Tax Data, Immigration Enforcement, and the Privacy of Voluntary Compliance: The IRS–ICE Data-Sharing Controversy and Its Comparative Implications Across Five Common Law Jurisdictions- 2026

Oghenehoro Evi Eni*

Independent Immigration & Business Law Scholar

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.1014MG0131

Received: 03 June 2026; Accepted: 08 June 2026; Published: 29 June 2026

ABSTRACT

In early 2026, the United States government entered into a data-sharing arrangement between the Internal Revenue Service (IRS) and Immigration and Customs Enforcement (ICE) that would permit immigration authorities to access federal tax return information for the purpose of locating undocumented immigrants. In March 2026, the United States Court of Appeals for the District of Columbia Circuit was urged to maintain a district court injunction blocking the arrangement in *Center for Taxpayer Rights et al., v. IRS et al.*, No. 26-5006. This article provides the first comprehensive legal and comparative analysis of the IRS–ICE arrangement. It examines the statutory framework governing taxpayer confidentiality under §6103 of the Internal Revenue Code, evaluates the agreement's compatibility with the United States' voluntary tax compliance architecture, and analyzes its constitutional implications under the First, Fourth, and Fifth Amendments. The paper further situates the controversy within a comparative framework by examining how Canada, Australia, New Zealand, and the United Kingdom have approached and uniformly rejected the use of tax authority data for immigration enforcement purposes. The article argues that the use of tax return data for immigration enforcement undermines the legal and institutional foundations of voluntary compliance, imposes substantial and under-acknowledged fiscal costs, and raises rule-of-law concerns that extend far beyond immigration policy. By eroding the confidentiality compact between the state and taxpayers, the IRS–ICE arrangement threatens the integrity of the tax system itself.

Keywords: Taxpayer Confidentiality; Internal Revenue Code §6103; IRS–ICE Data Sharing; Voluntary Tax Compliance; Immigration Enforcement

INTRODUCTION

The United States tax system works effectively because people choose to cooperate with it. Unlike systems where the government calculates every individual's tax bill, the U.S. relies on taxpayers to report their own income, claim deductions, and submit accurate returns each year. The Internal Revenue Service (IRS) checks only a small percentage of the more than 160 million individual tax returns filed annually, yet overall compliance remains high, somewhat above 80 percent (National Taxpayer Advocate 2026).

This high level of compliance is not accidental. It exists because most taxpayers believe that the information they provide to the IRS will be used only to assess and collect taxes, not for unrelated government enforcement purposes. In other words, people comply because they trust the system.

That trust forms what can be described as a confidentiality compact between taxpayers and the government. Under this compact, individuals are legally required to disclose sensitive personal and financial information such as income sources, home addresses, employers, and family details and the government, in return, promises to

protect that information from misuse. Without this assurance, voluntary compliance would collapse, because rational taxpayers would not be willing to disclose information that could later be used against them.

However, congress formally recognized this reality in 1976 when it enacted Section 6103 of the Internal Revenue Code. This provision makes taxpayer confidentiality the default rule and allows disclosure only in fairly defined circumstances expressly approved by Congress (IRC §6103). The law was a direct response to historical abuses, including the use of tax records for political and law-enforcement purposes during the Watergate era. Since then, Section 6103 has functioned as a structural safeguard for the tax system, not as a privacy rule, but a primary means of sustaining compliance and revenue collection.

In addition, the IRS–ICE data-sharing arrangement announced in early 2026 challenges this compact at its foundation. Under the arrangement, immigration enforcement authorities would gain access to tax return information, especially data associated with Individual Taxpayer Identification Numbers (ITINs) to help locate undocumented immigrants. This development prompted litigation in *Center for Taxpayer Rights et al., v. IRS et al.*, where a federal district court blocked the policy and the DC Circuit was asked to decide whether that block should remain in place (Center for Taxpayer Rights 2026).

The controversy goes beyond immigration policy. The central issue is whether the government can promise confidentiality to encourage tax compliance, and then later repurpose that same information for enforcement actions unrelated to tax law. If taxpayers begin to believe that filing a return could expose them to deportation or any other unrelated sanction, the incentive to comply disappears.

