WRITTEN TESTIMONY OF LAURA MACCLEERY,
SENIOR DIRECTOR FOR POLICY AND ADVOCACY, UNIDOSUS

Presented at
"Updating America's Financial Privacy Framework for the 21st Century"

Submitted to
Committee on Financial Services

Submitted by
Laura MacCleery
Senior Director for Policy and Advocacy
Policy and Advocacy
UnidosUS
Raul Yzaguirre Building
1126 16th Street NW, Suite 600
Washington, DC 20036-4845

March 17, 2026

Chairman Hill, Ranking Member Waters, and members of the Committee, thank you for the invitation to testify. My name is Laura MacCleery. I am the Senior Director for Policy and Advocacy at UnidosUS, the nation's largest Latino civil rights and advocacy organization, with more than 300 community-based Affiliates nationwide. I have spent 25 years working for the public interest to support democratic systems, consumer protections, and civil rights.

We agree that the Gramm-Leach-Bliley Act (GLBA) is in need of an update. The data economy it governs has transformed beyond recognition since 1999. We welcome the Committee's attention to this problem, and seek to work with Members of both parties on a bill that delivers progress on privacy. Securing strong data protections has never been a more urgent task.

Latinos are a growth engine for the American economy, yet they remain underserved by financial institutions. The U.S. Latino "GDP" reached $4.1 trillion in 2025, an economy that would rank fifth among nations and is growing faster than China's. In 2024, one million Latinos turned 18. Latinos are projected to account for 70% of new homeowners by 2040, and Hispanic household wealth has tripled over the past decade.

Yet among families earning $30,000 to $50,000 annually, Hispanic households are unbanked at nearly five times the rate of white households, and 20% still use costlier alternatives to mainstream banks. These families are navigating complex financial systems at a moment when the security of their personal data is paramount.

I. The discussion draft does not advance consumer privacy

In 1933, after the crash and the Great Depression, Congress enacted the Glass-Steagall Act to separate commercial banking from investment banking and insurance. In 1999, GLBA repealed those barriers, permitting mergers that created the financial conglomerates that today dominate the economy.

The privacy provisions in Title V were among the consumer protection trade-offs that made this consolidation politically viable: requiring privacy notices and an opt-out right for third-party sharing, but providing no restriction on data sharing within corporate entities and no private right of action. Under statute, GLBA was a federal floor, with states free to go further.

Less than a decade later, the consolidation that GLBA permitted contributed to a financial crisis that nearly broke the global economy. Hispanic households lost 66% of their wealth between 2005 and 2009—the largest percentage drop of any racial or ethnic group, driven by the collapse of the housing market, in which nearly two-thirds of Latino net worth was concentrated. Latino homeownership actually decreased by 4% between 2007 and 2014, reversing historic trends.

Consumer financial protection had been fragmented across seven federal agencies, none of which had it as a primary mission. UnidosUS fought, alongside others, to create the Consumer Financial Protection Bureau (CFPB) to consolidate that authority into a single accountable agency, in part because the existing consumer protection framework, including GLBA, had so badly failed the communities we serve.

Since then, the financial data ecosystem has been rebuilt from the outside by companies GLBA did not anticipate, while the consolidation it facilitated means that data flows freely among "affiliates" within the multi-faceted conglomerates it created, diminishing the reach of GLBA's requirements for notice to consumers in practical terms.

Today, data aggregators sit between financial institutions and the apps consumers link to their accounts, including payment services, budgeting tools, and investment platforms. When a consumer connects an app to a bank account, the app generally does not communicate with the bank directly. An aggregator reaches into the account, pulls transaction data and delivers it.

For years, most aggregators did this by collecting consumers' actual bank login credentials and using them to access the account, a practice called screen scraping. Problematically, the bank cannot distinguish the aggregator from the customer. In addition, the aggregator often collected far more data than the app needed. And neither the consumer nor the bank had meaningful control over what happened to that data afterward.

By 2020, data aggregators reported that nearly 25% of Americans with bank accounts have connected to them via an app. Although they had become essential infrastructure, they remained outside GLBA and faced no comparable federal oversight.

The asymmetry this created was stark. Banks were subject to GLBA privacy requirements, federal supervisory examinations, security standards, and state privacy laws. Data aggregators were subject to essentially none of these at the federal level. The only meaningful constraints on their behavior came from state laws and private bilateral agreements with banks.

The banks had a reasonable complaint: Institutions subject to rigorous oversight were competing against entities that handled the same sensitive data without similar obligations. Section 1033 of Dodd-Frank, enacted in 2010, directed the CFPB to write the rules that would close this gap, but the rulemaking was long a neglected priority.

