CHCI POLICY BRIEF
Developing the Next Generation of Latino Leaders®
CHCI CONGRESSIONAL HISPANIC CAUCUS INSTITUTE

March 2026

Data Leak: How the Lack of Federal Data Privacy Protections Leaves Both Citizens and Non-citizens Vulnerable

By **David Catalan,** CHCI Law Postgraduate Fellow

Executive Summary

The internet's worldwide usage has led to vast amounts of personally identifiable information (PII) being online, including names, birthdays, emails, faces, and even Social Security numbers.[1] With the plethora of personal data available online, companies, malicious third parties, and governments use PII as a form of currency.[2] Currently, there is no federal data privacy law protecting citizens' data from the aforementioned actors. On April 7, 2025, in a memorandum of understanding (MOU), the Department of Homeland Security (DHS), the Internal Revenue Service (IRS), and the Department of the Treasury agreed to share taxpayer information with Immigration and Customs Enforcement (ICE), breaking a long-standing tradition of the IRS not sharing data with other government agencies.[3] Under this MOU and other data-collecting strategies employed by companies, people, especially marginalized groups like Latinos, are at the whim of these actors with no autonomy over their PII.[4] [5]

Background

The U.S. began handling data in the 1700s with measures ensuring postal carriers' bags were sealed until they arrived at their destination.[6] The federal government's last significant attempt to regulate data privacy occurred with the Privacy Act of 1974, designed for an era of paper records and mainframe computers. The Privacy Act only applies to the federal government and only within federal agencies. There are other laws in place, such as the Health Insurance Portability and Accountability Act (HIPAA) (protects health data), Gramm-Leach-Bliley Act (GLBA) (some protections for private financial information), and the proposed Children's Online Privacy Protection Act 2.0 (COPPA 2.0 has been introduced and would update the age and requirements of COPPA 1.0)[7] (prevents the collection of children's PII).[8] However, these laws do not provide enough protection to prevent the abuse of PII.

The explosion of internet technologies in the early 2000s fundamentally altered how data is collected and monetized. Companies like Google, Meta, and Amazon now operate in an ecosystem built on continuous data harvesting, tracking user behavior, geolocation, health information, and even biometric identifiers.[9] Without comprehensive federal guidance, corporate data collection practices have grown unchecked, and enforcement mechanisms remain weak. The Federal Trade Commission (FTC), the main federal agency overseeing privacy issues, can only act under its limited 'unfair or deceptive practices' authority, often intervening after violations occur rather than preventing them.[10]

The absence of federal regulation has allowed the emergence of powerful data brokers who trade in vast datasets containing individuals' personal details. These brokers sell information to advertisers, political campaigns, and government agencies, including law enforcement. The 2018 Cambridge Analytica scandal, where Facebook data from over 87 million users was harvested for political microtargeting, demonstrated the dangers of unregulated

data sharing.[11] It revealed how personal information could be exploited to manipulate voters and influence democratic outcomes without their consent or knowledge.

For Latino communities, the stakes are even higher. Federal and local agencies, particularly ICE, increasingly rely on commercial and governmental data to monitor and target immigrant populations. Through partnerships with local law enforcement and private surveillance firms, ICE has accessed data from facial recognition software, license plate readers, and even smartphone applications.[12] In some cases, federal agencies have obtained taxpayer data through MOUs.[13] These practices blur the boundaries between lawful data use and state surveillance, raising civil rights and due process concerns.

The lack of federal oversight exacerbates inequality in digital protections. While wealthier individuals can afford privacy tools or live in states with stronger privacy laws, lower-income and minority communities often cannot. Latinos, who represent nearly 20 percent of the U.S. population, are disproportionately exposed to data misuse through both public surveillance and private data exploitation.[14] Recent judicial decisions, such as *Noem v. Perdomo*, which temporarily allowed language as a proxy for probable cause, underscore how easily digital and demographic data can be weaponized against Latino communities.[15] In this environment, the absence of a federal data privacy standard is not merely a regulatory gap—it is a matter of equity, civil rights, and public trust.