This risk is not theoretical. Approximately 4.4 million undocumented immigrants currently file U.S. tax returns using ITINs, contributing between $11 billion and $13 billion annually in federal income and payroll taxes (Tax Policy Center 2026). These individuals file precisely because the law and the IRS itself has consistently communicated that tax compliance does not trigger immigration enforcement. Breaking that understanding threatens to reduce filings, lower revenue, and weaken the tax system as a whole.

Furthermore, a tax system based on voluntary compliance cannot survive if compliance becomes dangerous. When the government uses tax data as an enforcement weapon outside the tax context, it undermines the very trust that makes the system work. The IRS–ICE arrangement therefore raises questions not only about statutory interpretation, but about the long-term stability of voluntary taxation and the rule of law itself.

The Statutory Framework

Why §6103 Exists

Section 6103 of the Internal Revenue Code is the backbone of taxpayer confidentiality in the United States. It exists for a practical reason: the federal tax system depends on people being honest about their finances. To make that honesty possible, Congress made a clear legal promise information given to the IRS for tax purposes would remain confidential unless Congress itself explicitly allowed otherwise.

Before 1976, this promise did not exist in a meaningful way. Tax information could be shared relatively freely within the executive branch, and historical investigations later revealed that tax records had been used for political targeting and law-enforcement leverage. In response, Congress fundamentally reversed the default rule. Instead of disclosure being allowed unless prohibited, §6103 made confidentiality the rule and disclosure the exception (National Taxpayer Advocate 2026).

This shift is important. Section 6103 is not a narrow privacy statute. It is a structural feature of the tax system designed to preserve voluntary compliance.

The Default Rule

Section 6103(a) states that tax "returns and return information shall be confidential" and may not be disclosed by federal employees except as authorized by statute (IRC §6103(a)). The definition of

"return information" is intentionally broad. It includes:

i. a taxpayer's name and address

ii. income sources and amounts

iii. employer information

iv. tax identification numbers, including ITINs

v. dependent and household data

vi. any information collected by the IRS related to tax liability

This depth matters because immigration enforcement relies on this type of information. Addresses, employer names, and identification numbers are among the most valuable tools for locating individuals. Congress knew this when it drafted §6103 and deliberately placed this information behind a strong confidentiality barrier.

Moreso, if information comes from a tax return or is connected to tax administration, it is protected unless Congress has said otherwise.

The Exceptions

Section 6103 does allow disclosure in limited circumstances, but these exceptions are highly constrained. They are not general permissions; they are carefully designed carve-outs with procedural safeguards.

Three exceptions are most relevant to the IRS–ICE controversy, including:

Disclosure to State Tax Authorities (§6103(d))

This provision allows the IRS to share tax information with state tax agencies, but only for tax administration purposes. It does not permit sharing for criminal investigations, civil enforcement, or immigration control. Its logic is cooperative taxation, not enforcement expansion.

Disclosure to Federal Law Enforcement (§6103(i))

Section 6103(i) allows disclosures to federal law enforcement agencies, but only under strict conditions. The requesting agency must submit a written application identifying a specific, named taxpayer and demonstrate that the information is relevant to a non-tax criminal investigation. This exception was designed for targeted, case-by-case requests, not for broad or automated data access (IRS Chief Counsel Guidance 2025).

Notably, immigration status violations are generally civil, not criminal. Even when criminal charges are possible, §6103(i) does not authorize bulk searches or category-based data sharing. The statute requires individualized suspicion and judicial oversight.

Disclosure for Tax Administration (§6103(k)(6))

This provision allows limited disclosures necessary for administering tax laws for example, verifying income or enforcing tax collection. Immigration enforcement does not fall within tax administration. Courts and the IRS itself have consistently interpreted this provision narrowly (National Taxpayer Advocate 2026).

Why the IRS–ICE Arrangement Exceeds Statutory Limits

The main legal problem with the IRS–ICE data-sharing arrangement is that it does not fit within any of these exceptions. According to publicly available court filings, the arrangement would allow ICE access to ITIN-related data at scale, rather than through individualized requests tied to specific criminal investigations (Center for Taxpayer Rights 2026).

That approach directly conflicts with §6103's structure. The statute does not permit executive agencies to decide on their own that immigration enforcement justifies broader access to tax data. If Congress had intended to allow immigration-based disclosures, it could have written such an exception. It did not.

