
**Comments of the World Privacy Forum**

**to the Consumer Financial Protection Bureau**

**Regarding Notice of Proposed Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB-2023-0052**

*via: regulations.gov and email to: 2023-NPRM-Data-Rights@cfpb.gov*

Consumer Financial Protection Bureau
1700 G Street NW,
Washington, DC 20552.

29 December 2023

The World Privacy Forum welcomes the opportunity to submit comments on the Consumer Financial Protection Bureau's (CFPB) Notice of Proposed Rulemaking on its Required Rulemaking on Personal Financial Data Rights, 88 Federal Register 74796 (October 31, 2023).

The World Privacy Forum is a nonprofit, non-partisan 501(C)(3) public interest research group. The organization is focused on conducting in-depth research, analysis, and consumer education in the area of data privacy and data governance, and focuses on pressing and emerging issues. It is among one of the only privacy-focused NGOs conducting independent, original, longitudinal research. The core area of focus for the World Privacy Forum is on complex data ecosystems and their governance, including privacy. The World Privacy Forum's work has provided analysis and insight in important issue areas, including AI and predictive analytics, identity ecosystems, health

privacy, medical identity theft, data brokers, and large-scale digital and financial data flows, and work on vulnerable populations and inclusion. The Forum was founded in 2003 and works both nationally and internationally. The Forum also works to encourage collaborative efforts among other non-profits. WPF frequently chairs or co-chairs international working groups focused on research and data governance/data protection, most recently at the WHO, UN, and OECD. WPF co-chairs the UN Statistics Data Governance and Legal Frameworks working group, and is co-chair of the WHO Research, Academia, and Technical Constituency. At OECD, WPF researchers participate in the OECD.AI AI Expert Groups, among other activities. WPF participated as part of the first core group of AI experts that collaborated to write the OECD Recommendation on Artificial Intelligence, now widely viewed as the leading normative principles regarding AI. WPF research on complex data ecosystems governance has been presented at the National Academies of Science and the Royal Academies of Science. World Privacy Forum: https://www.worldprivacyforum.org.[1]

WPF is pleased to read this NPRM and we support the goals it articulates. We applaud the Bureau for paying attention to the privacy and security interests of consumers. We also applaud the careful evaluation of proposed policies on a clear, substantial evidentiary basis.

In these comments, we discuss and analyze various aspects of the proposal. We also highlight several gaps and challenges regarding privacy protections for consumers in the financial sector that by our analysis would still remain if the NPRM were installed as proposed.

The proposed rulemaking affords an important opportunity to address these meaningful gaps. WPF urges the CFPB to act to close these gaps given this rare opportunity to do so.

## I. Electronic Access to Personal Financial Data: Additional thoughts and data

The NPRM contains an excellent overview of the development of electronic access to consumers' personal financial data. We found this overview helpful and relevant. WPF agrees with the assertion in the NPRM that most consumers today are banking digitally, and often banking across several platforms, especially mobile. We add to this analysis several thoughts.

[1] World Privacy Forum's home page includes information about our activities, as well as numerous data governance and privacy research, data visualizations, and resources. https://www.worldprivacyforum.org.

**A. Most consumers are banking digitally, but more advances are on their way soon**

First, we acknowledge the impact digital acceleration has had on the financial sector. The COVID-19 pandemic accelerated the adoption of digital services in general, including digital and mobile banking.[2]

The digital acceleration has been felt across many regions, including the U.S. While regional contexts differ, the data is showing that the U.S. digital infrastructure generally advanced by an estimated decade, though these estimates vary by sector and other factors. We can agree, however, that digital financial services development certainly sped up as a result of the urgent needs the pandemic placed on the financial sector.

We mention this issue because the development of digital banking in the U.S. context has been lagging behind some of the most forward-leaning digital banking ecosystems. This is especially true of countries with highly developed digital identity and digital services "stacks." For example, India has an advanced and complex mobile digital banking and financial sector ecosystem in place via the "India digital stack." [3] This digital services stack was built to intentionally include digital consumer banking beginning. This work began in earnest in 2010 when the backbone of the near-real-time Aadhaar unique identity system that has 1.4 billion enrollees was built. Today, India's digital services stack reaches nearly 100% of the country's population.

