Yale Journal of Law & Technology
Volume 28, Symposium Issue

Privacy Paradox in Digital Service Taxation

Zhaoyi Li[*]

As the digital economy expands, tax jurisdictions face increasingly large challenges, as taxable activities like online shopping and advertising frequently extend beyond national borders. This shift has led to the emergence of the European Union's Digital Services Tax ("DST"). While current discussions on this topic focus on the optimal methods and equitable distribution of taxing rights among countries, they overlook user privacy issues inherent in taxes like the DST. In light of the ongoing debate over whether the U.S. should tax digital transactions, this Article examines the legal framework of the DST and explores its implications from a data privacy perspective.

By analyzing the implications of taxing the collection, use, and security of consumer data in the digital economy, this Article illustrates the broader effects of digital taxes on privacy rights and compliance. While the DST offers fiscal benefits, it simultaneously raises significant privacy concerns that must be addressed to safeguard consumer interests in an increasingly data-driven marketplace. To resolve this tension, this Article advances a privacy-centric model for the DST, integrating privacy protection measures directly into the DST's structure and objectives. This comprehensive approach underscores the need for a harmonized framework that balances the economic goals of taxation with the protection of individual privacy, fostering a fairer and more equitable digital ecosystem for all stakeholders.

---

[*] Assistant Professor, Albany Law School. I would like to thank Reuven Aviyonah, Ray Brescia, Assaf Harpaz, Michael Hatfield, Andrew Hayashi, Noah Hertz Marks, Omri Marian, Diane Ring, Blaine Saito, Shayak Sarkar, Darien Shanske, Adam Thimmesch, Rebecca Wolitz, Alex Zhang as well as the participants at Northeastern Junior Scholars Conference, BYU Law Winter Deals Conference, Governing Data Symposium at Yale Law School for their thoughtful suggestions and valuable comments on an earlier draft of this Article. All mistakes are mine.

Article Contents

Introduction

Data capitalism allows companies to transfer intangible assets and earn income across borders, which contradicts the principle of levying taxes on the basis of a company's physical presence.[1] The economic realities of this data-driven era make it difficult to apply traditional source-country tax principles in a manner that captures the income that countries consider generated in their jurisdictions. As intangible investment has ballooned, by the mid-1990s, the U.S. was already allocating more capital to intangibles than to tangibles;[2] it is vitally important to address these taxation difficulties.

In response, many governments have established taxes targeted at digital activities. For example, many leading European countries adopted a Digital Services Tax (DST) for entities that operate web-based platforms.[3] Similarly, Maryland adopted a similar Digital Advertising Gross Revenues Tax.[4] Under this tax, if Amazon earns $1 million from digital ads in Maryland, and its global revenue exceeds $100 million, the company would be taxed at a variable rate of 2.5% to 10%.

However, current discussions on tax policy often overlook the close interconnection between taxes and privacy. For instance, when taxpayers claim healthcare costs for an abortion

---

[1] Omri Marian, *Taxing Data*, 47 BYU L. REV. 511, 531 (2022) ("[H]istorical processes that challenge the traditional model of taxation . . . : globalization, dispersion, and the decline of tangible capital, or 'intangible-ization' of the economy . . . challenges the traditional underpinnings of income tax design: source, ownership, and monetary value . . . can no longer serve as underlying instruments to identify one's 'ability to pay'.").

[2] *Id.* at 540.

[3] Young Ran Kim, *Digital Services Tax: A Cross-Border Variation of the Consumption Tax Debate*, 72 ALA. L. REV. 131, 132 (2020). The origin of DST is the U.K.'s diverted profits tax, in which the U.K. government imposes a higher tax rate on profits that are transferred from the U.K. to other jurisdictions with lower tax rates. For a more in-depth explanation, see Reuven Avi-Yonah, Young Ran Kim & Karen Sam, *A New Framework for Digital Taxation*, 63 HARV. INT'L L.J. 279, 287 (2022); *Investigation into the Digital Services Tax*, NAT'L AUDIT OFF. (Nov. 23, 2022), https://www.nao.org.uk/reports/investigation-into-the-digital-services-tax/?nab=1#downloads [https://perma.cc/DG9W-99XR].

[4] MD. CODE. REG. 03.12.01.02 (2025) (effective Dec. 13, 2021).

on their tax returns, tax authorities may inadvertently gather highly sensitive personal information, including the stage of gestation at which the procedure took place.[5] The U.S. Immigration and Customs Enforcement (ICE) recently began using the Internal Revenue Service's (IRS) sensitive personal data to locate and deport undocumented immigrants, which is likely to result in a decrease in tax returns filed by this targeted group.[6] Despite long-standing yet shockingly lax policies regarding taxpayer data in the U.S., tax privacy has never received much attention from the public, the courts, or even academia.[7] This limited attention may be due, in part, to the general public not knowing (1) how tax authorities share sensitive taxpayer information, nor (2) with whom the information is shared (e.g., other government agencies, or with external parties such as the media). It may also stem from the absence of a high-profile breach, comparable to the globally recognized Cambridge Analytica case,[8] since a well-publicized breach could have spotlighted tax privacy as a serious public issue.

This Article uses the DST as a case study to illustrate the critical role of taxation privacy in safeguarding sensitive personal data.[9] Unlike traditional corporate income taxes,

---

[5] Michael Hatfield, *Privacy in Taxation*, 44 FLA. ST. U. L. REV. 579, 601 (2017).

[6] Olivia Empson, *IRS Nears Deal with Ice to Share Data of Undocumented Immigrants – Report*, GUARDIAN (Mar. 23, 2025, 13:48 EDT), https://www.theguardian.com/us-news/2025/mar/23/irs-ice-deal-share-data-undocumented-immigrants [https://perma.cc/BYU9-SVT7].

[7] For example, early U.S. tax policies permitted tax authorities to disclose taxpayers' names and addresses for the purpose of discouraging tax evasion. Hatfield, *supra* note 5, at 601.

[8] Sam Meredith, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal*, CNBC (Apr. 10, 2018, 7:22 AM), https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html [https://perma.cc/C337-ES8G].

[9] The future of the DST is uncertain. For the most recent updates, *see, e.g.*, Brooks E. Allen et al., *Trump Revives and Expands the Battle Over Digital Services Taxes*, SKADDEN PUBL'N (Feb. 28, 2025), https://www.skadden.com/insights/publications/2025/02/trump-revives-and-expands-the-battle-over-digital-services-taxes [https://perma.cc/23FP-4S4E]; *Defending American Companies and Innovators from Overseas Extortion and Unfair Fines and Penalties*, WHITE HOUSE (Feb. 21, 2025), https://www.whitehouse.gov/presidential-actions/2025/02/defending-

which apply broadly to all corporate revenue, the DST specifically targets economic activities such as data collection and monetization. This focus is especially pertinent to discussions about how tax policies can influence corporate behavior related to privacy. Furthermore, the nature of DST enforcement diverges significantly from conventional tax mechanisms. Unlike traditional tax reporting, where taxpayers actively engage in disclosures, DST-driven data collection is largely passive and automated, with little exercise of taxpayer discretion. This structural shift introduces heightened vulnerabilities, justifying more robust privacy safeguards.