This distinction matters because §6103 reflects a legislative balancing of interests. Congress weighed enforcement needs against compliance risks and chose confidentiality as the default. Executive agencies are bound by that choice.

Why Executive Authority Is Not Enough

The government has argued that executive authority over immigration enforcement justifies the arrangement. However, this argument misunderstands the hierarchy of law. Immigration authority does not override tax confidentiality statutes. Where Congress has spoken clearly as it has in §6103, executive discretion must yield.

However, courts have consistently held that statutory confidentiality protections cannot be bypassed through inter-agency agreements or policy memoranda (Law360 Analysis 2026). Allowing otherwise would render §6103 meaningless, as any administration could redefine enforcement priorities to justify disclosure.

The Structural Consequence

The limits of §6103 are not technical obstacles; they are intentional guardrails. If tax information can be repurposed whenever enforcement priorities change, taxpayers lose the ability to predict the consequences of compliance. That uncertainty undermines trust, reduces voluntary filing, and ultimately weakens revenue collection.

Thus, the statutory question is not simply whether the IRS may assist ICE. It is whether Congress's confidentiality framework still controls the use of tax data or whether it can be overridden by executive preference.

Constitutional Dimensions

Beyond statutory limits, the IRS–ICE data-sharing arrangement raises serious constitutional concerns. These concerns do not depend on whether Congress *could* authorize such data sharing in the future. Rather, they arise from how the policy affects individual rights under the First, Fourth, and Fifth Amendments as the system currently operates. The controversy is about whether the government may compel people to disclose sensitive information for one legal purpose and then use that information against them for another.

Fourth Amendment

The Fourth Amendment protects individuals against unreasonable searches and seizures, including government intrusion into private information. The Supreme Court has long held that the Amendment safeguards information in which a person has a "reasonable expectation of privacy" (*Katz v. United States*, 1967).

Tax return information clearly falls within this category. Filing a tax return requires individuals to disclose deeply personal financial details: where they live, where they work, how much they earn, and with whom they share their household. Importantly, taxpayers do not disclose this information voluntarily in the ordinary sense, they do so because the law requires it.

What makes tax data unique is that the expectation of privacy is not just social; it is legal. Section 6103 of the Internal Revenue Code explicitly guarantees confidentiality. This statutory promise shapes what expectations are "reasonable" for Fourth Amendment purposes (National Taxpayer Advocate 2026).

When undocumented immigrants file tax returns using ITINs, they do so with the understanding supported by years of IRS practice that their information will not be shared with immigration enforcement. Allowing ICE to access that information transforms tax filing into a mechanism for surveillance. From a Fourth Amendment

perspective, this resembles an unreasonable search: the government is exploiting compelled disclosures for a purpose unrelated to the reason the data was collected.

Recent Supreme Court jurisprudence has emphasized that large-scale government access to personal data, even when held by third parties, raises constitutional concerns, especially when individuals lack meaningful choice (*Carpenter v. United States*, 2018). Tax filings involve even less choice than commercial data sharing, strengthening the privacy claim.

Fifth Amendment

The Fifth Amendment protects individuals from being compelled to provide information that may be used against them in legal proceedings. Although immigration enforcement is often described as "civil," the consequences including detention, removal, and permanent bars to reentry are severe. Moreover, immigration-related information can also be used to support criminal charges in certain circumstances.

Additionally, filing a tax return is mandatory. Failure to file can result in civil penalties and, in some cases, criminal liability. When individuals are legally compelled to disclose information and that same information is later used as a basis for enforcement actions against them, the line between compliance and self-incrimination becomes blurred.

Precisely, the IRS–ICE arrangement raises this concern. Information such as a taxpayer's address or employer provided solely to comply with tax law could be used to locate and apprehend that individual. While courts have traditionally allowed compelled disclosures for regulatory purposes, they have also recognized limits when disclosures are later used punitively (*Marchetti v. United States*, 1968).

The constitutional problem is not resolved by labeling immigration enforcement as civil. What matters is that the government would be converting compelled compliance into evidence against the individual. This undermines the protective purpose of the Fifth Amendment and discourages lawful compliance.