With this digital services backbone in place, India's digital banking footprint is complex, highly developed, and at a more mature level of advancement than that of the U.S. There were many early problems in the India Stack, and there were significant regulatory and privacy growing pains. WPF conducted field research in India on this topic, and this research has been peer-reviewed and published. It is too lengthy to repeat here, but it is sufficient to cite the research and note that India learned hard regulatory lessons via a fair and helpful India Supreme Court design, the landmark Aadhaar decision, which essentially kept the benefits of the India Stack, and required the installation of privacy legislation as well as specific mitigations in the financial sector, among other mitigations. There is an enormous amount of beneficial learning

---

[2] Asli Demirgüç-Kunt, Loera Klapper, Dorothe Singer, and Saniya Ansar, *COVID-19 drives global surge in the use of digital payments; The Global FIndex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19.* World Bank Group, 2021. https://www.worldbank.org/en/publication/globalfindex.

[3] See, IndiaStack, https://indiastack.org/ . *See also*: Digital Public Infrastructure Event, *Digital Public Infrastructure Accelerating Action Workshop.* World Bank Group, September 12-14 2023. https://www.worldbank.org/en/events/2023/09/12/digital-public-infrastructure-accelerating-action-workshop. See in particular the research associated with G2Px Initiative, https://www.worldbank.org/en/programs/g2px.

that can be acquired from the experiences and mitigations that have been produced in the India Stack context.[4]

However, after the digital acceleration from the pandemic, the U.S. is now rapidly advancing with complex build-outs of the provision of digital financial services. The research WPF has conducted n India regarding its advanced digital ecosystems indicated - based on the growing pains in privacy and other areas — that it will be important to get advanced digital banking policies in place now to address expected developments that have already taken place in other contexts that are ahead of where the U.S. is today.

All contexts are different, but it is still possible to derive beneficial lessons learned from the extensive digitalization in one of the largest digital financial and identity ecosystems in the world that precedes that of the U.S. by a decade.

**2. Mobile identity appears to be the digital ID system the U.S. is going to adopt — which has consequences for the digital banking sector ecosystem and for consumer privacy**

Digital identity[5] will be a critically important factor in U.S. consumer digital financial services and consumer privacy. The U.S. is in quite a different position from the majority of the world, in that the U.S. does not have a national ID, and it does not have a cabinet or ministerial-level position for an identity authority, something that is well-established in many other jurisdictions.

National identity systems are often accompanied by corresponding identity legislation as well as privacy legislation to control how the identities are used and protected across sectors. In Figure 1, below, the ratio of nations with national ID systems in relation to those without a national ID system has become stark, and updated research has only made this data even more stark.[6]

---

[4] Pam Dixon, A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S., Springer Nature, Health Technology. DOI 10.1007/s12553-017-0202-6. http://rdcu.be/tsWv

[5] The images in this section of the comments are taken from research conducted by WPF and presented at the Federal ID Forum Conference, 6 September 2023 on the topic of data governance and the U.S. ID ecosystem. The information about the four key ID platforms is adapted with permission from Dr. Joseph Atick's plenary presentation in Nairobi, Africa, 23-25 May, 2023, where WPF was present as a rapporteur for the event. ID4Africa AGM: https://events-agm.herokuapp.com/2023.

[6] See the 2022 *World Bank ID4D Data Series*, which includes data about all national ID systems, as well as identity authorities and corresponding legislation. The World Privacy Forum's data visualization is based on World Bank data. ID4D Data Series, World Bank, 2017-2022. https://datacatalog.worldbank.org/search/dataset/0040787 .