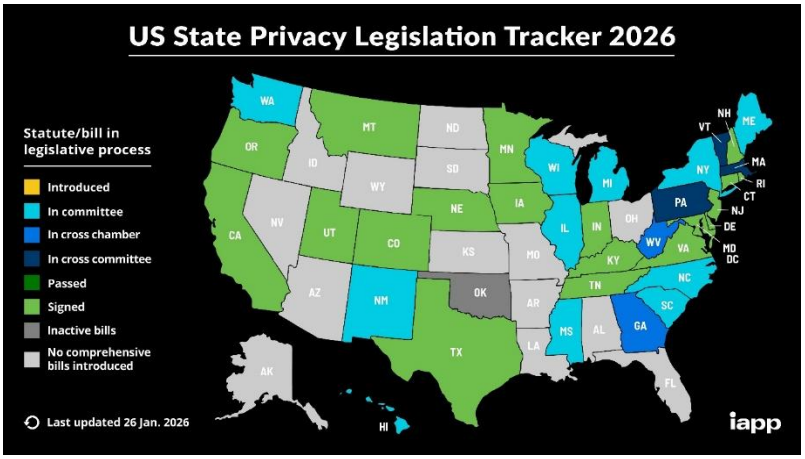
Problem Analysis

The absence of a federal data privacy law has left the U.S. with a fragmented, inconsistent system that fails to protect individuals or promote fairness across the digital economy. The problem lies not only in the lack of uniform standards but also in the growing exploitation of personal data by both private corporations and government agencies.

Since the 1970s, Congress has repeatedly failed to enact a comprehensive privacy framework. The Privacy Act of 1974 was never designed to address the scale and complexity of data collection that defines the 21st century. Today, the federal government depends on sectoral laws: HIPAA, the Fair Credit Reporting Act (FCRA), COPPA, GLBA, and others, each is limited to specific contexts.[16] None of these statutes provides baseline protections for everyday data transactions, leaving massive regulatory blind spots.

In the absence of congressional action, state legislatures have stepped in. California's Consumer Privacy Act (CCPA) and Virginia's Consumer Data Protection Act (CDPA) offer limited control over personal data, such as rights to access and delete information.[17] However, only a handful of states have adopted similar measures, resulting in a "privacy patchwork" that confuses consumers and burdens businesses with varying compliance obligations. Companies operating across multiple states must adhere to conflicting standards, while residents of states without privacy laws remain vulnerable to data exploitation. The FTC's limited enforcement capacity compounds the issue. The FTC can penalize companies for "unfair or deceptive practices," but this authority does not cover the systemic, anticipatory regulation needed to prevent harm.[18] Enforcement actions occur only after violations, and penalties rarely deter future misconduct.

The modern economy treats data as a commodity, an invisible currency that drives innovation, advertising, and political influence. In 2024, the global data brokerage industry was valued at over $389 billion, with U.S. companies controlling nearly half of the market.[19] These firms buy, aggregate, and resell sensitive personal information, often without the subject's knowledge or consent. Data brokers assemble detailed profiles, including Social Security numbers, home addresses, health conditions, consumer preferences, and even location history.[20] This information is then sold to advertisers, insurers, political campaigns, and, increasingly, law enforcement.



Furthermore, artificial intelligence companies increasingly rely on vast quantities of personal data to train and refine their models, demand for such information will intensify further incentivizing data brokers to expand collection practices with even fewer meaningful safeguards.[21]

In continuance, The Cambridge Analytica scandal of 2018 exemplifies the consequences of unregulated data commerce. The firm harvested Facebook data from 87 million users to create psychographic profiles used for microtargeting voters during the 2016 U.S. presidential election.[22] Users were unaware their information had been taken, nor could they opt out. This episode revealed the profound vulnerability of American consumers under a system where data ownership is ill-defined, and privacy is treated as a privilege rather than a right. The federal government responded by issuing modest fines but did not implement structural reforms to prevent recurrence.

For businesses, inconsistent state regulations create inefficiencies. Large corporations lobby for a weak federal privacy standard that would preempt stronger state laws, while smaller firms struggle with compliance costs across multiple jurisdictions.[23] Without a uniform federal law, the market tilts toward major technology companies that can afford sophisticated compliance infrastructures, reinforcing monopolistic dominance in the data economy. Economic inequality is thus mirrored in data governance: the entities with the greatest power to collect and manipulate information face the least meaningful oversight.