First Amendment

The First Amendment is commonly associated with speech and expression, but it also protects against government actions that chill lawful behavior. A "chilling effect" occurs when people avoid lawful activity because they fear government retaliation or punishment.

Filing a tax return is a legal obligation. Yet if individuals reasonably believe that filing will expose them to immigration enforcement, many will choose not to file. This is not speculation; behavioral research consistently shows that perceived enforcement risk significantly reduces compliance (Tax Policy Center 2026).

The constitutional concern is that the government would be discouraging compliance with one law by threatening enforcement under another. Courts have long viewed such arrangements with skepticism, particularly when the chilled activity is legally required rather than merely permitted (*Speiser v. Randall*, 1958).

In this context, the chilling effect extends beyond undocumented immigrants. Once trust in tax confidentiality is weakened, other vulnerable populations mixed-status families, temporary visa holders, and even citizens in sensitive circumstances may question whether tax compliance is truly safe.

A system that penalizes compliance cannot function as a voluntary system. From a First Amendment perspective, policies that deter lawful conduct through fear of unrelated punishment are constitutionally anomalous.

Why These Constitutional Issues Matter Together

Individually, each constitutional concern raises serious questions. Together, they point to a deeper structural problem. The IRS–ICE arrangement effectively redefines tax filing from a neutral civic obligation into a risk-laden enforcement trigger. That transformation undermines privacy expectations, coerces self-exposure, and discourages lawful behavior.

The Constitution does not prohibit the government from enforcing immigration law. But it does constrain how enforcement is carried out, especially when it relies on information obtained through compulsion and trust. When multiple constitutional protections point in the same direction, courts traditionally treat that convergence as a warning sign (ACLU 2026).

Fiscal Consequences of Compliance Erosion

The most immediate impact of the IRS–ICE data-sharing arrangement is not only legal or constitutional, it is financial. The U.S. tax system depends heavily on voluntary compliance, meaning people file and pay taxes because they believe it is safe to do so. When that belief weakens, tax revenue drops. This section explains what that loss looks like in practical terms.

What undocumented tax filing currently contributes

Even though undocumented immigrants are not citizens or lawful permanent residents, many still file tax returns using Individual Taxpayer Identification Numbers (ITINs). They do this to comply with tax law, report income, and often to maintain employment records or support future immigration applications.

Economically, this group contributes more to public revenue. Current estimates suggest that undocumented immigrants using ITINs contribute approximately $11 billion to $13 billion annually in federal income and payroll taxes (Tax Policy Center 2026; National Taxpayer Advocate 2026). This does not include additional state and local taxes such as sales taxes, rent-related taxes passed through housing costs, and other indirect contributions.

Importantly, this revenue exists because the system is built on trust. The IRS has historically maintained that filing taxes does not, by itself, trigger immigration enforcement. That understanding is central to why millions of individuals file despite their immigration status.

Why trust affects tax revenue

Tax systems like the U.S. system rely on what economists call “compliance confidence”, the belief that cooperation will not be punished in unrelated ways. When people believe that providing information could expose them to deportation or other enforcement actions, they respond in predictable ways: they withdraw from the system.

In this context, the IRS–ICE arrangement changes the perceived risk of filing a tax return. Instead of being seen as a neutral legal obligation, tax filing begins to look like a potential pathway to detection by immigration authorities.

Once that perception spreads, even partially, it can reduce participation in the system. This is not limited to undocumented immigrants. Mixed-status households, temporary visa holders, and others with sensitive personal situations may also become more cautious about filing accurately or at all.

The “compliance cliff” effect

The primary fiscal risk is not a gradual decline, it is what economists describe as a compliance cliff: a sudden drop in participation once trust is broken.

If a significant share of ITIN filers decide that filing taxes increases their risk of immigration enforcement, they may choose non-filing as a rational alternative, even if it exposes them to civil tax penalties. For many individuals, the risk of deportation is far more serious than the risk of tax penalties.

Policy estimates suggest that even a 50% reduction in ITIN filing would result in a loss of approximately $5.5 billion to $6.5 billion annually in federal revenue (Tax Policy Center 2026). This is not a speculative figure, it is based on current contribution levels and conservative behavioral assumptions about compliance reduction.