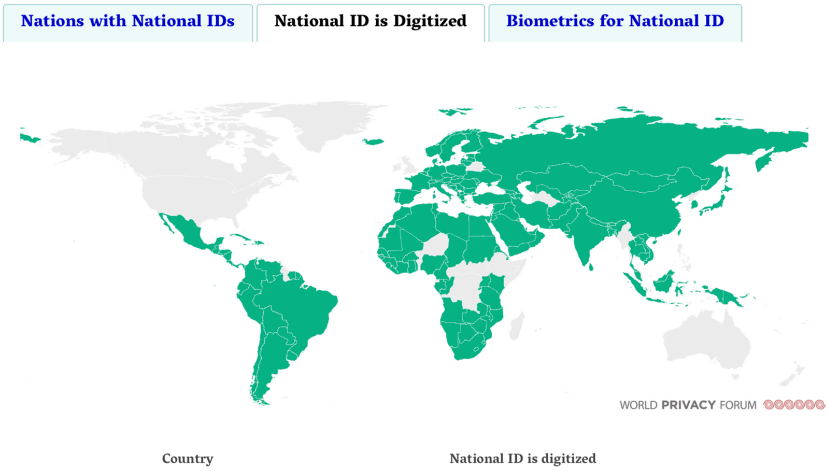



*Figure 1: This figure shows a screen shot of the **National ID systems Around the World** data visualization on WPF's web site. The visualization shows the diffusion of national ID systems, including digital ID systems and biometric national ID systems. This chart is available at https://www.worldprivacyforum.org/2021/10/national-ids-and-biometrics/ .*

Articulating the way that identity intersects with the financial sector regarding "Know-Your-Customer" or KYC requirements, anti-fraud systems, transactional resolutions, and in multiple other contexts is absolutely critical to data governance and data privacy rules and outcomes. In the U.S., there are very large gaps in privacy and security protections regarding digital identity. This creates a problematic basis for the articulation of identity within these financial systems as they grow more complex.

To begin to untangle some of the issues here, we begin by setting forth a factual basis for contextualizing this general area of knowledge. To do so, we share in these comments the 4 key identity platforms of today. These are global platforms, common to almost all jurisdictions with some form of national ID system. These identity platforms can also function at smaller subnational scales, and in some cases, scales even smaller than that. WPF thanks Dr. Joseph Atick for his articulation and presentation of these key platforms at the plenary session of the ID4Africa Annual General Meeting in Nairobi, Kenya in May 2023; it remains the best and most concise presentation WPF has seen on the topic of modern identity. WPF has adapted the information slightly for the U.S. context. The identity platforms are presented below in order of system maturity levels.

The legend for the core components of identity platforms can be seen in Figure 2. Each modern identity platform consists of a type, with a unique credential storage, token, digital credential presentation or verification, and trust model.

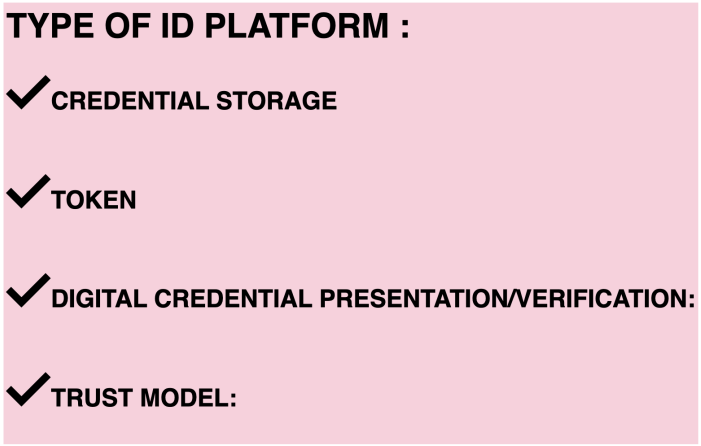



*Figure 2. Each modern identity platform consists of a type, with a unique configuration of credential storage type, token type, digital credential presentation or verification type, and trust model.*

The four key identity platforms of today include:

1. Electronic Identity
2. Mobile Identity
3. Digital Identity (true )
4. Decentralized Digital Identity

The platforms are listed in order of complexity and maturity, with decentralized digital identity platforms being the most advanced systems that are available today. Figure 3, below, is a diagram of the four key platforms for identity.