The DST paradox underscores the inherent tension between the tax's intended goals, which are ensuring fair revenue collection and promoting responsible data use, and the unintended risks it poses to user privacy. While designed to correct tax imbalances in the digital economy, the DST's reliance on user data to assess liabilities can inadvertently expose sensitive information to heightened scrutiny and misuse. Thus, although the DST can solve problems related to tax inequities, it can also create new problems that exacerbate privacy erosion if it lacks a well-designed framework. Addressing this paradox requires rethinking the DST not as a static fiscal instrument, but as a dynamic regulatory tool that integrates privacy protection into its core function. Just as taxation serves dual purposes in climate policy by discouraging harmful behaviors while incentivizing positive change, the DST can similarly operate as both a deterrent and an incentive in advancing privacy rights. Accordingly, this Article proposes a reimagined framework in which privacy protection is the central mission of the DST, rather than merely an incidental benefit.

By repositioning the DST as a corrective mechanism for the structural imbalance between data-driven business models and individual privacy rights, the tax becomes more than a revenue-recovery tool. Instead, it directly confronts the systemic harm caused by invasive data practices. Under this approach,

---

american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/ [https://perma.cc/E64Y-N2Z6]; Jacinta Caragher, *Digital Services Taxes: DST Global Tracker*, VAT CALC (Mar. 1, 2025), https://www.vatcalc.com/global/digital-services-taxes-dst-global-tracker/ [https://perma.cc/T6UW-EDL8].

revenue generation serves as a means to support broader privacy initiatives, rather than as the primary goal. Grounding the DST in this regulatory purpose extends its legitimacy beyond fiscal concerns, transforming it into a proactive instrument for mitigating the societal costs of data exploitation.

Part I explores the rationale behind imposing a DST on large technology firms and outlines the methods for effectively taxing these major players in the digital economy. Part II examines the impact of a DST on user privacy, highlighting privacy challenges that arise with its implementation for companies and tax authorities. Part III analyzes the broader implications of redesigning the DST as a privacy-protecting tax and the potential economic and regulatory consequences of such a redesign. Part IV offers a conclusion.

I. What Is the DST?

This Part introduces the basic framework for the DST, the rationale behind its implementation, and how it influences big tech companies.

A. Why Tax Big Tech Companies?

There is no dispute that governments need to collect taxes in order to function, but opinions differ not only on what to tax generally, but also specifically on whether to tax data.[10] Large multinational firms often profit from users in regions where they have limited or no on-the-ground infrastructure.[11] Under traditional tax rules, these companies are taxed where they are based, not where their users are located. This can lead to significant tax revenue losses for market countries. A DST can address this gap by taxing digital products where they are used, regardless of whether the tech company is locally established, thereby promoting fairer global taxation.[12]

By specifically targeting big tech rather than small businesses, a DST furthers a significant purpose of corporate taxation, which is to "counter the concentration of power" in

---

[10] Marian, *supra* note 1, at 520–21.
[11] Cristina Enache, *Digital Taxation Around the World*, TAX FOUND. (Apr. 30, 2024), https://taxfoundation.org/research/all/global/digital-taxation/ [https://perma.cc/E5VC-26GF].
[12] *Id.*

companies.[13] Big tech companies maintain dominance in the digital economy by harnessing massive volumes of user data, enabling them to entrench their market positions.[14] For example, not only can Amazon provide data insights to third-party businesses, but it can also leverage the information from these vendors to refine its own products and secure a competitive edge on the platform.[15] Big tech companies like Amazon leverage the massive amounts of data to generate revenue through targeted advertising, all while obtaining this data at little to no cost.[16]

One problem with this business model is that these companies do not pay the social cost of using this data. For example, the collection and use of personal data may harm user privacy, including by leading to data breaches, unauthorized use of information, and the manipulation of users, yet these consequences are not directly reflected in a company's balance sheet. Thus, companies can use these data practices to generate economic rent even when these practices harm society more than benefit it.[17] Smaller businesses, in contrast, have neither comparable volumes of user data nor the means to exploit it and thus cannot generate similar levels of economic rent or influence market dynamics as significantly.[18] By targeting only the largest tech companies, a DST can help offset the social costs of these approaches by internalizing the resulting negative impacts into the cost structure of the digital

---

[13] Marian, *supra* note 1, at 520 ("Professor Reuven Avi-Yonah explicitly argues that the United States corporate tax was adopted in 1909 partly to counter the concentration of power with corporate managers during the age of corporate consolidation.").

[14] *Id.* at 549.

[15] *Id.* (illustrating the self-perpetuating cycle phenomenon where big tech companies such as Google have incorporated tracking features into most websites). As usage of a search engine increases, the search result accuracy improves, which promotes users to return. *Id.*

[16] Young Ran Kim & Darien Shanske, *State Digital Services Taxes: A Good and Permissible Idea (Despite What You Might Have Heard)*, 98 NOTRE DAME L. REV. 741, 779 (2022).

[17] *Id.*

[18] Adam Hayes, *Economic Rent: Definition, Types, How It Works, and Example*, INVESTOPEDIA (Sep. 1, 2023) https://www.investopedia.com/terms/e/economicrent.asp [https://perma.cc/7KQ2-4YUF].

advertising business,[19] thereby reducing their ability to accrue economic rents and aligning their private interests more closely with public welfare.

Furthermore, by targeting a concentrated group of large multinational corporations, DSTs offer a practical and efficient approach to tax administration. This method substantially decreases administrative complexity, enforcement burdens, and resource expenditures, especially compared to the imposition of similar taxes on a broad base of smaller firms. Monitoring and auditing a limited number of high-revenue entities allows tax authorities to focus on comprehensive and rigorous enforcement efforts where the stakes are highest, ensuring greater compliance with fewer resources. This focused approach not only streamlines tax collection processes but also minimizes the risk of errors and inconsistencies in enforcement, which can be more prevalent when dealing with a large number of small taxpayers with diverse business models.

Some critics may contend that taxing only large tech companies may constitute unlawful discrimination in favor of traditional advertisers, [20] but this critique overlooks the distinction that these two types of companies essentially operate in completely separate markets.[21] Unlike traditional television or print advertising, which offer fixed rates based on ad placement and lack precise audience targeting, data-driven digital advertising platforms like Google or Facebook can personalize ads to specific users, such as recommending red Nike shoes to a user who prefers red. Additionally, they can charge advertisers based on real-time user engagement, like clicks or views, whereas traditional advertising lacks this kind of transparent return on investment. Due to these fundamental differences, firms that offer digital advertising services are not direct competitors with traditional advertising companies. As long as the tax does not place digital businesses at a competitive disadvantage, it cannot be labeled as discrimination.[22]

---

[19] Marian, *supra* note 1, at 520.
[20] Ruth Mason, *Legal Problems with Digital Taxes in the United States and Europe*, *in* EDWARD ELGAR, INTERNATIONAL TAX AT THE CROSSROADS, 265, 265 (2023).
[21] Kim & Shanske, *supra* note 16, 781–82.
[22] *Id.*

In sum, a well-designed DST is an appropriate and effective response to many of the unique economic rents and social costs generated by big tech's data-driven business models. Limiting DST enforcement to large multinational tech corporations enhances legal defensibility and tax policy coherence. Targeting a concentrated group of high-revenue digital firms reduces administrative complexity and focuses enforcement on entities that pose the greatest risks of market distortion and tax avoidance.