Fourteen years later, when the CFPB finally issued the Personal Financial Data Rights Rule in October 2024, it attempted to restructure the power dynamics of the financial data ecosystem by imposing obligations on all sides for the first time:

- Consumers gained the right to take their data and give it to a competing provider, including the ability to switch banks or try a new financial product without losing their financial history.
- Banks were required to build secure data pipelines to replace screen scraping and provide data at no charge.
- Aggregators and fintechs, for the first time under federal law, faced limits on what they could do with the data they accessed: They could only collect what was reasonably necessary for the service the consumer requested; they could not sell the data or use it for targeted advertising; and they had to delete it after one year unless the consumer reauthorized access. These third-party obligations were the consumer protection innovation GLBA had not anticipated.

The 1033 rule has bipartisan roots. The statute was enacted under President Barack Obama, while the rulemaking was initiated under the first Trump administration's CFPB director. Its basic diagnosis—that all participants in the financial data ecosystem should face comparable obligations—drew at least some support from banks, consumer groups, and even data aggregators.

That balancing act has now been abandoned in favor of a one-sided approach. The original rule, which faced a legal challenge by industry, was enjoined by a federal court. After a confusing series of reversals, the CFPB issued an Advance Notice of Proposed Rulemaking in August 2025, signaling it intends to reconsider core provisions, including whether banks may charge fees for data access and whether third parties can access data on a consumer's behalf at all. A coalition of consumer organizations wrote to this Committee, urging it to defend the original rule's data privacy protections and to hold hearings on the emerging practice of large banks charging fees for access to consumer data.

On a separate front, the CFPB's data broker rule was withdrawn and its examination and enforcement capacity gutted, as described below. The regulatory infrastructure that had finally been converging to create a world in which banks, fintechs, aggregators, and data brokers all faced comparable oversight has been dismantled before it could take effect. Meanwhile, the Federal Trade Commission (FTC), which would have jurisdiction over aggregators newly covered by GLBA, does not conduct regular supervisory examinations. Instead, it acts only after a violation has occurred and been identified.

Taking the CFPB largely offline did not just weaken consumer protections, though it did do that. It also halted the only serious federal effort to bring fintechs and data aggregators under the same rules as banks, which is the level playing field this Committee has said it wants to create. The CFPB was the major federal entity building regulatory infrastructure to close the gap between banks and unregulated entities handling the same data, including through the 1033 rule, the data broker rule, and larger participant rules. All of these initiatives have since stalled or been transmuted.

The discussion draft is being offered in that vacuum, and it contains some genuine improvements, such as expanded biometric, geolocation, and access credential definitions, a data minimization provision, an Artificial Intelligence (AI) disclosure requirement, and a continuing opt-out right. These are worth building upon, as they represent steps in a positive direction.

But these modest gains are undermined by several problematic and far more important legislative choices: the continuation of the ineffective opt-out model and an increasingly broad preemption provision, which now adds security to privacy as preempted topics and extends preemption to data aggregators.

First, the draft retains GLBA's opt-out model for third-party sharing and extends it to aggregators' use of consumer credentials. Under an opt-out, the default is that consumer data is shared unless the individual acts to stop it, so the path of least resistance is the path of least protection.

Behavioral research confirms what common sense suggests: Most consumers do not change default settings, and "dark patterns" (which are unregulated by the bill) frequently make the choice to limit sharing harder to find and exercise. Opt-out rates are also dramatically lower among people with limited English proficiency or lower digital literacy. For millions of Latino consumers, an opt-out presented only in English, with no requirement for multilingual notices or accessible formats, provides no meaningful protection.

The draft also creates a new exception for data collection and disclosure where a financial institution obtains "evidence of such individual's authorization." Financial institutions routinely embed consent in fine-print terms-of-service agreements and digital onboarding communications, including documents most consumers sign without reading, in contexts where refusing consent may mean foregoing a needed financial product. Yet the bill does not define what constitutes valid authorization, require that consent be knowing and voluntary, or prohibit consent as a condition of service. In practice, this exception could legitimize coercive consent practices simply by ensuring that those practices are better documented.

The data minimization provision (Section 502(f)) limits collection to what is "necessary for [the institution's] legitimate business, legal, or regulatory purposes." This allows an institution to decide what its legitimate business purposes are. The provision is also subject to all current GLBA exceptions and four additional carve-outs, including a catch-all for any purpose "otherwise required by law."