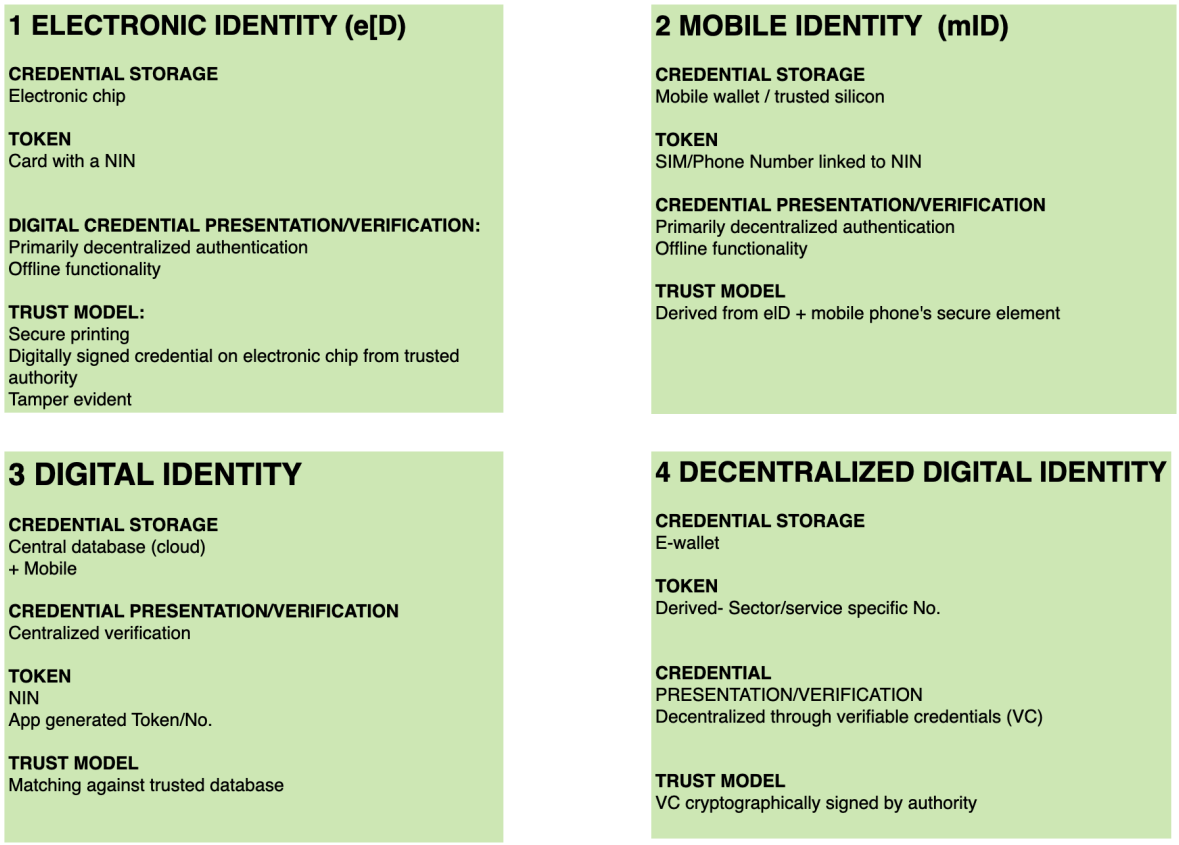



*Figure 3. The four key modern identity platforms today. Adapted from ID4Africa, Plenary Session by Dr. Joseph Atick, Annual General Meeting, Nairobi Kenya, May 2023.*

As of 2023, the available evidence strongly indicates that the U.S. is moving to a mobile ID or mID. The International Standards Organization (ISO) mDL standard provides the harmonized standardization for the model, and the National Institute of Standards and Technology (NIST) has now published its draft *Identity and Access Management Roadmap.* In addition, AAMVA has published its *Mobile Driver's License (mDL) Implementation Guidelines.* It is probable that these foundational standards and initial implementation roadmaps plus adoption by populous states such as California, Texas, Florida, and New York will provide the core impetus for this model. See Figure 4.