B. Defining the Tax Base for Intangible Assets

One of the key considerations in developing a DST is determining how to price the services to be taxed. Pricing tangible assets is often straightforward: the taxable value is the sales price. And when the government thinks an asset is being undervalued in order to evade taxes, the government can instead tax the asset based on its observable market value by referring to comparable sales data. [23] However, such an approach is not optimal for intangible assets like data, algorithms, or user engagement; comparable prices are not only often inaccessible but also highly subjective.[24]

For example, suppose Google develops its algorithm in Country A, but generates advertising revenue from users in Country B. How much of Google's income should be taxed by Country B depends on how much value the algorithm creates in Country B. However, there's no market price for Google's algorithm, and it is difficult to determine how much of Google's income comes from Country B's users versus the value of the algorithm itself. Corporate income tax is typically based on "where value is created". [25] Assigning income across jurisdictions requires determining how much of the profit should be attributed to the algorithm itself, developed in Country A, versus the user base and market activity in Country B. Traditional transfer pricing rules, which rely on comparing transactions, have limited relevance here because the market lacks similar deals for unique intangibles like Google's

---

[23] Marian, *supra* note 1, at 542.
[24] *Id.*
[25] *See generally*, Allison Christians & Laurens van Apeldoorn, *Taxing Income Where Value Is Created*, 22 Fla. Tax Rev. 1 (2018).

algorithm.[26] As a result, governments are forced to engage in complex negotiations and disputes over income allocation, which often lead to double taxation or tax avoidance.

The difficulty in pricing intangible assets and allocating income fairly across borders has given rise to a number of alternative proposals for fairly and accurately establishing the tax base, the most promising of which is a revenue-based tax known as the DST. By allowing each market country to tax gross revenue based on user location, a DST simplifies valuation challenges and provides governments with a more administratively efficient solution.

An important aspect of a well-designed DST is that it is levied on total revenue.[27] Linking the DST to non-manipulable indicators, such as total revenue, not only solidifies the tax base[28] but also increases transparency and ensures that taxes are levied where value is created. For example, a revenue-based DST ensures that these companies contribute to the tax system based on their overall economic activity, even if they offer free services to users, since they still generate revenue through advertising.[29] In contrast, if a DST were imposed on net profits, a multinational corporation could shift income from Country A, where the tax rate is 20%, to Country B, where the tax rate is 5%.

Critics may argue that, compared to only taxing profits, the disadvantage of taxes based on total revenue, like the DST, is that it discourages firms from expanding investments. However, this concern appears less applicable to the vibrant, well-funded big tech companies that dominate the digital economy. As one scholar has pointed out, "[i]f Facebook can earn profits that are nonrival to its operations elsewhere from interacting with a given country's residents, it should not be expected to adjust its activity and investment choices in response to even a 99 percent

---

[26] Francesco Cannas & Edoardo Traversa, *Designing Orthopaedic Boots for a Clay-Footed Giant: Unconventional Fixes for the International Corporate Tax System*, 22 EJOURNAL TAX RSCH. 41, 73 (2024).

[27] Jane Gravelle, *The OECD/G20 Pillar 1 and Digital Services Taxes: A Comparison*, CRS PRODS. (2024), https://www.congress.gov/crs-product/R47988 [https://perma.cc/A6CF-7FDJ].

[28] Avi-Yonah, Kim & Sam, *supra* note 3, at 333.

[29] Kim & Shanske, *supra* note 16, at 764–65.

tax on those profits."[30] In other words, companies capable of tapping into markets with minimal additional expenses are often indifferent to taxes imposed on profits earned in those regions.[31] If returns remain favorable after taxation, there is no incentive to withdraw from or restrict access to those markets.[32] This dynamic suggests that for dominant, well-capitalized digital firms with low marginal costs, the typical drawbacks of taxes based on total revenue, such as deterring investment, are less significant, as these companies are unlikely to scale back operations in response to such levies.

Another concern is potential classification conflicts. A DST is a turnover tax because it is based on "gross revenue."[33] If it were classified as an income tax, a DST might cause double taxation.[34] For example, in the U.S., income tax is calculated based on net income. A DST, however, is calculated based on gross income, so it would not meet the requirements of the U.S. income tax.[35] Therefore, even if a U.S. company pays DST to European tax authorities, it cannot use that amount as a credit against the U.S. income tax.[36] Double taxation is not a concern because, essentially, there are two different tax bases: the DST is levied on gross revenue in the market country, whereas corporate income tax is based on "net income after deducting expenses from gross revenue" in the country of residence.[37]

DSTs also generally avoid a problem common to traditional turnover taxes: cascading taxation. Taxes cascade when they are added at each stage of production,[38] such as when a book moves from paper to printer to bookstore. This cascading tax

---

[30] Dan Shaviro, *Bittker's Pendulum and the Taxation of Multinationals*, 104 TAX NOTES INT'L 535, 546 (2021); Adam B. Thimmesch, *A Future for the State Corporate Income Tax*, 77 TAX L. 761, 792 (2024).
[31] Thimmesch, *supra* note 30, at 793.
[32] *Id.*
[33] Kim, *supra* note 3, at 159.
[34] *Id.* at 166–67 (discussing how various tax bases influence taxes' category).
[35] *Digital Services Taxes (DSTs): Policy and Economic Analysis*, Congressional Research Service, 1, 13 (2019).
[36] Avi-Yonah, Kim & Sam, *supra* note 3, at 282.
[37] Kim, *supra* note 3, at 166–67 (discussing how various tax bases influence taxes' category).
[38] *Tax Pyramiding*, Tax Foundation, https://taxfoundation.org/taxedu/glossary/tax-pyramiding/ [https://perma.cc/QTY6-7AHD].

can reduce economic efficiency and stifle innovation.[39] In contrast, digital service like streaming platforms earn revenue directly from users with minimal extra costs per user.[40] Since there are not multiple stages, and because a DST applies only to the platform's gross revenue, this cascading effect is avoided, thereby reducing the price impact.[41] This advantage, however, does not apply to all digital activities. For example, digital advertising ecosystems could involve multiple intermediaries, including publishers, ad tech platforms, and data brokers, meaning that a DST could indirectly cascade across layers. Similarly, e-commerce platforms and cloud service providers may have more complex value chains or significant infrastructure costs, which could amplify the economic impact of a DST. Therefore, while it minimizes negative cascading effects for direct-to-consumer digital services, a DST's impact can vary across different segments of the digital economy.

As an alternative to a DST, New York is considering implementing a severance tax on big tech companies based on the number of users whose data is collected,[42] but this method raises several difficulties. First, defining a "user" is not straightforward, as individuals may use virtual private networks or share devices.[43] Second, simply multiplying a tax rate by the number of users in a corporation's database ignores the fact that not every user is equally valuable to a corporation. For instance, if user A spends more money per ad impression than user B does, user A's data may be more valuable. Third, basing a tax solely on the number of users results in identical liability for the corporation whether it has collected one piece of data per user or one hundred.[44] Finally, user-based tax rates could cause small businesses to operate in a way that actually negatively affects privacy. Specifically, to minimize tax burdens, they might shift away from directly collecting large volumes of user data and rely instead on inferred connections between individuals and various data points obtained from third-party data brokers. These inferred connections may involve, for

[39] *Id.* at 172.
[40] *Id.*
[41] *Id.*
[42] Kim & Shanske, *supra* note 16, at 799.
[43] Avi-Yonah, Kim & Sam, *supra* note 3, at 339.
[44] *Id.* at 338.

example, using probabilistic matching algorithms to link anonymized purchase histories, browsing behavior, or geolocation patterns to probable user identities. This will make it harder for users and regulators to track the origins and flow of the data, thus rendering regulation more difficult.

One critic argues that a DST should be levied based on data volume in gigabytes,[45] instead of on the number of residents or total worth.[46] This proposal would avoid sensitive data privacy issues, such as tracking an individual user's place of residence. It would also mean that companies that process larger volumes of data and potentially derive greater economic benefit would pay more, making the tax burden more in line with the benefits, and therefore fairer.[47] However, this approach faces limitations as well, since companies may strategically compress or obscure data to minimize their tax liability, creating enforcement and valuation challenges.