The bill's access and deletion rights are, similarly, weaker than they appear. Financial institutions have 45 business days to respond to consumer requests, or three months. Europe's General Data Protection Regulation requires a response within a month. California's Consumer Privacy Act allows only 45 *calendar* days, or half the proposed time. The discussion draft's preemption clause would also likely prevent states from legislating shorter timelines.

The deletion right is further limited by being available to former customers only. The deletion timeline makes some sense—current customers obviously cannot be invisible to a company. But it ignores a larger problem: Consumers should have both visibility on and control over which subsidiaries can do what with their personal information. Because the mergers GLBA permits may include corporate affiliates a consumer has never heard of and has no relationship to, customers should have much more transparency about how data is moving within corporate structures, and the law should create a right to explicitly select or deny relationships they want. And it is subject to broad exceptions (for compliance and regulatory purposes, for example) that substantially narrow the universe of data an institution must actually delete, leaving the parameters largely in their hands.

Most problematically, the draft contains a broad preemption provision ("shall *supersede and preempt* the application of any statute, regulation, order, interpretation, or other law in effect in any State that establishes privacy or security requirements." In contrast, Section 507 of GLBA explicitly provides that the law would not supersede state laws that provide greater protection.

That allowed states to respond when the federal standard fell short. And they did: California enacted opt-in consent for sharing sensitive financial data. Illinois created biometric privacy protections applicable to financial institutions. Colorado, Connecticut, Virginia, and others followed with comprehensive frameworks. These laws give consumers rights GLBA does not: to know what is collected, to delete it, and, critically, to sue when it is mishandled. They represent some of the most consequential consumer privacy advances of the last decades.

Section 301 of the discussion draft would replace the floor with a ceiling, providing that it "shall supersede and preempt the application of any statute, regulation, order, interpretation, or other law in effect in any State that establishes privacy or security requirements for nonpublic personal information." Many states with large Latino populations, California included, are among those likely to have enacted or be considering stronger protections. The draft would eliminate those protections without raising the federal standard above them.

The draft's treatment of insurance follows the same structure, creating the same problem. Section 301(b) allows state insurance regulators to adopt rules to implement it but caps those rules at the federal standard. Insurance touches nearly every family, including auto, homeowners, and health-related products, and is an area in which AI-driven surveillance pricing is already emerging, with companies using data profiles to charge different consumers different rates based upon an inferred willingness to pay. Capping state regulators at the federal standard forecloses their ability to respond as these practices develop or worsen.

The most counterintuitive consequence involves data aggregators. Many state privacy laws, including California's, Virginia's, and Colorado's, exempt entities already covered by GLBA, on the basis that federal financial privacy law already regulates them. Notably, data aggregators currently are not covered by GLBA, so they also fall outside that exemption. State privacy laws and state causes of action apply to them in full. Consumers have used those laws to bring successful class actions against major aggregators for obtaining login credentials through deceptive means.

As described above, the discussion draft changes GLBA's definition of "financial institution" to include data aggregators. Aggregators would thus become GLBA-covered entities and, in states with entity-level GLBA exemptions, would be immediately exempt from state privacy laws.

In other words, data aggregators would be covered by GLBA's minimal obligations, including privacy notices and opt-out compliance—requirements that banks have operated under comfortably for 25 years and that are totally ineffective. But because GLBA lacks a private right of action and relies on federal enforcement, this is a good trade. In exchange for obligations that consumers cannot enforce in court, data aggregators get exempted from legal claims under state law that consumers can enforce.

That exchange might be defensible if federal enforcement in this instance were robust enough to offer considerably stronger protections, but it is not. Every protection in this bill depends on federal regulators, and the agencies responsible are barely operational. Under current law, when federal enforcement falls short, states fill the gap. Under this bill, that option disappears. Rights on paper that no one can vindicate, enforced by agencies operating at a fraction of their capacity, but that nonetheless supplant state protections that work, is not a framework, but a void.

II. The CFPB's decimation is harmful to consumers and the rule of law

The Bureau returned $21 billion to consumers over 14 years on a budget under $700 million, capping overdraft fees, capping credit card late fees, removing medical debt from credit reports, and changing industry behavior across mortgage lending, debt collection, and student loans. Bipartisan polling consistently shows that two-thirds of Americans support the CFPB, including a majority of Republicans.

The CFPB has been subjected to mass terminations and stop-work orders. This systematic destruction of both staff and practical legal authority is producing measurable harm. Federal Reserve research confirms that when fair lending enforcement stops, discrimination rises. Nearly one-third of Latino families pay overdraft fees that the CFPB had tried to cap. And credit bureaus have sharply reduced complaint resolution rates since enforcement weakened, as ProPublica reports.