Beyond the economic sphere, the absence of federal privacy protections has facilitated government surveillance that disproportionately affects Latino and immigrant populations.[24] Agencies such as ICE, under DHS, have entered data-sharing agreements with state and local authorities, granting access to millions of personal records.[25] These arrangements include the use of facial recognition technology, license plate readers, and commercial data purchased from brokers like LexisNexis and Thomson Reuters.[26]

This surveillance regime is increasingly understood not as incidental data collection, but as a form of "migrant data extractivism." As Marianna Poyares (interdisciplinary researcher at Georgetown Law Center on Privacy and Technology) argues, contemporary migration governance relies on technologies such as biometric databases, DNA collection, AI-driven platforms, and monitoring applications, that are imposed as prerequisites for accessing basic rights or services, including education, humanitarian relief, or lawful presence. Under these conditions, meaningful consent is effectively impossible. Migrants are transformed from rights-bearing individuals into sources of behavioral and biometric data whose everyday interactions generate value for private technology firms and government agencies. This extractive model disproportionately targets racialized and precarious populations, particularly migrants from Latin America, whose legal vulnerability makes them preferred subjects of data capture. Crucially, migrant data extractivism reflects a normative shift away from a system grounded in human dignity toward one based on service provision conditioned on surveillance, where data collected for civil or humanitarian purposes is repurposed for enforcement, profiling, and long-term control. The result is a durable regime of racialized dispossession in which migrant communities are subjected to perpetual monitoring while lacking meaningful legal standing, transparency, or avenues for redress.[27]

The consequences of this system extend beyond immigration enforcement itself. Algorithmic decision-making tools increasingly rely on historical data that encode existing racial and socioeconomic biases, amplifying disparities in detention, deportation, and access to relief. Predictive systems used in immigration screening, facial

recognition, and risk assessment have demonstrated higher error rates for Latino individuals, reinforcing cycles of misidentification and over-policing. These technological practices deepen mistrust in public institutions and discourage immigrant families from engaging with schools, health systems, and tax authorities for fear that their data may later be weaponized against them.

Investigations by advocacy groups such as the Electronic Frontier Foundation have shown that ICE routinely purchases data from private companies to track individuals' movements and identify undocumented immigrants.[28] Because these transactions occur outside traditional law enforcement warrant requirements, they circumvent Fourth Amendment protections.[29] The surveillance extends to sensitive datasets such as tax filings and health records.

The targeting of Latino communities through data surveillance is compounded by implicit bias in algorithmic systems. Artificial intelligence and predictive policing tools use historical data that reflect existing inequities, amplifying discrimination in law enforcement and immigration proceedings.[30] For example, algorithmic decision-making in visa processing, facial recognition, and "risk assessment" software misidentifies Latinos at higher rates, leading to wrongful detentions and deportations.[31]

The consequences are chilling. Immigrant families increasingly fear engagement with public institutions, schools, hospitals, or tax agencies because their data might later be shared with ICE.[32] The erosion of trust in government data collection undermines essential services, impeding accurate census counts, public health research, and disaster response efforts in Latino-majority communities.

The lack of federal privacy protections raises fundamental civil rights concerns. Without clear legal standards, individuals have no guaranteed right to know what data is collected about them, to correct inaccuracies, or to request deletion. This asymmetry of power between corporations and consumers mirrors broader inequities in American society. Minority communities, particularly Latinos, face overlapping vulnerabilities: language barriers, limited access to legal representation, and disproportionate exposure to surveillance.

At the same time, the U.S. has fallen behind international norms. The European Union's General Data Protection Regulation (GDPR), implemented in 2018, established strict consent requirements, data minimization principles, and enforcement mechanisms with penalties up to four percent of a company's global revenue.[33] In contrast, U.S. citizens lack comparable guarantees, and American firms often store or process data abroad to avoid domestic scrutiny.[34] This weakens both consumer protection and international trust in U.S. technology exports.

Federal inaction also undermines democracy. Data-driven disinformation and microtargeting, enabled by the unregulated trade of personal information, distort political participation.[35] Latinos are frequent targets of online misinformation campaigns that exploit linguistic and cultural segmentation.[36] Without federal rules governing political data use, these practices continue unchecked, threatening electoral integrity.

Conclusion

Ultimately, the failure to enact a federal data privacy law represents a failure of governance. The absence of a comprehensive federal data privacy law exposes Americans to unprecedented levels of surveillance, exploitation, and inequality. What began as a regulatory gap has evolved into a systemic failure that undermines civil rights, market fairness, and democratic accountability. In the digital economy, data is power, and without uniform rules governing its collection and use, that power remains concentrated in the hands of corporations and state actors.

For Latino communities, the stakes are particularly acute. Weak federal standards allow ICE and other agencies to access PII, often purchased from private brokers or obtained through local law enforcement partnerships, without meaningful oversight. This surveillance has tangible human costs: fear of deportation, mistrust in public institutions, and the silencing of entire communities. At the same time, misinformation and algorithmic bias

target Latinos as both consumers and voters, amplifying systemic disparities in economic opportunity and political representation.