Opponents also contend that a DST artificially inflates the tax base by calculating the tax on the gross revenue derived from refined data, instead of basing it on the initial, unprocessed value of that data.[48] The substantial economic value of data in today's digital landscape is often compared to oil,[49] which highlights not only its role as a critical resource in the modern economy but also the significant increase in value that data accrues through refinement and processing. Taxing data solely at its initial stage, therefore, would fail to capture this enhanced value, much like undervaluing oil that has not yet been refined into fuel or other products. Raw data can contain a lot of noise and it requires significant processing to become valuable. If it is not known whether the raw data can be processed successfully, or the specific value that may be generated after processing it, then the raw data may have little market value. Refining raw data requires a significant investment in technology and expertise. Without a clear expectation of the value that could be returned, companies may

---

[45] Reuven Avi-Yonah et al, *A New Framework for Digital Taxation*, 63 Harv. Int'l L.J. 279, 284 (2022).
[46] Marian, *supra* note 1, at 561.
[47] *Id.* at 563; Avi-Yonah, Kim & Sam, *supra* note 3, at 337.
[48] Kim & Shanske, *supra* note 16, at 797.
[49] Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1498 (2020).

be reluctant to invest heavily in raw data, which further reduces their initial market value. Moreover, user-based and data-volume approaches raise practical enforcement concerns, risk behavioral distortions, and may incentivize opaque data sourcing practices. In contrast, DSTs link taxation directly to gross revenue, which is easier for tax authorities to determine and less susceptible to manipulation, thereby reducing administrative burdens and promoting uniformity in global enforcement.

II. Privacy Challenges

This Part discusses the impact of a DST on data privacy from the perspectives of both major technology companies and tax authorities. It explores how a DST could potentially alter the data collection practices of multinational corporations and examines how tax authorities handle sensitive user data, which could affect individual privacy rights.

A. How Does a DST Influence Users' Privacy?

The primary criteria for evaluating the effectiveness of a tax system are efficiency and fairness.[50] Privacy, on the other hand, has traditionally been a peripheral concern in taxation and remains an underexplored topic in this context.[51] However, in today's increasingly data-driven world, threats to personal privacy are now ever-present.[52] Troublingly, although a DST could help solve many of the issues that arise when it comes to taxing big tech, it would also create heightened challenges to taxpayer privacy. For example, a DST would further strain the

---

[50] Hatfield, *supra* note 5, at 583.

[51] For the history of taxpayer privacy, see e.g., George K. Yin, *Preventing Congressional Violations of Taxpayer Privacy*, 69 TAX L. 103 (2015); Alex Zhang, *Fiscal Citizenship and Taxpayer Privacy*, 125 COLUM. L. REV. 235 (2025).

[52] "Data breaches and the digital invasion of privacy seem to have become an inevitable part of daily life. In securing our privacy, we have two formidable tasks: communicating information securely and keeping information secure." Kiran K. Garimella & Daniel Conway, *Zero-Knowledge Proofs and Privacy: A Technical Look at Privacy*, *in* HUMAN PRIVACY IN VIRTUAL AND PHYSICAL WORLDS: MULTIDISCIPLINARY PERSPECTIVES 157, 157 (Mary C. Lacity & Lynda Coon eds., 2024), https://link.springer.com/book/10.1007/978-3-031-51063-2 [https://perma.cc/SSF5-PJD6].

resources of the already underfunded tax authorities that guard taxpayers' data. [53] Particularly, this development would increase the collection, storage, and international exchange of user information, thereby presenting even greater challenges to national tax authorities that are currently facing cuts to their budget and personnel, such as the IRS in the U.S.[54]

The U.K.'s DST provides an illustrative example of how a DST leads to increased data collection. Its DST, which came into force in 2020, levies a "2% tax on the revenues of search engines, social media services and online marketplaces which derive value from UK users."[55] All businesses that offer digital services to U.K. users are required to register with the U.K. government, and to collect data on any of their users that are "normally located or established in the U.K."[56] Such data, which is used to determine whether it is "reasonable to assume"[57] that a user is located in the U.K., includes, but is not limited to, physical addresses where goods are delivered, the user's payment details, and the IP address from which the user

---

[53] Hatfield, *supra* note 5, at 611–12.

[54] *See* Janet Holtzblatt, *Cuts in Spending and Staff Dim Hopes for Transformational Change at the IRS*, TAX POL'Y CTR. – URB. INST. & BROOKINGS INST. (Apr. 2, 2025), https://taxpolicycenter.org/taxvox/cuts-spending-and-staff-dim-hopes-transformational-change-irs [https://perma.cc/KPC3-P6KL].

[55] HM REVENUE & CUSTOMS, POLICY PAPER: DIGITAL SERVICES TAX (Mar. 11, 2020), https://www.gov.uk/government/publications/introduction-of-the-digital-services-tax/digital-services-tax [https://perma.cc/P6KR-V5AK].

[56] HM REVENUE & CUSTOMS, GUIDANCE: CHECK IF YOU NEED TO REGISTER FOR DIGITAL SERVICE TAX (Apr. 1, 2020), https://www.gov.uk/guidance/check-if-you-need-to-register-for-digital-services-tax [https://perma.cc/7ZSB-YNU8].

[57]

> The "reasonable to assume" test is effectively a test of probability. A user will be a UK user when it is more likely than not that they are normally located in the UK. This judgement should be made based on the information available to the group. It will be a reasonable assumption when a reasonably informed and independent person would reach the same conclusion based on that evidence.

HM REVENUE & CUSTOMS, HMRC INTERNAL DIGITAL SERVICES TAX MANUAL: DST32000 - UK USERS (July 31, 2024), https://www.gov.uk/hmrc-internal-manuals/digital-services-tax/dst32000 [https://perma.cc/8DND-SSQ5].

accessed the company's web-based services.[58] In other words, by requiring companies to use various data points to infer a user's probable normal location instead of relying on real-time geolocation at the point of transaction, the U.K. DST may compel even businesses that do not traditionally track users' geographical data to begin doing so.[59] If a user obscures their device's location, the company may then need to identify the device, associate it with the individual user, and deduce their geographic location to comply with DST obligations, further entrenching invasive data collection practices.

---

[58] HM REVENUE & CUSTOMS, HMRC INTERNAL DIGITAL SERVICES TAX MANUAL: DST33000 - EVIDENCE IDENTIFYING A UK USER (July 31, 2024), https://www.gov.uk/hmrc-internal-manuals/digital-services-tax/dst33000 [https://perma.cc/Z737-4M7Z].

> Groups should determine whether a user is normally located or established in the UK based on the information available to them . . . groups should consider the information they hold and use the most appropriate evidence, or mix of evidence, to identify user location.
>
> Some sources of evidence which are commonly collected by providers of DST activities include:
>
> - Delivery address
> - Payment details
> - IP address
> - Intended destination of advertising based on contractual evidence
> - The address of property or location of goods which are rented out
>
> Some groups will collect more than one source of user information. There may be cases where the different data sources provide conflicting evidence regarding user location.
>
> In these cases, the group should consider which evidence is most appropriate, remembering that the test is where the user is normally located, not where they are located at the time of the transaction. In making this determination, the business should consider whether a reasonably informed and objective observer would be likely to conclude that it is probable the user is a UK user.

Id.

[59] HM REVENUE & CUSTOMS, HMRC INTERNAL DIGITAL SERVICES TAX MANUAL: DST56000 - RECORD KEEPING (July 31, 2024), https://www.gov.uk/hmrc-internal-manuals/digital-services-tax/dst56000 [https://perma.cc/R4JL-MZGU].