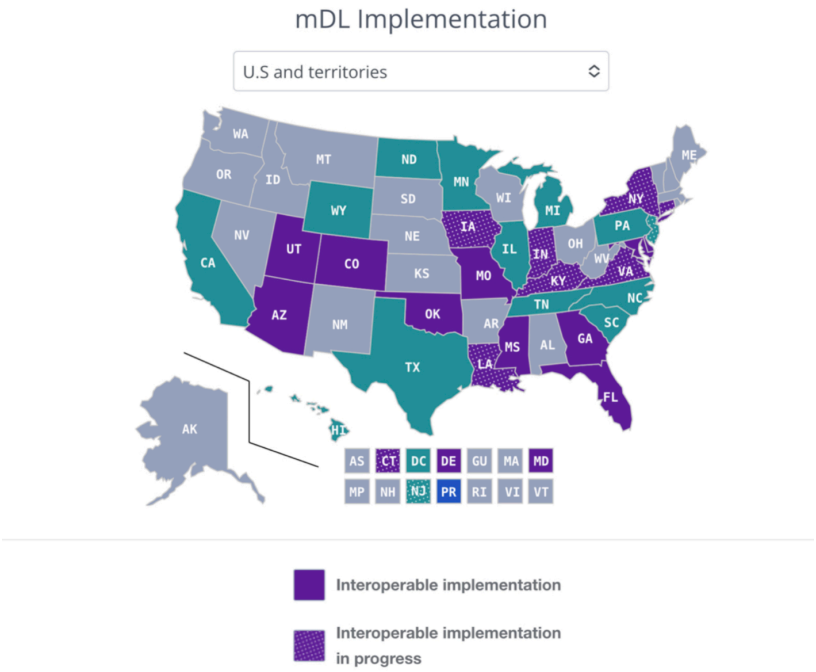



*Figure 4. mDL implementation in the US, as of December 2023.*

However, while the pathway to a particular identity platform looks like it is forming, questions about regarding what this identity platform, when fully adopted, will ultimately look like in terms of financial sector regulation. For example:

- What regulatory entity and which specific rules regulate financial services identity transactions and resolutions in commercial digital wallets?
- What privacy and security protections apply?
- What ultimate authority (or company) determines the validity of the identity?
- Is this identity authority or company regulated? By whom?
- Are identity determinations fair and transparent to the consumer? Is there a standard for the financial services context?

- Is there consumer redress for problems, such as errors and identity theft complications? (Including in mobile financial provisions?)
- What happens to the financial sector information downstream, and what happens to the second, third, and onward uses of this data?

The same kinds of questions apply to mixed consumer-initiated transactions where different types of financial services products may be used at one time, bridging different ecosystems. For example, an individual making a split purchase using a debit card from a traditionally regulated brick-and-mortar-based bank combined with a credit card from a private sector company branded on top of an Internet bank, all mediated through a third party payment website that has just approved the consumer for a separate "Buy Now Pay Later" transaction that splits the bill into four parts. All parties to this transaction will need to resolve consumer identity in some way. In the future, mobile identity may have a part to play in financial sector consumer transaction in addition to other forms of verification and authentication that are already occurring.

In most countries, these kinds of complex transactions will be governed by a government agency, or subagency, with a dedicated identity authority backed by specific regulations for uses of identity in the financial and other sectors. The identity authority would have the ability to provide oversight and enforcement regarding how digital identities would be used across the sectors, and comprehensive privacy law would cover other specific aspects such as sensitive health and financial sector transactions. As a result of interactions with digital identity ecosystems, digital financial transactions come under a variety of regulatory controls, all of which are clearly laid out.

In the U.S., however, such a system of identity-specific regulation with corresponding sectoral guidance and dedicated identity authorities to assist with interpretation and enforcement does not exist. This creates a major gap, and it stands to become much larger. Consider, for example, the analysis of transactions that take place through current mobile digital wallets in the U.S. Depending on the wallet configuration, phone operating system, digital platform or wallet ownership, regulatory status of the entity conducting the transaction(s), downstream parties, and state level regulations (among other factors) — the web of regulatory coverage and regulatory gaps is already confounding.

Figure 5 lays out some very basic regulatory structures that identity-based transactions have to contend with. It is messy, and this figure just posits the basics. There are many additional layers of complexity.