What makes this important is that these losses would not be offset by increased enforcement efficiency. Most of the individuals whose data would be shared are already present in IRS systems. ICE would not be discovering entirely new populations; instead, the policy risks pushing existing taxpayers out of the system.

Broader fiscal ripple effects

The fiscal consequences extend beyond direct tax revenue losses.

i. Reduced payroll tax contributions: Lower filing rates reduce contributions to Social Security and Medicare trust funds, which rely more on payroll taxes (National Taxpayer Advocate 2026).

ii. Lower state and local tax reporting compliance: Many states use federal tax compliance as a baseline indicator of income reporting. Reduced federal filing can indirectly reduce state revenue accuracy.

iii. Higher enforcement costs: Increased non-filing and informal employment can require more administrative and enforcement spending by both tax and immigration authorities.

iv. Economic informality: When people stop filing taxes, they are more likely to move into informal or cash-based work arrangements, which are harder to regulate and tax.

Together, these effects create a net fiscal loss beyond the initial $11–13 billion contribution baseline.

Why the fiscal risk matters legally and politically

The fiscal impact is not just an economic concern, it is directly relevant to the legal analysis. Courts often consider whether government actions undermine the practical functioning of statutory schemes. In this case, the tax system depends on voluntary participation.

If a policy reduces participation in a predictable and significant way, it does not merely change enforcement strategy, it weakens the system itself.

Therefore, from a policy perspective, the irony is clear: a measure intended to improve immigration enforcement could reduce the government's overall revenue base, weakening the very institutions that fund enforcement.

Comparative Perspectives

One way to understand how unusual the IRS–ICE data-sharing arrangement is, is to compare it with how other similar countries handle tax data and immigration enforcement. The United States is not the only country that collects taxes from migrants or manages immigration enforcement. Countries like Canada, Australia, the United Kingdom, and New Zealand face the same basic challenge: people pay taxes while their immigration status may be uncertain.

What stands out is that these countries have made a clear institutional choice: tax systems are kept separate from immigration enforcement. The goal is the same everywhere, protect trust in tax systems so people continue to file honestly.

Canada: strict separation between tax and immigration systems

In Canada, the Canada Revenue Agency (CRA) collects taxes, while the Canada Border Services Agency (CBSA) handles immigration enforcement. These are completely separate institutions with different legal mandates.

Canadian tax law strongly protects taxpayer confidentiality under section 241 of the *Income Tax Act*. This rule means that CRA officials generally cannot share taxpayer information unless the law clearly allows it, and immigration enforcement is not one of those purposes (Income Tax Act, RSC 1985, s 241; Treasury Board of Canada 2025).

Even though Canada uses immigration screening systems and tracks temporary residents, it does not use tax filings as a tool to locate or deport individuals. The policy assumption is simple: people are more likely to pay taxes if they do not fear immigration consequences (Canada Revenue Agency Guidance 2025).

Australia: strong legal firewalls around tax data

Australia follows a similar model. The Australian Taxation Office (ATO) collects tax information under strict confidentiality rules in the *Taxation Administration Act 1953*. That law makes unauthorized disclosure of tax data a serious legal violation.

Australia also uses a Tax File Number (TFN) system that links individuals to income records. In theory, this system could be very useful for immigration enforcement because it tracks who is working and earning income. However, Australian law deliberately prevents that kind of use.

Immigration enforcement is handled by the Department of Home Affairs, which does not have direct access to ATO tax databases for enforcement purposes. The separation is intentional: Australia treats tax compliance as something that must be protected from immigration enforcement pressures to preserve revenue integrity (ATO Governance Report 2025; OECD Tax Administration Review 2025).

United Kingdom: legal restrictions and data protection limits

In the United Kingdom, HM Revenue & Customs (HMRC) manages tax collection under the *Commissioners for Revenue and Customs Act 2005*. Section 18 of that law makes taxpayer information confidential and even criminalizes improper disclosure.

At the same time, the UK has strict immigration enforcement rules under the "Right to Work" system, which requires employers to check immigration status before hiring workers. However, this system operates separately from tax collection.