This approach pushes companies into the business of profiling users' long-term behavior and making probabilistic judgments about personal facts, such as where individuals live, without the users' explicit consent or even awareness. Users making a one-time digital purchase may unknowingly have their location history reconstructed and retained for six years under the U.K.'s DST laws,[60] despite having no reasonable expectation that such intrusive analysis would occur. Requiring companies to collect and store this information amplifies the risk of data breaches, misuse, and unauthorized access. Companies may store user information for longer than six years, which further increases the risk of data leaks. Additionally, due to a potential £3,000 penalty per record-keeping failure,[61] businesses will likely elect to over-collect and over-retain user data. By relying on fragmented and potentially inaccurate indicators to infer personal details and requiring long periods of data retention, the U.K.'s DST framework undermines the General Data Protection Regulation ("GDPR")'s core principle of data minimization [62] and normalizes invasive profiling for routine transactions.

Another downside of the U.K.'s "reasonable to assume" location test is that it grants companies significant discretion and interpretive flexibility, thus increasing the risk of misclassification based on limited, outdated, or inaccurate information. For example, a user who is visiting the U.K. on a short-term basis may be incorrectly categorized as being normally located in the U.K. based on transient data such as IP addresses or recent transactions. This misclassification could lead not only to unnecessary and excessive data collection but also to downstream privacy harms if the user's erroneously constructed profile is subsequently shared with third parties. Such harms include:

---

[60] *Id.*

[61] HM REVENUE & CUSTOMS, HMRC INTERNAL DIGITAL SERVICES TAX MANUAL: DST65500 - FAILURE TO KEEP AND PRESERVE RECORDS (July 31, 2024), https://www.gov.uk/hmrc-internal-manuals/digital-services-tax/dst65500 [https://perma.cc/9FFM-88MF].

[62] *Data Protection Glossary: Data Minimization*, EUR. DATA PROT. SUPERVISOR, https://www.edps.europa.eu/data-protection/data-protection/glossary/d_en [https://perma.cc/TA3G-A5DF].

- Insurance companies adjusting their risk assessments based on the incorrect assumption that the user lives in a jurisdiction with higher healthcare costs and different life expectancy tables than their actual home country, resulting in higher insurance premiums for the user;
- Financial institutions treating the user as a higher compliance risk and thus requiring additional identity verification, documentation, or transaction scrutiny, which can lead to delays in accessing financial services or even denial of services;
- Employers denying job applications when background checks, which often rely on third-party information to verify candidates' profiles,[63] note a discrepancy between the user's claimed residence and third-party data, which could raise unfounded concerns about honesty, stability, or eligibility for certain roles, particularly in highly regulated sectors.

These erroneous denials, elevated costs, and intrusive compliance demands can result in the user suffering considerable mental distress, especially given that they would likely have no knowledge of the underlying profiling error and have few viable options for correcting it, even if they were aware. The U.K. DST's reasonable assumption standard, therefore, magnifies both informational asymmetries and user vulnerability, which fundamentally undermine principles of transparency, data minimization, and autonomy.

Even if a company that charges a DST discloses in its privacy agreement that it must share data with third parties to comply with tax obligations, these privacy agreements are often so extensive and intricate that few users actually read them, and even fewer are prepared to engage in negotiations as if they were contracts.[64] If users do not agree to allow their data to be shared, they may be barred from using the software, [65] as compliance with DST requirements could necessitate such disclosures. This predicament places users in a difficult position, potentially compelling them to choose

---

[63] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 802 (2022).
[64] Marian, *supra* note 1, at 548–49.
[65] *Id.* at 549.

between their privacy and access to digital services.[66] Therefore, it is uncertain whether users genuinely consent to this sharing.[67]

To pay less DST, companies may misidentify users' locations. For example, a European user might be algorithmically classified as residing in the U.S., leading the platform to display promotional offers, advertisements, or pricing schemes that are only valid for U.S. users. Similarly, location manipulation can have regulatory consequences. For example, Japan's dating apps require users to be at least eighteen years old;[68] a sixteen-year-old could falsely set their location to the U.S., potentially bypassing that age restriction. Additionally, since product prices and tax obligations can vary across regions, inaccurate location data may cause consumers to be charged unfairly, paying either more or less than they would have in their actual jurisdiction.

In the field of privacy law, regulations such as the GDPR and various U.S. state privacy laws, including the California Consumer Privacy Act (CCPA), primarily focus on corporate data practices rather than privacy concerns related to taxation. This regulatory gap may allow companies to justify increased data tracking under the guise of tax compliance, further enabling those companies to sell taxpayer data to third parties, using it for targeted advertising, or both. In tax law, many countries, including the U.S., have established safeguards to protect taxpayer privacy to some extent, such as the right to confidentiality under the IRS's Taxpayer Bill of Rights and I.R.C. § 6103.[69] However, this protection was originally designed to secure traditional, fundamental information provided in tax return forms instead of digital data. It does not prevent data exposure during transmission. This highlights a subtle and important distinction: privacy is much broader in

---

[66] *Id.* at 548.

[67] *Id.*

[68] *Age Verify to Chat with Matches*, TINDER, https://www.help.tinder.com/hc/en-us/articles/360041821872-Age-verify-to-chat-with-matches [https://perma.cc/DU9R-S6HJ].

[69] *Taxpayer Bill of Rights 8: The Right to Confidentiality*, I.R.S. (Oct. 15, 2025), https://www.irs.gov/newsroom/taxpayer-bill-of-rights-8 [https://perma.cc/W4N2-X99P]; 26 U.S.C. § 6103.

scope than just confidentiality.[70] Privacy is the right of each person to decide who is permitted to access their personal information, while confidentiality only refers to keeping information secret. Unfortunately, hacking incidents targeting tax system databases occur from time to time.[71] If a hacker breaks into the database of a tax authority and obtains information about where a user's transaction took place, privacy law would be more likely to apply to such an incident, while confidentiality would not, because the tax authority did not actively disclose the information.

What poses an even more serious threat to user privacy is that multinational companies may be required to transfer this data across borders and to share it with tax authorities or auditing offices in multiple jurisdictions. Such cross-border data flows amplify the risks of unauthorized access and potential misuse, particularly when companies implement divergent compliance strategies for user data from different countries due to varying legal requirements.[72] When tax authorities request that DST data be transferred from Europe to a non-European jurisdiction, for example, Europe implements its strict GDPR. Other countries, however, may not have privacy laws as strict as the GDPR, thereby increasing the risk of data breaches. Additionally, to assess DST liability accurately, companies must go beyond identifying the user's jurisdiction; they must also monitor user behavior to determine whether a transaction was completed. This requires excluding those users who are just browsing and those who cancel their orders, further intensifying the scope and intrusiveness of user tracking for DST compliance purposes.

---

[70] Hatfield, *supra* note 5, at 603, 605 ("[T]axpayers' interest in privacy has been equated with the interest in avoiding inappropriate disclosure . . . privacy is considered quite narrowly. It tends to be equated with the right to prevent disclosure."); Adam B. Thimmesch, *Tax Privacy?*, 90 TEMP. L. REV. 375, 380 (2018).

[71] *See, e.g.*, *Massive IRS Data Breach Much Bigger than First Thought*, CBS NEWS (Feb. 29, 2016, 7:00 AM EST), https://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/ [https://perma.cc/AY77-LGEJ]; Thimmesch, *supra* note 70, at 389.

[72] Zhaoyi Li, *Layered Fiduciaries in the Information Age*, 98 IND. L.J. 625, 660 (2023).