Supervision, or the regular examination of financial institutions for compliance, is the primary mechanism for enforcement. It is one reason why institutions maintain compliance programs, test lending models, and correct problems before they become crises in public confidence.

Under this Administration, the CFPB has slashed its examination program and terminated experienced staff. The agency averaged more than 600 supervisory events per year from fiscal 2020 through 2024; it is expected to conduct fewer than 70 in 2026, all virtual, with examiners required to recite an absurd "humility pledge" to companies they oversee.

A recent Government Accountability Office (GAO) report documents the severity of these changes. The largest financial institutions in the country now face virtually no ongoing federal supervision specifically focused on consumer protection and fair lending compliance. Violating statutory requirements, the CFPB has also abruptly shuttered every single disparate impact investigation, which is the primary tool for detecting systematic discrimination in automated lending.

The travesty of Colony Ridge illustrates what happens when enforcement is captured by other priorities or co-opted and its legal meaning hollowed out. Colony Ridge, a Houston-area developer spanning 40,000 lots, marketed properties to tens of thousands of Hispanic families through Spanish-language TikTok ads promising affordable homeownership.

What buyers received was flood-prone land without water, sewer, or electrical infrastructure, financed at interest rates three to five times the market price. Colony Ridge did not verify ability to repay, and one in four loans ended in foreclosure. The company repossessed properties and then resold them—some four or more times. According to the federal complaint, Colony Ridge accounted for 92 percent of all foreclosures in Liberty County between 2017 and 2022.

The CFPB and Department of Justice (DOJ) sued in December 2023. The current Administration's $68 million proposed settlement would provide no money directly to defrauded families. Instead, it earmarks $20 million for immigration enforcement in the communities where the victims live and imposes new documentary citizenship requirements on buyers.

In other words, a civil rights case brought to protect Hispanic consumers from predatory lending was converted into an immigration enforcement action funded by the defendant's money and directed at the same communities that the original lawsuit sought to protect. A coalition of organizations led by the National Fair Housing Alliance, including UnidosUS, filed an *amicus* brief prepared by Democracy Forward to challenge the Colony Ridge settlement. At a recent hearing, in which the DOJ's representative failed to appear, the court refused to approve the proposed settlement, citing the *amicus* brief and concerns about the agreement.

The pattern of legal distortion extends well beyond Colony Ridge. Under current leadership, the CFPB has dropped or sought to reverse more than 20 enforcement actions. For example, it attempted to undo its own Townstone Financial settlement, which was a product of a fair lending case brought by the first Trump administration. The federal judge denied the request, calling it "an act of legal hara-kiri that would make a samurai blush."

The agency has also moved to terminate its pending redlining consent orders nationwide, essentially giving official sanction to well-documented patterns of discrimination. ESSA Bank in Philadelphia, and Lakeland Bank in Newark, New Jersey, were required under consent orders to remedy deliberate lending discrimination against Black and Hispanic neighborhoods through branch investments, loan subsidies, and community outreach in the areas they had excluded.

When the DOJ sought to terminate the ESSA order early, the court denied the motion after civil rights organizations intervened, finding the order was still needed to ensure equal access to credit. In New Jersey, two DOJ attorneys requested to withdraw rather than file a motion to terminate the order, and civil rights groups again intervened to contest the termination. In each instance, the government is using the legal system to undermine the laws it is charged with enforcing, and in each instance, outside organizations are standing before federal judges to insist the laws against discrimination in housing and lending mean what they say.

What is clear is the message that these cases send. Every family that is trying to decide whether to report fraud, file a complaint, or cooperate with an investigation will consider their options, and many will reasonably conclude that the risk of engaging with the government now outweighs any benefit. When the government's promise of protection can be revoked, and data gathered to help people can be redirected against them, public trust—an essential ingredient in the stability of both our legal and financial systems—erodes.

III. The federal government is actively undermining data privacy

Multiple federal courts have found that federal agencies are actively undermining data privacy and weaponizing personal data in ways the law prohibits. That is the larger context in which this Committee is being asked to preempt state protections and concentrate consumer protection authority in the federal government.

The example of immigrant taxpayers is illustrative. For more than thirty years, the Internal Revenue Service (IRS) promised tax filers using Individual Taxpayer Identification Numbers (ITINs) that their information would stay confidential. Section 6103 of the Internal Revenue Code, enacted after Watergate specifically to prevent the political weaponization of tax data, made that promise law, by creating a presumption of confidentiality in the tax code. In 2022, ITIN holders paid $59 billion in federal income taxes, $26 billion to Social Security, and $6.4 billion to Medicare annually, funding programs from which they receive no benefits.