A major constraint in the UK is data protection law. Under the UK's retained GDPR framework and the *Data Protection Act 2018*, government agencies are limited in how they can reuse personal data. Information collected for tax purposes cannot simply be repurposed for immigration enforcement without a lawful and compatible basis (UK Information Commissioner's Office 2025; HMRC Compliance Guidance 2025).

Furthermore, tax data cannot be reused for immigration enforcement just because it is useful. The law requires a separate legal justification.

New Zealand: privacy law as a structural barrier

New Zealand also keeps tax and immigration systems separate. The Inland Revenue Department (IRD) collects tax information under the *Tax Administration Act 1994*, while Immigration New Zealand handles border and visa enforcement.

What makes New Zealand particularly strict is its privacy law framework. The *Privacy Act 2020* includes a principle that personal information must only be used for the purpose it was collected, unless a very narrow exception applies (Privacy Act 2020, IPP 10; New Zealand Privacy Commissioner 2026).

This means that even if tax data could technically help immigration enforcement, it cannot legally be used for that purpose unless Parliament explicitly authorizes it. No such authorization exists in New Zealand.

A recent report by the New Zealand Privacy Commissioner noted that maintaining this separation is important for maintaining public trust in government data systems (Privacy Commissioner Immigration Oversight Report 2026).

What these countries have in common

Across all four jurisdictions, the pattern is consistent:

i. Tax authorities are separated from immigration enforcement

ii. Tax data is protected by strict confidentiality laws

iii. Immigration agencies do not have routine access to tax records

iv. Data protection or tax secrecy laws limit cross-use of information

v. Governments prioritize tax compliance over enforcement convenience

The reasoning is practical, not ideological. These systems assume that if taxpayers fear their financial disclosures could be used against them in unrelated enforcement actions, they will stop complying fully with tax obligations.

Why the U.S. approach stands out

Against this global background, the IRS–ICE arrangement is unusual. It moves in the opposite direction of the prevailing international model by linking tax data collected under a promise of confidentiality to immigration enforcement activity.

This creates a structural difference:

i. In Canada, Australia, the UK, and New Zealand → tax data is protected to preserve compliance

ii. Under the IRS–ICE arrangement → tax data becomes a potential enforcement tool

The concern raised by comparative analysis is not that the U.S. is "different," but that it may be moving away from a model that has been widely adopted to protect tax system stability.

Rule of Law Concerns

At its core, the rule of law means that government power must be predictable, consistent, and limited by clear legal rules, not changed informally through policy agreements or administrative convenience. People should be able to understand, in advance, what the legal consequences of their actions will be.

The IRS–ICE data-sharing arrangement raises serious rule of law concerns because it changes how information is used after people have already complied with the law. In simple terms, it changes the "rules of the game" after people have already played by those rules.

Changing the consequences after people have already complied

One of the most important principles in any legal system is legal certainty. People must know, at the time they act, what the consequences of their actions will be. Millions of taxpayers, especially undocumented immigrants using ITINs—filed tax returns under a long-standing understanding reinforced by statute: that tax information would remain confidential and used only for tax purposes (IRC §6103; National Taxpayer Advocate 2026). This understanding is not informal; it is embedded in law and IRS practice.

The rule of law concern arises when that same information is later used for a completely different purpose, including immigration enforcement. Even if the government argues that the law technically allows it, the practical effect is that individuals are being exposed to consequences they could not reasonably predict at the time they complied.

This is why legal scholars often say that retrospective changes in enforcement undermine trust in legal systems, even if they are technically lawful (OECD Rule of Law Indicators 2025).

The problem of "retrospective surprise"

A major issue here is what can be called retrospective surprise: people acted under one assumption, but the government later changes how their past actions are used. For example, individuals who filed tax returns in 2020 or 2022 did so under the assumption that this data would remain within the tax system. Under the IRS–ICE arrangement, that same data could later be used for immigration enforcement in 2026.

This creates a fairness problem. The issue is not just whether the government has legal authority today, but whether it is fair to change the consequences of past compliance after the fact. Courts and legal institutions often treat this as a rule of law concern because it weakens trust in legal stability (U.S. National Taxpayer Advocate 2026; ACLU 2026).

Institutional integrity

Another rule of law concern is institutional role distortion. The IRS was created to administer tax law, not immigration enforcement. Its effectiveness depends heavily on its perceived neutrality. People are more likely to report income honestly if they believe the IRS is focused only on taxation.