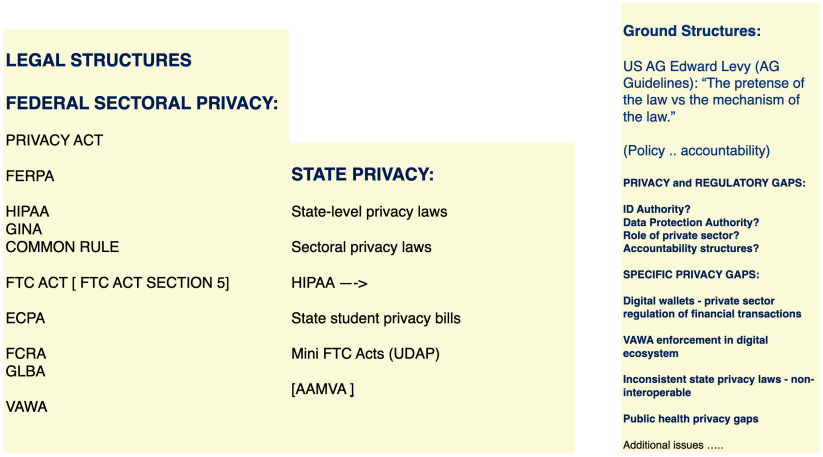



*Figure 5. A simplified overview of legal structures that modern digital identity will need to address in the U.S. context, and "law on the ground structures" that provide the actual day-to-day mechanisms of how the law works in practice.*

In this midst of these complexities, we raise one further issue relating to identity and consumer financial services, and that is data aggregators or data brokers. The World Privacy Forum is concerned about the acquisitions of identity solutions companies that some Consumer Reporting Agencies have made. WPF submitted comments to the CFPB in 2023 which includes information about this topic, which we incorporate by reference here.

## B. Technical developments in the digital financial sector preceded global privacy norms

Technical developments in the digital financial sector largely preceded today's existing heightened global privacy and security norms; these norms are widely acknowledged to have stemmed from European privacy models.[7] There is no question that today, the General Data Protection Regulation (GDPR)[8] and substantially similar national-level legislation in 164 countries and jurisdictions and counting forms a near-worldwide regulatory structure.

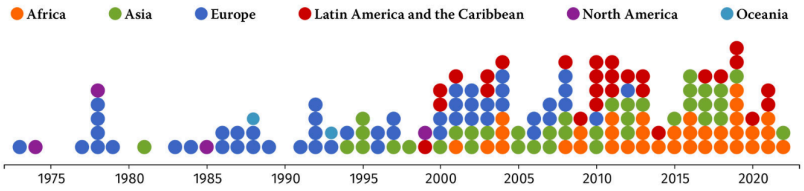
---

[7] For example, an early European-influenced articulation of individual privacy may be seen in OECD's Recommendation on Privacy (the Fair Information Practice Principles) from 1980. A full articulation of the European approach may be seen in Directive 95/46/EC, 1995 O.J. (L 281) 31 and in the current EU General Data Protection Regulation, which dates from 2018.

[8] EU General Data Protection Regulation. Full text: (EU) 2016/679 (GDPR), Full text: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504&qid=1532348683434. The uptake of the GDPR comprises a mature and nearly global regulatory footprint although significant differences in policy and implementation remain.

In Figure 6, WPF's global table of national privacy laws visualizes the slow development of national privacy law over decades, especially since the 1970s. Figure 7 visualizes the defined regional patterns of the passage of such laws. Notably, the U.S. is one of only a few remaining developed countries that have not passed modern comprehensive national privacy legislation that covers the private sector.

Because of this, there exists in the U.S. a substantial gap in consumer privacy protections regarding personal financial data in certain scenarios, especially in the emerging digital financial ecosystem, which is complex and intertwined with certain types of identity data as well as in some cases proprietary digital wallets, apps, and or platforms and services.




(Source: World Privacy Forum. Research: Pam Dixon, Kate Kaye. Data Visualization: John Emerson.)

*Figure 6: Table of Global Privacy Laws (Source: World Privacy Forum, October, 2023. Research: Pam Dixon, Kate Kaye. Data Visualization: John Emerson.)*