In 2025, the Administration tried to break that promise. After months of escalating pressure, including DOGE operatives who were seeking access to IRS data and DHS requests for millions of addresses, the IRS and Department of Homeland Security (DHS) signed a Memorandum of

Understanding in April 2025 that cited to the President's Executive Order on immigration enforcement.

DHS pressed the IRS to provide location data on 7 million individuals. One request asked for information including home addresses, employers' information, relatives, bank names, IP information, and Social Security or taxpayer identification numbers. Career officials at every level resisted: the Acting Commissioner, the Chief Risk Officer, the Chief Privacy Officer, and roughly 50 senior information technology executives reportedly were sidelined or resigned. When DHS subsequently requested 1.28 million records, after going back and forth on terms, the IRS disclosed 47,000 taxpayer addresses on the same day that the confirmed IRS Commissioner was fired.

Despite disinformation published on the official DHS site, further data sharing remains enjoined under two federal court orders. In November 2025, in *Center for Taxpayer Rights v. IRS*, a federal judge enjoined the IRS from responding to a similar request, finding the Administration's policy was unlawful and arbitrary and capricious. In a subsequent declaration, the government admitted, due to a processing error, that thousands of disclosures had violated the law even under its own interpretation of its legal obligations. In a ruling in response to the admission by the government, the judge went further, saying that the IRS had violated the law "approximately 42,695 times by disclosing last known taxpayer addresses to ICE…The IRS not only failed to ensure that ICE's request for confidential taxpayer address information met the statutory requirements, but this failure led the IRS to disclose confidential taxpayer addresses to ICE in situations where ICE's request for that information was patently deficient," she wrote.

In *Community Economic Development Center v. Bessent*, a different judge issued a preliminary injunction finding a high likelihood that the IRS-ICE data sharing violated and continues to violate the Internal Revenue Code, enjoining the Department of Homeland Security from using or even viewing it.

The term "data betrayal," which it appears I coined last year, describes when information provided by someone for one purpose is used to harm or threaten them. The general concept is grounded in caselaw. In *Center for Taxpayer Rights*, for example, the judge found that "[a] reasonable taxpayer would likely find it highly offensive to discover that the IRS now intends to share that information permissively because it has replaced its promise of confidentiality with a policy of disclosure."

This tracks the common law tort of intrusion upon seclusion, recognizing the concept of data betrayal as a cognizable harm. Interestingly for our purposes here, the cases stem from privacy analysis in the banking context. The court noted that examining a person's private bank account is one of the "types of invasion intrinsic in the tort," and drew an analogy from the Restatement. The judge reasoned that if someone uses a forged court order to obtain bank records, the customer's prior disclosure of information to the bank does not defeat the privacy claim—because the customer still has a privacy interest in the records with regard to the intruder. The court applied the same logic to taxpayers: they disclosed information to the IRS, individuals falsely purporting to have lawful access demanded it, and when Treasury acquiesced, their privacy was invaded.

The principle applies here as well: The institution holding the data, whether a bank or a government agency, is responsible to the trusted relationship, and cannot redirect data for purposes the individual never consented to. Financial data privacy legislation should codify that principle. Data collected for one purpose should not be used for an unrelated one without informed consent. Exceptions should be narrow, and generally the sale of consumer financial data to government agencies should require a court order.

There is also a cost in the loss of trust to the federal Treasury. When tax records submitted in good faith are used for purposes those taxpayers never consented to and could not have anticipated, it undermines the voluntary compliance on which the entire tax system depends. The Yale Budget Lab estimates the cost to be as high as $300 billion in lost revenue over the next decade.

The abuse of data rights, unfortunately, by the federal government extends well beyond taxes. While early attention focused on DOGE's access to sensitive federal databases, an ongoing threat is the systematic infrastructure now being built to consolidate and repurpose program data.

UnidosUS and Citizens for Responsibility and Ethics in Washington (CREW) recently submitted comments opposing a Treasury notice that would merge sensitive personal and financial data from eight pandemic-era relief programs. The proposal would combine data from the Emergency Rental Assistance Program, the Homeowner Assistance Fund, the State Small Business Credit Initiative, and other programs into a single federal system with broad routine uses. The notice cites Executive Order 14243 as legal authority, though an executive order cannot override the Privacy Act, the program statutes, or the tax code.