When tax authorities are used as a data source for immigration enforcement, the IRS effectively takes on a dual identity:

i. Tax administrator

ii. Immigration enforcement information provider

This dual role creates what governance scholars describe as "function creep," where an institution gradually becomes involved in purposes outside its original legal mandate (OECD Governance Review 2025). Once this happens, the boundaries between agencies become blurred, and individuals can no longer easily predict how their information will be used.

Proportionality and fairness in enforcement

Rule of law systems also require that government actions be proportionate. This means the government should not use overly broad or harmful measures when less intrusive options exist.

In this case, the fiscal and administrative harm of weakening tax compliance must be weighed against the enforcement benefit of accessing IRS data. Existing immigration enforcement tools already include access to:

i. DMV records

ii. Employment verification systems

iii. Border and visa databases

iv. Commercial and financial data sources

Given these alternatives, critics argue that using IRS tax data adds only limited enforcement value while significantly increasing harm to tax compliance behavior (Tax Policy Center 2026; Congressional Budget Office 2025). From a rule of law perspective, the concern is not only effectiveness, but whether the government is using the least harmful means available to achieve its objective.

Why these concerns matter together

Individually, each of these issues including retrospective effects, institutional blending, and proportionality raises concerns. Taken together, they point to a deeper problem. The IRS–ICE arrangement shifts the tax system from a predictable legal framework into a flexible enforcement tool.

That shift matters because tax systems depend more on trust than on force. If people believe that compliance can later be reinterpreted as a source of vulnerability, they will adjust their behavior by reducing transparency or exiting the system altogether. This is why rule of law principles are not abstract here, they directly affect whether the tax system continues to function effectively.

CONCLUSION

This paper has examined a single policy question, whether the IRS can share tax return information with ICE for immigration enforcement but the implications go far beyond that narrow issue. At the centre of the debate is a basic question of governance: can a government safely reuse information collected under a promise of confidentiality for a completely different enforcement purpose?

The analysis suggests that the answer, under current U.S. law and comparative practice, is no.

The legal conclusion

At the statutory level, Section 6103 of the Internal Revenue Code creates a strong default rule: tax return information is confidential and can only be shared in limited, clearly defined circumstances. None of those exceptions clearly authorizes bulk sharing of tax data with immigration enforcement agencies for the purpose of locating undocumented immigrants (IRC §6103; IRS Chief Counsel Guidance 2025).

This matters because the structure of §6103 is intentional. It was designed to prevent exactly this kind of broad, repurposed use of tax data, especially after historical abuses of tax records for non-tax purposes (National Taxpayer Advocate 2026). The IRS–ICE arrangement therefore sits in tension with the original purpose of the statute, even if arguments are made about executive discretion.

The constitutional conclusion

From a constitutional perspective, the key concern is not only what the government is doing, but how it changes the relationship between individuals and the state. Under the Fourth Amendment, taxpayers provide deeply personal information with a reasonable expectation of confidentiality supported by law (*Katz v. United States*, 1967; *Carpenter v. United States*, 2018).

Under the Fifth Amendment, they are compelled to disclose financial information under legal obligation, raising concerns when that information is later used in enforcement contexts (*Marchetti v. United States*, 1968). Under the First Amendment, policies that discourage lawful tax filing create predictable chilling effects (ACLU 2026; Tax Policy Center 2026). These concerns show that the issue is not only technical legality, it is structural. A system that depends on voluntary disclosure cannot function properly if disclosure becomes risky.

The fiscal conclusion

The fiscal analysis reinforces the legal concerns. The U.S. tax system depends heavily on voluntary compliance, including contributions from approximately 4.4 million undocumented immigrants using ITINs. These taxpayers contribute an estimated $11–13 billion annually in federal revenue (Tax Policy Center 2026; National Taxpayer Advocate 2026).

If even a partial breakdown in trust occurs, the result is a measurable revenue loss. Conservative estimates suggest that a 50% reduction in ITIN filing could reduce federal revenue by approximately $5.5–6.5 billion per year (Tax Policy Center 2026). furthermore, this loss is not easily recoverable through enforcement. Once trust is damaged, compliance does not automatically return even if policies are later reversed.