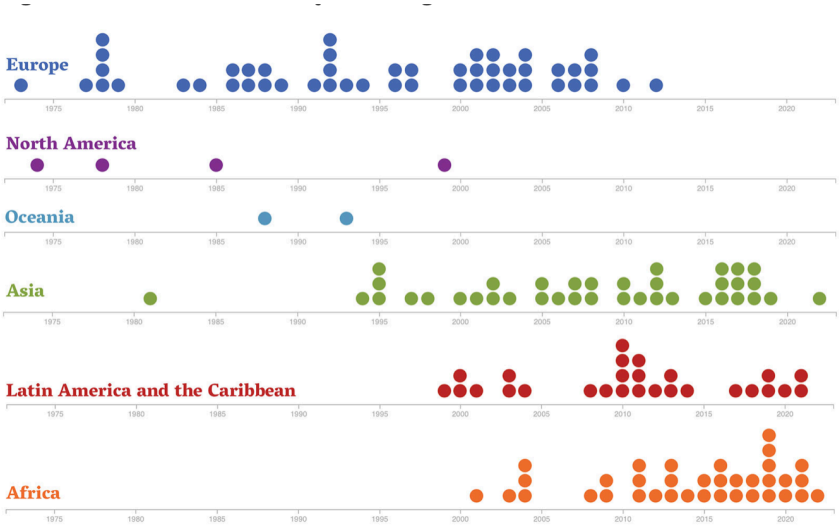



*Figure 7: Table of Global Privacy Laws, Regional Breakout (Source: World Privacy Forum, October 2023. Research: Pam Dixon, Kate Kaye. Data Visualization: John Emerson.)*

To fill privacy the gaps in consumer privacy protections in the U.S., for several years now a growing number of state privacy laws have been passed. This has overall been a positive development. However, it is important to point out that due to a deeply problematic exemption issue, there is a meaningful privacy gap in the financial privacy aspect of most state privacy laws in the US today. It is this gap to which we now turn our attention.

## II. The Role of Gramm-Leach Bliley in the NPRM, and in the U.S. Privacy Landscape

We have two substantive areas of comment in this section. First, regarding the Bureau's approach to security and GLB in the NPRM. Second, the Bureau's approach to privacy and GLB in the NPRM.

### A. The role of Gramm-Leach Bliley in the NPRM regarding security practices

First, we observe with approval the Bureau's approach to security in the NPRM. Specifically, the Bureau seeks to require that all data providers subject to the proposal must comply with the Gramm-Leach-Bliley's (GLB) existing Safeguards Framework. In case that the GLB does not apply to a data provider, then that data provider must

comply with the FTC's Safeguards rule. We understand and fully accept the need for common, uniform security policies and practices that apply to all without duplication or overlap.

Uniformity of rulemaking is fine when the rules themselves are sufficient to achieve their objectives. We agree with the Bureau that existing ***security*** rules meet their objectives and do not need augmentation in this rulemaking. For these reasons, WPF supports the approach the NPRM takes to the construction of the Security provisions.

However, the case for privacy is different, which we discuss at length in the next section.

### B. The role of Gramm-Leach Bliley in the NPRM regarding security practices

A core financial sector privacy problem is that there is a fundamental lack of privacy for consumers in the American financial sector. We acknowledge that the FCRA provides meaningful protections. However, these protections are narrowly crafted for consumer credit reporting, and leave open the larger questions of digital banking, digital wallets, open banking, etc. The law that is supposed to fill this gap is the Gramm-Leach Bliley Act, or GLB.

GLB includes a few minor privacy provisions that offer virtually no meaningful protections for consumers. Yet many legislators and others seem to assume – wrongly in our view – that the privacy protections of GLB are so good that every financial institution subject to regulation by GLB has adequate privacy requirements in place. Although the rulemaking does not state this premise overtly, the CFPB seems to rely on this assumption at least to some degree in this rulemaking.

As evidence of the widespread reliance on GLB to protect consumer privacy needs, we observe that most every state privacy law in the U.S. exempts institutions or data subject to GLB regulation in various ways. Some states have provided "*data* level exemptions" for entities regulated under GLB. In this case, only data regulated by GLB receives an exemption from stronger state privacy law. Other states provide for full "*entity* level exemption" for entities regulated under GLB. Entity-level GLB exemptions from state privacy laws effectively give the entity that is regulated a regulatory pass. So, if a GLB-regulated entity also has a marketing or data broker unit, those data uses and activities would (depending on the construction of the regulatory language), be exempt from the comprehensive state privacy law.

The premise of most laws exempting GLB data or entities from further privacy protections seems to be that additional privacy protections for consumers in the financial sector are unnecessary because GLB is protective enough. We seriously doubt, however, that any state legislator believing this to be true has actually read the privacy provisions of the GLB statute. We suspect that the near-universal acceptance

of that premise is more a testament to the political clout of the financial lobby than to the realities of existing law.