In short, families facing economic devastation who disclosed Social Security numbers, ITINs, household income, and addresses to qualify for programs such as emergency housing relief are now at risk of having that data consolidated and made available for purposes, including immigration enforcement, that the programs' authorizing statutes never contemplated and to which applicants never consented.

The machinery is bureaucratic, technical, and incremental, but the effect is the same: information provided in trust, redirected against the people who provided it. The pervasive betrayal of public trust that millions of families are experiencing from the actions of their government is the context in which this Committee is being asked to weaken their financial data protections.

IV. AI can transform data aggregation into a potent and unprecedented surveillance tool

Discussions of AI in financial regulation tend to focus on AI as an intelligence capability, including its uses in lending decisions, fraud detection, or customer service. Those applications matter. Algorithmic bias that can impact consequential decisions is a serious problem.

But another profound risk that AI poses to financial data privacy concerns its capacity and use for data aggregation. Financial data that are wholly anodyne, such as grocery purchases, gas station transactions, or rent payments, can become a surveillance tool when AI is used to connect it across sources and at scale.

A checking account, considered alone, reveals only some information. But combined with location data from a phone, browsing history, health information from a wearable device, and purchase records from retailers, it produces a detailed portrait of a person's life: where they sleep, what they believe, whom they associate with, what they can afford, or what they may think of the government and its actions.

Recent reporting reflects a very problematic and rights-infringing use of such data by government, including when immigration enforcement agents in Minneapolis addressed a Constitutional observer by name and recited her home address. That sort of surveillance capability is built from the same financial and commercial data that this Committee's policies affect, and allowing it to be regulated only by a moribund federal agency is the wrong policy choice for this moment.

Data brokers today sell this information about every American, collected from phones and other devices without meaningful consent. This powers the online ad economy, where auction sites sell packets of consumer data at breakneck speed at auction. At the same time, 80% of Americans believe the government should need a warrant to buy it.

The harm from AI-driven data aggregation is also already reshaping what consumers pay. In 2024, the FTC launched a formal investigation into "surveillance pricing:" the use of AI and personal data profiles to charge different consumers different prices for the same product based on data-driven inferences about their willingness to pay. Companies use location data, browsing behavior, purchase history, and demographic inferences to generate individualized or segment-specific pricing recommendations, updated as frequently as every few minutes.

The upshot is a new form of market unfairness: A consumer in a lower-income zip code, or one whose browsing pattern suggests urgency, may pay more for the same product than a consumer the algorithm identifies as a comparison shopper. The financial data that this bill governs, such as transaction histories, account balances, and payment patterns, is the same information that makes these systems possible.

In short, weakening constraints on how financial data flows to third parties expands the raw material available for surveillance pricing and for government surveillance. Congress should not create an exemption that can block future state action to respond to these growing and serious problems.

Importantly, the rapid pace of improvements in AI makes insights into data at population scale possible. That is why the recent Anthropic controversy is driving concerns. When one of America's leading AI companies refused to allow its technology to be used for mass surveillance of Americans, the Administration retaliated by threatening to designate it as a supply chain risk, a designation never before applied to a domestic company. When AI can synthesize what scattered commercial datasets reveal about any person's life, the absence of judicial oversight over the government's acquisition of that data becomes a Constitutional emergency.

The law has not kept pace with these capabilities. As a coalition of civil liberties, civil rights, and technology organizations, including UnidosUS, wrote to Congress this month, the Foreign Intelligence Surveillance Act (FISA) reauthorization presents an opportunity to close the data broker loophole that enables warrantless bulk data collection. That loophole allows government agencies to purchase from data brokers the same information they would otherwise need a court order to seize. Closing this gaping legal gap would establish a critical legal safeguard before warrantlessly acquired data is fed into AI surveillance systems.

This discussion draft would make that problem worse. Removing constraints on collection, weakening purpose limitations through ill-defined data minimization standards, and preempting state restrictions on data flows to third parties all would expand the pool of financial data available for AI-driven profiling by corporations, data brokers, and governments.

The discussion draft does include an AI disclosure requirement, which is the first of its kind in federal financial regulation. That is worth preserving. But disclosure without constraint is mere transparency without accountability. The bill would impose no substantive limits on uses of AI in financial products or by data aggregators, such as testing for bias in lending outcomes. Nor would it create a right for consumers to challenge discriminatory AI-driven outcomes or create a clear pathway for accountability for decisions.