B. The Government as the Third Party

Identifying potential third parties is essential in the context of taxation privacy. Because users of online services often do not know of third parties' existence or role, they cannot monitor or control how their personal data is shared and used, nor can they make informed decisions about their data. In this context, third parties are not limited to private entities; they can also include other government agencies beyond the tax authority itself.[73] For instance, the IRS routinely shares data with the Department of Justice.[74] Although immigration authorities are not listed among the recipients, the IRS is now disclosing tax information to Immigration and Customs Enforcement (ICE).[75]

A key component of tax compliance is that taxpayers trust that tax authorities will protect their data. Taxpayers are willing to disclose their tax-related information not only due to the IRS's "special powers of legal compulsion [that] give it a unique ability to acquire information," but also because they trust the government to securely safeguard their data.[76] This trust mirrors the assurance clients place in their lawyers when revealing sensitive case details, believing that their information will be handled with the utmost security.[77]

However, this trust in tax authorities is also fragile. Individuals are already in a vulnerable position compared to institutions.[78] If tax authorities share user information with other departments or third parties without users' consent, the

---

[73] Hatfield, *supra* note 5, at 602.

[74] 26 U.S.C. § 6103; *IRS Privacy Policy*, I.R.S. (Nov. 17, 2025), https://www.irs.gov/privacy-disclosure/irs-privacy-policy [https://perma.cc/4HSM-AR4U].

[75] Kevin Liptak, *IRS Nearing Agreement to Use Its Data to Help ICE Locate Undocumented Migrants*, CNN (Mar. 23, 2025, 1:54 PM EDT), https://www.cnn.com/2025/03/23/politics/irs-ice-data-undocumented-immigrants/index.html [https://perma.cc/8TV9-TMKC] ("Two immigrant rights groups . . . sued . . . IRS . . . ICE and DHS aren't listed as exceptions to the confidentiality rules in the tax code.").

[76] Paul M. Schwartz, *The Future of Tax Privacy*, 61 NAT'L TAX J., 883, 891 (2009).

[77] *Id.*

[78] *Id.*

trust that underpins voluntary compliance will be broken,[79] which will negatively affect tax compliance. Undocumented immigrants in particular, who are already relatively vulnerable, may with good reason be reluctant to report their income, considering that doing so could lead to deportation.[80] But even if the tax agency itself does not intend to violate privacy protection regulations, employees with authorized access to sensitive data can and sometimes do disclose it to the media for financial gain, [81] raising further concerns about the confidentiality of taxpayer data. This could potentially be a massive privacy vulnerability.

The DST was introduced only recently, and many users are unaware that their geolocation data is being shared and analyzed for tax compliance. However, there may be a small, informed group of people who are aware that this is happening. Despite this, it is crucial that companies and tax authorities do not misconstrue any resigned acceptance of privacy intrusions as permission to mishandle sensitive information. The mandatory nature of taxation leaves users with no choice but to provide data to authorities.[82]

---

[79] For other examples of cooperation between the IRS and ICE, see Shayak Sarkar, *Internal Revenue's External Borders*, 112 CAL. L. REV. 1645, 1664 (2024).

[80] Andrew Duehren, *Top I.R.S. Officials Said to Resign After Deal to Give ICE Migrants' Data*, N.Y. TIMES (Apr. 8, 2025), https://www.nytimes.com/2025/04/08/us/politics/irs-ice-tax-data-deal.html [https://perma.cc/2CSZ-JYBK].

[81] *See, e.g.*, Griffin v. Int. Rev. Serv., 730 F. Supp. 3d 1312, 1314 (S.D. Fla. 2024). Taxpayer Kenneth C. Griffin sued the Internal Revenue Service in 2023, claiming that the agency was "responsible for the public disclosure of his confidential tax return information to various media outlets," including the investigative journalism organization ProPublica. *Id.* Upon the 2024 resolution of Griffin's case, the IRS posted a statement on its website, "sincerely apologiz[ing]" to Griffin and "the thousands of other Americans whose personal information was leaked to the press." *IRS Statement As Part of the Resolution of* Kenneth C. Griffin v. IRS*, Case No. 22-cv-24023 (S.D. Fla.)* (June 25, 2024), https://www.irs.gov/newsroom/irs-statement-as-part-of-the-resolution-of-kenneth-c-griffin-v-irs-case-no-22-cv-24023-sd-fla [https://perma.cc/EZ2P-3LNX]. In its statement, the IRS attributed the disclosure to government contractor Charles Littlejohn, while also noting that the agency "takes its responsibilities seriously and acknowledges that it failed to prevent Mr. Littlejohn's criminal conduct and unlawful disclosure of Mr. Griffin's confidential data." *Id.*

[82] Thimmesch, *supra* note 70, at 410–11.

As concerns over privacy deepen, the efforts by tax authorities to ensure compliance with tax laws could inadvertently exacerbate these vulnerabilities. In particular, in an attempt to find companies that evade taxes by exploiting loopholes in the law, these authorities may increase their supervision of online transactions, such as by turning to AI-driven surveillance technologies to track users' transactions and purchasing behavior on Internet platforms. However, this inevitably compromises privacy, as many users prefer to keep sensitive details, such as credit card data,[83] the timing of transactions, and the products purchased, private from both corporations and the government. This potential expansion of government surveillance, although aimed at curbing corporate misconduct, raises a critical question about accountability on the part of the public sector itself. While governments hold companies accountable, the question remains: who holds the government accountable? In the U.S., the IRS Oversight Board has served this type of supervisory role,[84] but it has been inactive since 2015.[85] Other entities, including the Government

---

[83] The U.K. government website provided examples about how to trace U.K. users.

> Example A
> User A lives in the UK and visits Sodor on holiday. She sees an advertisement for a dating app in Elsbridge and decides to take out a subscription while on holiday. User A supplies a UK location to meet people, UK contact details and credit card details. User A is a UK user as it is reasonable to assume they are normally located in the UK. User A also regularly uses a separate app to arrange local journeys, where the app introduces the user to an available transport provider. User A uses this app whilst on holiday in Sodor. The app has a history of previous journeys showing regular and frequent journeys in the UK. The app holds no further details such as payment history. As the only information available to the app links the user to the UK, it is reasonable to assume the user is normally located in the UK.

DST32000 - UK USERS, *supra* note 57.

[84] *IRS Oversight Organizations*, I.R.S. (Sep. 13, 2025), https://www.irs.gov/about-irs/irs-oversight-organizations [https://perma.cc/N7QH-VJ9T].

[85] Jory Heckman, *Senators Look to Restore Long-Neglected IRS 'Board of Directors'*, FED. NEWS NETWORK (July 26, 2018, 5:11 PM), https://federalnewsnetwork.com/agency-oversight/2018/07/senators-look-

Accountability Office, the Office of Management and Budget, and the Treasury Inspector General for Tax Administration, conduct general oversight,[86] yet none focus specifically on privacy. Aside from the IRS's own Chief Privacy Officer, there is no dedicated body responsible for taxpayer privacy. If this trajectory continues, the greatest threats to tax data privacy under the DST may come not from private corporations, but from the public authorities tasked with regulating them. To address this growing concern, tax authorities should establish independent privacy oversight committees, similar to those increasingly adopted by corporate boards, to ensure effective protection of taxpayer data.

Additionally, discovering a privacy violation is only the beginning; the more critical challenges lie in how to sue the government for privacy violations and, ultimately, how to prevail. If tax information is disclosed, a plaintiff can sue the IRS based on 26 U.S.C. § 7431.[87] However, as one Federal District Court's opinion in *Welborn v. IRS* illustrates, it is very difficult to establish "legally cognizable injuries"[88] and to prove a link between an IRS data breach and such injuries.[89] Another downside of litigation is that user data involved in the case may be disclosed to the public as part of the legal process.[90] As a result, individuals may be reluctant to pursue legal remedies, further weakening the accountability mechanisms that are necessary to protect sensitive taxpayer information.