A federal privacy law would not solve all these problems overnight, but it is a necessary foundation for restoring public trust and accountability. Uniform national standards could protect vulnerable communities, strengthen consumer rights, and establish guardrails for responsible innovation. Without such action, the U.S. will continue to rely on a patchwork of state laws that privilege the powerful and leave the marginalized exposed. Privacy, once considered a personal concern, has become a collective civic necessity, one that demands national leadership.

Policy Recommendations

1. **Establish a Federal Baseline for Data Rights**
   Congress should enact a uniform federal standard granting all individuals fundamental rights over their personal data, including access, correction, deletion, and portability. These rights must apply regardless of state residence, income, or citizenship status

2. **Create an Independent Data Protection Agency**[37]
   The Federal Trade Commission's limited jurisdiction makes it ill-equipped to manage the scope of modern data governance. A new independent agency should oversee compliance, investigate abuses, and issue guidance on emerging technologies such as AI and biometrics.

3. **Regulate Data Brokers and Surveillance Technologies**
   Legislation should impose licensing and transparency requirements on data brokers, limiting the sale of sensitive information such as geolocation and biometric data.

4. **Strengthen Cybersecurity and Corporate Accountability**
   Federal privacy legislation must include mandatory breach notification standards and substantial penalties for negligent data handling.

Endnotes

[1] McCallister, Erika, Tim Grance, and Karen Scarfone, "NIST SP 800-122, Guide to Protecting the Confidentiality Of Personally Identifiable Information (PII)" NIST, April 2010, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf.

[2] Ramirez, Edith, "Federal Trade Commission May 2014 Data Brokers," Federal Trade Commission, 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[3] EPI, "ICE and IRS Reach Agreement to Share Taxpayer Information of Suspected Undocumented Immigrants," Economic Policy Institute, November 24, 2025, https://www.epi.org/policywatch/ice-and-irs-reach-agreement-to-share-taxpayer-information-of-suspected-undocumented-immigrants/.

[4] Economic Policy Institute, "IRS–ICE Memorandum of Understanding," April 2025, https://files.epi.org/uploads/IRS_ICE_MOU-April-2025.pdf.

[5] Georgetown Law Center on Privacy and Technology, "American Dragnet: Data-Driven Deportation in the 21st Century," American Dragnet | Data-Driven Deportation in the 21st Century, 2025, https://americandragnet.org/.; Pinsof, Jennifer, "EFF, ACLU to SFPD: Stop Illegally Sharing Data with ICE and Anti-Abortion States," Electronic Frontier Foundation, September 18, 2025,

https://www.eff.org/deeplinks/2025/09/eff-aclu-sfpd-stop-illegally-sharing-data-ice-and-anti-abortion-states.

[6] Post Office Act of 1792, 1 Stat. 232 (1792).

[7] 15 U.S.C. §§ 6501–6506 (COPPA); https://d1dth6e84htgma.cloudfront.net/01_H_R_6291_COPPA_2_0_18d36ec858.pdf.

[8] 5 U.S.C. § 552a; Congressional Research Service, "Data Protection and Privacy in the U.S.: Overview and Issues," 2023.

[9] Reuters, "Data Privacy: U.S. Lags Behind Global Standards."

[10] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," FTC Report to Congress, 2012.

[11] Lapowsky, Issie, "Facebook Exposed 87 Million Users to Cambridge Analytica," Wired, April 4, 2018, https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/.

[12] KQED News, "How ICE Is Using Your Data—and What You Can Do About It,"; Georgetown Law Center on Privacy and Technology, "American Dragnet: Data-Driven Deportation in the 21st Century," American Dragnet | Data-Driven Deportation in the 21st Century, 2025, https://americandragnet.org/.

[13] Diamond-Sagias, Katia, "IRS & ICE Immigration Data-Sharing Agreement: Explainer," National Immigration Forum, May 20, 2025, https://forumtogether.org/article/irs-ice-immigration-data-sharing-agreement-explainer/.

[14] Meissner, Doris, Donald M. Kerwin, Muzaffar Chishti, and Claire Bergeron. 2013. Immigration Enforcement in the United States: The Rise of a Formidable Machinery, Report in Brief. Washington, DC: Migration Policy Institute. https://www.migrationpolicy.org/research/immigration-enforcement-united-states-rise-formidable-machinery.

