not meant as a defense of those who cheat on their taxes. I certainly do not condone faking financial hardship, fudging eligibility for social benefits, or hiding income from the IRS. Tax compliance is a serious problem, and one that deserves serious solutions. The underfunding of the IRS is likewise a serious problem and compels the agency to be creative in its enforcement solutions.

This conversation is yet another reminder that the IRS is tasked by Congress with too many responsibilities in addition to tax administration and revenue collection. The agency is the administrator of refundable tax credits that operate as social benefits. It plays a significant role in oversight of the tax aspects of retirement plans,

---

245 *See, e.g.*, EUBANKS, *supra* note 30 (discussing how Eubanks uses the example of the public shaming of TANF recipients who use ATMs in certain locations).

246 *See generally* Zelenak, *supra* note 56 (discussing how the public views tax cheats versus welfare cheats).

247 *See, e.g.*, Heather Kelly & Rachel Lerman, *America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police*, WASH. POST (June 3, 2020, 4:00 AM), https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/ [https://perma.cc/53ZG-9YKA] (describing law enforcement's use of surveillance cameras, body cameras, and face- and object-recognition software, as well as private citizens' use of smart phones, home security cameras, and vehicle cameras, and describing the metadata contained in these videos and photos).

nonprofit organizations, and healthcare-related provisions. It gets called upon to administer financial aid in times of crisis, as in the COVID-19 pandemic when the IRS was unexpectedly tasked with delivering economic impact payments to millions of individuals, including those with no taxable income or filing requirement. It stands to reason that the agency—overtasked and underfunded—is searching for shortcuts in the name of efficiency.

Despite these pressure points, to which I am sympathetic, I sincerely hope that the agency will choose not go down the road of cheap and easy in relying on big data and social media analytics for collection and examination purposes. The IRS aspires in its mission statement to "enforc[e] the tax law with integrity and fairness to all."[248] In my view, incorporating social media mining as a routine part of examination and collection would undermine the dignity of the taxpayers, as well as the integrity of the agency.

248 I.R.S. Policy Statement 1-236 (Oct. 24, 2016).