The comparative conclusion

Across other common law jurisdictions including Canada, Australia, the United Kingdom, and New Zealand, the consistent model is separation between tax administration and immigration enforcement. Tax agencies

protect confidentiality precisely to preserve compliance and prevent fear-driven underreporting (CRA 2025; ATO 2025; HMRC 2025; New Zealand Privacy Commissioner 2026).

The IRS–ICE arrangement therefore stands out not because it is innovative, but because it departs from a widely shared governance principle: tax systems function best when they are insulated from unrelated enforcement objectives.

Final observation

The central lesson of this analysis is simple. Modern tax systems do not rely primarily on force; they rely on trust. People comply because they believe the system is predictable, fair, and confined to its stated purpose.

When that trust is weakened, compliance becomes uncertain. And when compliance becomes uncertain, the fiscal foundation of the state becomes less stable.

The IRS–ICE arrangement, viewed through legal, constitutional, fiscal, and comparative lenses, raises a consistent concern: it risks converting a system built on voluntary cooperation into one shaped by fear of unintended consequences. For that reason, maintaining clear boundaries around tax data is not only a matter of privacy law. It is a matter of preserving the stability of the tax system itself.

REFERENCES

1. American Civil Liberties Union (ACLU). IRS–ICE Data Sharing Legal Challenge Brief (2026).
2. American Civil Liberties Union (ACLU). IRS–ICE Data Sharing Litigation Brief (2026).
3. Australian Taxation Office (ATO). Data Governance Report (2025).
4. Australia. Taxation Administration Act 1953 (Cth).
5. Canada Revenue Agency. Confidentiality and Data Governance Policy (2025).
6. Canada Revenue Agency. Data Governance and Confidentiality Guidance (2025).
7. Canada. Income Tax Act, RSC 1985, c 1 (5th Supp.) s 241.
8. Carpenter v. United States, 138 S. Ct. 2206 (2018).
9. Center for Taxpayer Rights et al., v. IRS et al., No. 26-5006 (D.C. Cir. 2026).
10. Congressional Budget Office (CBO). Federal Revenue and Compliance Sensitivity Report (2025).
11. Congressional Budget Office (CBO). Federal Revenue Sensitivity to Compliance Changes (2025 technical update).
12. Commissioners for Revenue and Customs Act 2005 (UK) s 18.
13. Data Protection Act 2018 (UK).
14. HM Revenue and Customs (HMRC). Compliance and Confidentiality Guidance (2025).
15. HM Revenue and Customs (HMRC). Taxpayer Confidentiality Guidance (2025).
16. Internal Revenue Code §6103.
17. Internal Revenue Service (IRS). ITIN Program Statistics and Filing Data (2025 update).
18. IRS Office of Chief Counsel. Disclosure Guidance on Return Information (2025).
19. IRS Office of Chief Counsel. Disclosure of Return Information Guidance (2025).
20. Katz v. United States, 389 U.S. 347 (1967).
21. Kevin Pinner. “DC Circuit Urged to Maintain Block on IRS–ICE Data Sharing.” Law360 (Mar. 20, 2026).
22. Marchetti v. United States, 390 U.S. 39 (1968).
23. National Taxpayer Advocate. 2026 Annual Report to Congress.
24. National Taxpayer Advocate. 2026 Annual Report to Congress.
25. New Zealand Privacy Commissioner. Immigration Data and Public Trust Report (2026).
26. OECD. Government Data Governance and Function Creep Report (2025).
27. OECD. Rule of Law Indicators and Governance Review (2025).
28. OECD. Tax Administration 2025: Comparative Information on OECD and Selected Non-OECD Countries (2025).
29. Privacy Act 2020 (New Zealand), Information Privacy Principle 10.

30. Speiser v. Randall, 357 U.S. 513 (1958).
31. Tax Policy Center. Revenue Effects of Reduced ITIN Filing (2026).
32. Tax Policy Center. Revenue Effects of Reduced ITIN Filing (2026).
33. Treasury Board of Canada Secretariat. Information Management Policy Update (2025).
34. UK Information Commissioner's Office (ICO). Public Sector Data Sharing Guidance (2025).
35. U.S. Constitution, amends. I, IV, V.