[15] Noem v. Vasquez Perdomo, 25A169 (U.S. Sept. 8, 2025), https://www.supremecourt.gov/opinions/24pdf/25a169_5h25.pdf.

[16] Congressional Research Service, "Data Protection and Privacy in the U.S.: Overview and Issues," 2023.

[17] International Association of Privacy Professionals, "US State Privacy Legislation Tracker," last updated 12 January 2026, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[18] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," FTC Report to Congress, 2012.

[19] CFPB, "CFPB Proposes Rule to Stop Data Brokers from Selling Sensitive Personal Data to Scammers, Stalkers, and Spies," Consumer Financial Protection Bureau, December 3, 2024, https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-stop-data-brokers-from-selling-sensitive-personal-data-to-scammers-stalkers-and-spies/.; Research and Markets, "Data Broker Market Forecasts, 2024-2029: Increasing Demand for Targeted Marketing, Rising Penetration of IoT with North America Projected to Lead Growth," Yahoo! Finance, November 15, 2024, https://finance.yahoo.com/news/data-broker-market-forecasts-2024-093500963.html.; U.S. Government Accountability Office, "Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace," Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace | U.S. GAO, November 15, 2013, https://www.gao.gov/products/gao-13-663.

[20] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," 2014.

[21] Brown, Christopher. "AI's Voracious Appetite for Data Imperils Key Privacy Principles." Bloomberg Law, October 2, 2025. https://news.bloomberglaw.com/litigation/ais-voracious-appetite-for-data-imperils-key-privacy-principles.

[22] Lapowsky, Issie, "Facebook Exposed 87 Million Users to Cambridge Analytica," Wired, April 4, 2018, https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/.

[23] *News from the States*, "Local Businesses—Not Just Big Tech—Push Back on Data Privacy Legislation."

[24] Lee, Nicol Turner, and Caitlin Chin-Rothman. "Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color." Brookings, April 12, 2022. https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

[25] William Turton, Christopher Bing, and Avi Asher-Schapiro, "The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE," ProPublica, July 15, 2025, https://www.propublica.org/article/trump-irs-share-tax-records-ice-dhs-deportations.

[26] KQED, "How ICE Is Using Your Data—and What You Can Do About It."

[27] Marianna Poyares, "Migrant Data Extractivism: Tech and Borders at the Limit of Rights," *International Migration* 63 (2025): e70065, https://doi.org/10.1111/imig.70065.

[28] Electronic Frontier Foundation, "ICE's Dragnet Surveillance and Data Purchases," 2021.

[29] *Carpenter v. U.S.*, 585 U.S. 296 (2018)

[30] Center for Democracy & Technology, "Algorithmic Bias and Immigration Enforcement," 2022.

[31] Georgetown Center on Privacy & Technology, "The Perpetual Line-Up: Unregulated Police Face Recognition in America," 2020, https://www.law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up/.

[32] Guariglia, Matthew, and Saira Hussain, "IRS-ICE Immigrant Data Sharing Agreement Betrays Data Privacy and Taxpayers' Trust," Electronic Frontier Foundation, April 25, 2025, https://www.eff.org/deeplinks/2025/04/irs-ice-immigrant-data-sharing-agreement-betrays-data-privacy-and-taxpayers-trust.

[33] European Commission. "General Data Protection Regulation (GDPR): Overview." 2018. https://commission.europa.eu/law/law-topic/data-protection/reform_en.

[34] "Executive Order 14117 of February 28, 2024, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," *Code of Federal Regulations*, 28 CFR 202: 1636-1752. https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern.

[35] Lai, Samantha. "Data misuse and disinformation: Technology and the 2022 elections." Brookings Institution, June 21, 2022. https://www.brookings.edu/articles/data-misuse-and-disinformation-technology-and-the-2022-elections/.

[36] Sanchez, Gabriel R., and Carly Bennett. "Why Spanish-Language Mis- and Disinformation Is a Huge Issue in 2022." Brookings Institution, September 11, 2025. https://www.brookings.edu/articles/why-spanish-language-mis-and-disinformation-is-a-huge-issue-in-2022/.

[37] Gillibrand, Kirsten. "Gillibrand Introduces New and Improved Consumer Watchdog Agency to Give Americans Control over Their Data - Kirsten Gillibrand: U.S. Senator for New York," Kirsten Gillibrand | U.S. Senator for New York, June 17, 2021, https://www.gillibrand.senate.gov/news/press/release/gillibrand-introduces-new-and-improved-consumer-watchdog-agency-to-give-americans-control-over-their-data/.