Yet AI lending systems have documented patterns of discrimination, which are avoidable with better models. Researchers have repeatedly demonstrated that less discriminatory models with comparable accuracy are technically achievable. The CFPB has closed all disparate impact investigations and proposed revisions to the applicable regulation, so no federal regulator is checking whether firms look for them. As federal enforcement retreats from AI accountability, states have also become a primary venue in this area.

At the same time, if governed well, use of AI tools could hold real promise for communities. AI could help to detect discriminatory lending patterns that human review misses, expand language access for the 13 million Americans who speak English less than “very well,” improve financial education tools, and help develop and validate lending models for underserved consumers. Personalized learning platforms, real-time translation, and job-matching tools designed with diverse communities in mind are concrete examples of how AI could support the economic mobility that Latino families are building.

But realizing that promise requires governance structures that channel innovation toward fair outcomes. In UnidosUS comments to the Office of Management and Budget (OMB) on AI governance, we proposed a framework anchored in enforceable rights, formal community participation in oversight, and investment in the digital capacity communities need to engage meaningfully with the technology that affects their lives. Accountability builds trust; trust enables adoption; adoption improves systems.

And as AI models rapidly improve through recursive learning, they can be used to help power this democratic process, including by monitoring outcomes, surfacing disparities, and adapting governance to evolving capabilities and public needs. The goal is feedback loops, not stasis. A governance framework designed with this dynamic in mind does not slow innovation. It builds the foundation of legitimacy on which durable innovation depends.

V. Disclosures should be required in the languages that consumers understand

Financial institutions have the resources and sophistication to reach Spanish-speaking consumers. One of the largest banks in the country reports nearly 4.5 million customers whose primary language is Spanish, with Spanish-language capabilities at almost 70% of its branches. Another major bank's call center supports more than 100 languages.

Yet privacy notices, opt-out mechanisms, terms of service, and account agreements remain overwhelmingly English-only. The industry's stated reason is legal liability, but this has no real basis given that these are written documents and can be developed as needed. The CFPB published Spanish translations of key disclosures, including adverse action notices, mortgage origination documents, and credit reporting notices, to address this concern, but their use is voluntary, they cover only a subset of consumer-facing documents, and the agency's willingness to maintain or expand them has been decimated.

Credit unions are demonstrating that the liability argument is not an insurmountable barrier. The *Juntos Avanzamos* network, a designation administered by Inclusiv for credit unions committed to serving Hispanic and immigrant communities, now includes 145 credit unions across 31 states, Puerto Rico, and the District of Columbia, collectively serving more than 13 million consumers. Designated credit unions are required to make information available in Spanish, employ bilingual and culturally competent staff, and accept alternative forms of identification. Individual credit unions in the network go further: One provides official documents and communications in Spanish, with a third of its front-line staff offering bilingual services; another has bilingual staff at 26 of 32 branches and pays a bilingual premium to certified employees. These are institutions with a fraction of the resources of the largest banks.

Several states already require translation of financial documents when the transaction was negotiated in a language other than English. California, Arizona, Illinois, Oregon, and Texas require that contracts and disclosures be provided in the consumer's language when the sale was conducted in that language. Nevada enacted a specific financial protection for Lower English Proficiency (LEP) consumers in 2021, giving consumers the right to rescind contracts that were negotiated in their language but documented only in English. These state laws reflect a straightforward principle: if an institution is sophisticated enough to find a consumer in their language, it should document the relationship in that language.

The discussion draft requires new privacy disclosures, including opt-out mechanisms, access requests, deletion requests, and AI disclosures, yet it requires none of them in any language other than English. It does not build on the principle these states have established. For the 13 million U.S. residents who speak English less than "very well," the bill's new disclosures are inaccessible.

An institution that markets its services to a consumer in Spanish, serves that consumer in Spanish at the counter, then hands them an English-only privacy notice with an English-only opt-out mechanism, has not provided a meaningful choice. It is evident that financial institutions know how to communicate with consumers in their own language when it serves their interests. There is simply no good reason not to require it for rights-related disclosures and communications as well.