III. Reforms and Considerations

This Part explores the broader implications of DST enforcement for data privacy, highlighting how tax compliance

---

to-restore-long-neglected-irs-board-of-directors/ [https://perma.cc/L6AK-J5PH].

[86] U.S. DEP'T OF THE TREASURY, DEPARTMENT OF THE TREASURY PRIVACY PROGRAM PLAN 9 (2024), https://home.treasury.gov/system/files/236/Department-of-the-Treasury-Privacy-Program-Plan.pdf [https://perma.cc/2YRR-YB5A].

[87] Erickson v. United States, 780 F. Supp. 733, 737 (W.D. Wash. 1990); *see also* 26 U.S.C. § 7431(a)(1).

[88] Welborn v. IRS, 218 F.Supp.3d 64, 77-78 (D.D.C. 2016).

[89] *Id.* at 76–77.

[90] Thimmesch, *supra* note 70, at 388.

obligations blur the boundaries between corporate and individual privacy interests and potential reform.

A. Blurring Boundaries: Corporate vs. Individual Privacy

In its 1950 decision in the case of *U.S. v. Morton Salt Co*., the Supreme Court ruled that businesses, due to their public-facing nature and significant influence on society, should not enjoy the same level of privacy as individuals.[91] Consequently, when regulatory bodies like the Federal Trade Commission (FTC) request information, businesses are expected to promptly comply.[92] The rationale underpinning the Supreme Court's differentiated privacy standard relies on a presumption that corporate information disclosure primarily impacts corporate interests, not individual rights. The DST, however, has made the dynamics of privacy protection more complex. Whereas the legal entity reporting is a corporation, the disclosed content intrinsically pertains to individual privacy rights, rather than corporate financial metrics like profits or costs. Calculating a DST involves gathering sensitive data from each user's digital interactions, including precise locations, behavioral patterns, and usage data, which resembles the type of personal data that typically triggers enhanced constitutional and legal protections when handled by governments or third parties.

The blending of corporate and individual privacy under a DST regime underscores the fact that the Supreme Court's views on corporate records and data, as articulated in *Morton Salt Co.*, are increasingly outmoded in today's digital context. Indeed, the traditional clear-cut distinction between corporate and personal privacy rights may no longer be adequate. When it comes to protecting individual privacy interests embedded within corporate-held data, privacy protections comparable to those directly granted to individuals are not only justified on normative grounds but also necessary to maintain trust in tax authorities and further the core values of data protection laws. If DST data is treated as purely corporate information, it could create a regulatory loophole, allowing governments to obtain

---

[91] United States v. Morton Salt Co., 338 U.S. 632, 652 (1950); Schwartz, *supra* note 76, at 892.

[92] *See, e.g.*, Morton Salt Co., 338 U.S. 632.

sensitive user data through corporate intermediaries without triggering the constitutional and statutory safeguards intended to shield individual privacy. Thus, even if tax authorities require the collection and disclosure of more detailed data pursuant to DST enforcement, companies should not default to automatically submitting that data.

B. Redesigning the DST to Safeguard Privacy

Privacy protection should serve as one of the primary objectives of the DST, rather than being treated as an incidental benefit. This marks a deliberate departure from the traditional framework, which views the DST primarily as a way to recapture lost tax revenue from digital platforms. By recasting the DST as a policy instrument for confronting the structural harms of data exploitation, the tax assumes a dual regulatory function: discouraging invasive data practices and financing systemic privacy safeguards. This shift demands a corresponding reallocation of tax revenues. Instead of subsuming DST proceeds into general funds, legislatures should earmark a significant portion of them for targeted privacy initiatives. In the U.S., these should include expanding the enforcement capacity of agencies such as the Federal Trade Commission, whose current privacy caseload is inadequate relative to the scale of harm; funding the development and adoption of differential privacy,[93] and supporting open-source privacy tools that reduce barriers to responsible data stewardship. Finally, a dedicated compensation fund for users harmed by large-scale data breaches would institutionalize an important and necessary restorative justice mechanism, anchoring the DST in principles of both accountability and equity. Reorienting the DST in this manner not only aligns the tax with evolving public expectations around digital rights but also affirms its legitimacy as a governance tool in the age of data capitalism.

Unlike traditional corporate taxes, which apply uniformly across all revenue types, a DST can be specifically designed to differentiate between business models that prioritize user

[93] *See* Lisa M. Austin & David Lie, *Safe Sharing Sites*, 94 N.Y.U. L. REV. 581, 593 (2019) ("Differential privacy is based on probabilities, so it uses a . . . mechanism to hide the true value of the data to preserve privacy—the introduction of noise or false data.").

privacy and those that profit extensively from data exploitation. A DST can be specifically designed to encourage privacy-friendly practices, rather than merely function as a penalty. A tiered DST rate system that directly correlates with a company's data usage intensity is needed. For instance, the DST could impose a higher tax rate on revenue derived from invasive data practices and targeted advertising, while offering deductions, rebates, credits, exemptions, or lower rates for companies that use anonymized or aggregated data, limit third-party data sharing, categorize users broadly rather than tracking them individually, or adopt opt-in consent models. This would encourage organizations to adopt frameworks like subscription-based platforms that deliver reliable revenue without relying on user data exploitation.

Moreover, an emphasis on user privacy is also conducive to improving a company's enthusiasm for paying taxes.[94] If a DST that incorporates no consideration of tax privacy is implemented, users of digital services may grow increasingly distrustful of the company that offers them. This could negatively affect the revenues of those companies, particularly if users avoid using their products due to concerns about whether the companies will share their data, such as GPS location, with tax authorities.[95] Not only will this decrease in usage negatively impact a company's income, it will also reduce the total amount of tax revenue that the company generates.

The tax should be structured so that companies with repeated privacy violations or data breaches face progressively higher tax rates. This would create a financial deterrent against negligent data handling and incentivize companies to proactively invest in privacy safeguards to avoid higher taxation. By combining rewards and deterrents, regulators can more effectively and proactively safeguard user privacy, as opposed to trusting entirely in corporate goodwill. Tax authorities could also impose additional taxes on companies that transfer personal data outside of specific jurisdictions without complying with local privacy standards. Conversely,

---

[94] Joshua D. Blank, *In Defense of Individual Tax Privacy*, 61 EMORY L.J. 265, 267–68 (2011) ("[I]ndividual taxpayers will comply with the tax system only if they trust that their personal tax information 'stops with the government.'").

[95] *Id.*

companies that voluntarily submit to third-party privacy audits could be eligible for DST rebates. These audits could uncover security gaps, verify adherence to evolving privacy laws, and demonstrate a commitment to responsible data governance, ultimately fostering greater consumer trust while offsetting the costs of maintaining high privacy standards.

By making it more costly to pursue aggressive data monetization strategies and relatively less costly to adopt privacy-preserving alternatives, DSTs can shift the economic calculus for firms. In such a structure, companies that continue with exploitative data practices may face a significant tax burden that erodes profit margins, whereas companies that invest in privacy-preserving measures could improve both their bottom line and public image. When competitors become aware of these incentives and observe the benefits received by others, they are likely to engage in a race to the top in data privacy standards, rather than a race to the bottom. This proposed approach features significant upsides. It transforms the tax from a punitive tool into a proactive instrument that encourages businesses to prioritize privacy, ultimately leading to stronger information management and consumer protection. This targeted design creates financial incentives that may lead companies to rethink how they collect and use personal data, not just because of the tax burden, but because protecting privacy could become a more cost-effective and reputationally valuable strategy.