VI. Congress should modernize GLBA by raising the floor, not lowering it

Congress should:

- **Preserve the federal floor.** GLBA functioned as a floor for 27 years, and states that built above it produced consequential consumer privacy advances, such as California's opt-in consent, Illinois' biometric protections, and suits that held data aggregators accountable. Eliminating state authority when federal enforcement has been deliberately diminished to fewer than 70 examinations a year concentrates all consumer protection risk in a system that is already demonstrably failing.
- **Require opt-in consent and provide it in relevant languages.** The opt-out model has failed for 27 years. Behavioral research and two decades of evidence confirm that it systematically fails consumers with limited English proficiency, lower digital literacy, or less time to navigate complex disclosures. Consumers should be able to access financial services whether or not they permit data sharing. That choice should be clear and accessible as a matter of design and available in any language in which the institution conducts business.
- **Create a private right of action.** The Colony Ridge settlement, Townstone reversal, terminated redlining consent orders, and closure of every disparate impact investigation demonstrate that accountability dependent on a single administration's appetite for enforcement is not a valid strategy over time. When federal enforcement is captured, consumers need the ability to vindicate their own rights in court.
- **Impose examination authority over aggregators and fintechs.** The bill brings aggregators under GLBA but provides only the nominal obligations banks have operated under for 25 years, enforced through occasional FTC actions after the fact. That is not comparable to the ongoing supervisory examination banks undergo. If Congress is serious about closing the regulatory gap, it should mandate the kind of oversight that matters.
- **Require AI testing for discriminatory outcomes before deployment.** Researchers have demonstrated that less discriminatory lending models with comparable predictive accuracy are technically achievable. The CFPB has closed every disparate impact investigation. No federal regulator is checking whether firms look for fairer models. Firms should be required to find them under law, and states should retain the authority to enforce that requirement, as Massachusetts did when it held an AI-driven lender accountable for models that penalized Black and Hispanic borrowers.
- **Define data minimization with enforceable boundaries.** The bill's data minimization provision lets the institution define what its own "legitimate business purposes" are and exempts everything else. Congress should set a firm standard for permissible collection defined by the sensitivity of the data and necessity of the use, not by the interests of the institution.
- **Prohibit data betrayal.** Congress must address the pattern of abuse of public trust that now includes tax records redirected for immigration enforcement, and pandemic relief and housing data being weaponized against communities it was supposed to help. Data privacy legislation should establish the principle that data collected for one purpose cannot be repurposed to harm someone, and should prohibit the sale of consumer financial data to government agencies absent a narrow and specific court order. The FISA reauthorization offers an immediate opportunity to close the data broker loophole

that enables warrantless bulk acquisition; legislation should complement that effort rather than expanding the pool of data available for purchase without providing any accountability for harms.

- **Establish governance standards for use of AI in financial services.** The bill's AI disclosure requirement is a first step, but disclosure without constraint is transparency without accountability. Congress should require testing of AI systems for discriminatory outcomes before deployment, mandate the use of less discriminatory alternatives when they are available, and give consumers a right to challenge AI-driven decisions that affect their access to credit, insurance, or financial products. The UnidosUS governance framework—which anchors AI governance to enforceable rights, creates formal roles for impacted communities in oversight, and fosters investment in the digital capacity communities need to engage with the technology that affects their lives—provides a model.

Public support for these measures is broad and bipartisan. A 2023 Pew survey found that 68% of Republicans and 78% of Democrats favor regulation of what companies can do with personal information. A UnidosUS poll the same year found that Hispanic voters' top concern about AI is its impact on personal privacy. The mandate for stronger protections exists.

Estonia, emerging from Soviet occupation, embedded data privacy in its constitution and built the most digitally advanced government in the world around one principle: Its people control the use of their data and are owed transparency on how it moves through private and public hands. In light of the evolution in data usage and its power, the United States can do better than a 27-year-old opt-out framework that tramples on state protections.

Conclusion: Data privacy is democratic infrastructure

The Framers designed the Republic to prevent the concentration of unaccountable power, including the power to surveil citizens without constraint. Financial data, combined with AI and the larger commercial data broker market, now provides a pathway to exactly the kind of concentration and abuse of power by government they would have feared.

A pattern in financial data regulation has been to deregulate, reap the consequences, regulate to address them, then ignore the lessons learned and deregulate again. The GLBA enabled consolidation, which contributed to a crisis. That crisis produced the CFPB. As the CFPB was working to close many of the gaps, the Administration gutted the CFPB.

And now Congress is being asked to preempt state laws that compensated for federal shortcomings and responded to consumer needs—and call the result modernization. We must not again consolidate the deregulation while blocking meaningful forms of accountability that are available to the public.

UnidosUS serves communities being harmed by the absence of meaningful data privacy rules. The promise of America is tested every time taxpayer data is misused for purposes other than what it was provided for, a civil rights case is redirected away from the people it was meant to protect, or a privacy framework is weakened. We must build financial data protections that keep that promise and maintain public trust. We urge the Committee to work together to break this cycle, serve a greater purpose, and answer the needs of this moment.