A tiered DST rate structure would be particularly beneficial for developing countries, where regulatory oversight is often limited. For instance, companies like Meta may engage in location-based targeted advertising by collecting GPS coordinates, IP addresses, and behavioral signals such as visited locations and Wi-Fi networks. While such practices may be technically permissible under the platform's terms of service, user consent is frequently secured through vague pop-up notices. Such consent results in the continuous surveillance of user behavior, generally without the user's awareness. In many jurisdictions in which these data-gathering techniques are used, local regulatory authorities frequently lack the financial resources, technical expertise, or institutional independence necessary to effectively oversee the conduct of large multinational technology firms. Meanwhile, many users have

limited awareness of digital privacy rights. A differentiated DST rate addresses these enforcement gaps by shifting the focus away from the formal validity of user consent, which is often functionally ineffective under traditional privacy regimes, and instead imposing higher tax rates on firms whose business models depend on invasive data practices. By tying tax liability to the degree of data exploitation rather than compliance with procedural formalities, the DST can, through economic pressure, introduce a financial deterrent that serves to align corporate behavior with privacy protection goals. This market-based approach enables countries with limited regulatory capacity to indirectly regulate privacy through fiscal measures, encouraging companies to adopt less intrusive and more privacy-respecting alternatives.

Critics might argue that if a company chooses between two activities, activity A earning $100 with a low tax rate of 5%, and activity B earning $1,000 with a much higher tax rate of 70%, it would still prefer activity B despite the steep tax rate because it remains more profitable overall. However, a tiered DST rate would significantly shrink the profit gap between high and low data-usage practices. For instance, before taxes, activity B (earning $1,000) appears ten times more profitable than activity A (earning $100). After the DST is applied, the profitability gap narrows dramatically: activity B's net profit drops to just $300, while activity A still nets $95. This reduces the profit difference from $900 down to only $205, substantially decreasing the appeal of heavily exploiting personal data. In the end, companies would be compelled to rethink whether the relatively modest gain justifies the compliance burden and reputational risks.

A potential drawback of DST-like taxes is that they could inadvertently incentivize companies to be more aggressive in tracking users and collecting their personal data. Furthermore, companies could use the guise of compliance to justify this increased collection. To counteract this drawback, DST regulations should be designed to require businesses to collect strictly the data necessary to determine user jurisdiction. Rather than mandating the retention of multiple indicators, including granular IP data, billing addresses, GPS coordinates, or login patterns, regulators should authorize reliance on just one or two prescribed data points, such as billing country or

country-level IP addresses. Additionally, standards like the U.K.'s reasonable inference methods should be replaced with a procedural safe harbor similar to the corporate law's good faith doctrine. Under this approach, as long as companies follow the designated procedures in good faith when determining user location, they would be shielded from penalties even if some users are later found to have submitted inaccurate or misleading information. This framework removes any basis for companies' excuses to over-collect, cross-reference, or retain sensitive personal data indefinitely, thereby decoupling tax compliance from invasive surveillance practices.

Minimizing data collection also makes enforcement by tax authorities more efficient and less privacy invasive. Rather than auditing extensive user-level datasets, authorities would simply verify procedural compliance to determine whether the company adhered to approved methods for identifying jurisdiction. Although this model will bring a certain margin of error, the privacy gains outweigh the costs of imprecision. Permitting a degree of error is a deliberate trade-off that protects individual privacy while maintaining tax enforceability. It reflects a shift in regulatory philosophy: rather than extracting maximum informational accuracy at the expense of user privacy, the main concern is to safeguard personal data through procedural accountability.

Ensuring transparency is vital throughout this process.[96] Just as the SEC mandates public companies to disclose information to maintain market integrity,tax authorities should require firms subject to a DST to publish key details on their websites. These disclosures should include how user data, such as geolocation, is collected, where it is stored, which internal departments or third-party entities have access to it, whether it is monetized, which foreign tax authorities receive it, and for what purposes.

Commentators may suggest that making corporate tax forms public can prevent tax evasion and enhance economic

[96] The U.K. HM Revenue & Customs demonstrate a strong tendency towards transparency since their DST specialists consistently provide prompt and helpful responses to email inquiries regarding the DST.

efficiency,[97] but the benefits of line-by-line disclosure are muted for DSTs. Whereas traditional corporate income taxes are shaped by complex internal deductions and cost structures, a DST targets only gross revenues tied to user locations and activities, making the tax base far simpler and more externally verifiable. Thus, while disclosure of aggregate DST payments per jurisdiction may be warranted, neither line-by-line disclosures of how each transaction is taxed, nor the exposure of user-level data such as personally identifiable information (PII), such as usernames, IP addresses, device identifiers, or behavioral data traceable to specific individuals, would be necessary. Additionally, requiring excessive transparency significantly raises the likelihood of privacy violations. A transparency regime should therefore aim to strike a careful balance: not only should it require disclosure of institutional procedures and total tax contributions, but it should also strictly protect individual privacy and avoid disclosures that serve little regulatory purpose.

If Company A can observe how Company B complies with these minimally invasive DST reporting requirements and sees that B earns public trust as a result, Company A has an incentive to adopt similar practices. Conversely, if Company B suffers penalties or reputational damage due to weak compliance or lax privacy safeguards, Company A can take corrective steps to avoid replicating those failures.[98] In this way, transparency fosters regulatory learning and incentivizes privacy-conscious innovation across the industry. Ultimately, the goal is not to burden firms arbitrarily, but to use tax transparency as a mechanism for privacy-enhancing regulation. When users have information about how their data is secured, where it travels, and who controls it, they can make autonomous, informed decisions about which services to use. Just as investors use 10-K disclosures to assess financial risk and corporate integrity, digital citizens should be empowered

---

[97] Joshua D. Blank, *Reconsidering Corporate Tax Privacy*, 11 N.Y.U. J.L. & BUS. 31, 87 (2014).

[98] Blank, *supra* note 94, at 287–89 ("[H]ow would taxpayers comply with the tax system if they could see *other* taxpayer's tax returns . . . specific examples of tax enforcement are likely to influence individuals' perceptions of certain elements of the tax system, which, in turn, may affect their decisions to comply with the tax law").

to evaluate technological risk and data ethics through comparable transparency standards.

Security measures surrounding DST-related data handling should also form a critical component of corporate disclosure. This includes technical safeguards such as encryption protocols for data, access controls specifying who within the organization or external vendors can retrieve location-related data, data minimization policies that limit the duration and scope of storage, and audit logs that track internal and external access to sensitive datasets. Companies should also disclose whether they implement privacy-by-design frameworks and maintain breach notification procedures aligned with GDPR or CCPA. By normalizing the disclosure of security infrastructure as part of the DST compliance, policymakers can set industry-wide standards that raise the floor for privacy protection across the digital economy. This approach moves beyond mere revenue collection and reconceives the DST as a regulatory lever. While implementing these security measures undoubtedly entails costs such as investment in cybersecurity personnel, compliance software, and legal oversight, these costs could be partially offset by lowering DST rates for firms that demonstrate robust privacy and security protocols. In doing so, the tax system would actively reward firms for reducing privacy risks.

Conclusion

The design process for taxes regulating digital activities should avoid triggering privacy invasions or introducing new or heightened data privacy risks. This Article does not call for the abolition of the DST, but instead underscores the broader implications of data-driven taxation amid rapid advancements in AI and data science. Even if the DST were eliminated, the growing reliance on digital infrastructure guarantees that data-related taxation will remain a critical issue. As tax filing becomes increasingly digital, concerns over data transmission, security, and privacy will only intensify. Navigating these challenges is vital for building a responsible and transparent data ecosystem.