If you examine the privacy language of GLB, you find two provisions for consumers. First, each financial institution must have a privacy notice. At the time of GLB's passage, requiring a privacy notice was a modest step forward. Today, virtually every privacy law around the world includes some form of consumer notice. Notice is a fundamental and completely non-controversial element of privacy at this point, and it is widely perceived as a liability to not have a policy. Therefore, the notice aspect of GLB is fine, but at this point, it primarily provides procedural guidance rather than setting forth a progressive step in consumer financial privacy protection.

Second, GLB requires that a financial institution that wants to share personal information with anyone outside the corporate umbrella ("a non-affiliated third party") must give consumers the chance to "opt-out" under some circumstances. Even if a consumer fails to exercise that opt-out right, the law still usefully prevents sharing of account and credit card numbers for third-party marketing uses.

However, the right to opt-out does not apply to joint marketing agreements with other financial institutions. The result is that if one financial institution wants to share consumer information with another financial institution, it can do so through a joint marketing agreement. In that case, consumers have no opt-out rights. This leaves consumers with a very small island of choice to stand on, which consists of the control on disclosure for non-affiliated third-party sharing. This particular carve-out for consumers is not particularly effective for wide-scale provision of privacy because few consumers read notices and even fewer bother to opt out.

There is not much else in GLB for consumer privacy.[9] There are no limits on data collection. There are no rights of access or amendment. There are no restrictions on use or disclosure. There are no accountability measures. There are no requirements for privacy impact assessments. There is not a requirement that CFPB review privacy impact assessments.

As a result of the absence of meaningful privacy limitations, large financial institutions with multiple lines of business can share consumer data freely with affiliated and potentially unrelated businesses (with a joint marketing agreement in place) without restriction from GLB.

Returning for a moment to the security requirements in GLB, we agree with the Bureau that the GLB security obligations are adequate to the purpose. Security is necessary to privacy, but it is far from sufficient. Security protects financial institutions as much or

---

[9] We note that state privacy laws also typically exempt covered entities (or protected health information) covered by the Health Insurance Portability and Accountability privacy rule. The HIPAA exemption makes much more sense than the GLB exemption because HIPAA offers real and comprehensive privacy protections for patients.

more than it protects consumers. From their beginning, banks always took security measures and evolved those measures over time. Everyone benefits from greater security.

However, the state of financial privacy is, as a result of GLB's limitations, in such a difficult position that there are serious calls from privacy and legal scholars for the *repeal* of GLB privacy provisions in order to improve consumer privacy. Repeal of those provisions would allow the application of stronger state privacy laws to financial institutions.[10] Most of the new comprehensive state consumer privacy laws would give consumers greater privacy protections than they have today. Instead, financial institutions are typically exempted at the data or entity level from meaningful privacy regulation by newer state privacy laws.

In the context of the current rulemaking, the Bureau is clearly aware that there may be gaps in existing law for some third parties covered by the proposed rule: "The CFPB understands that all or most data providers and third parties seeking to access consumer-authorized information are subject to the GLBA"[11] security rules or other security rules.

Even though most of these institutions may be covered by existing security rules, the proposed rule includes an entire section (§ 1033.421) that would impose privacy and security rules on the minority of third parties that may not be financial institutions under GLB and that may not be subject to any state privacy or security law. We applaud the Bureau for taking note of the gaps in existing privacy laws in this manner and for taking action to fill those gaps. The care that the Bureau took in finding and filling gaps is praiseworthy. We largely agree that the proposed rule "will foster a data access framework that is (1) safe, by ensuring third parties are acting on behalf of consumers when accessing their data, including with respect to consumers' privacy interests…"[12]

We urge the Bureau to take the next step and take note that there are larger gaps in current privacy regulation of financial institutions covered by the proposed rule. We ask that the Bureau find a way to apply the privacy protections in proposed § 1033.421(a) through (f) to any financial institution subject to the rule that does not already have similar or overlapping obligations in existing law. These financial institutions are, as we argued above, subject to no existing meaningful privacy law at all. The gap here is huge, and the Bureau can take action to fill that gap. Unless the Bureau acts, a handful of third parties will have privacy rules while the rest of this particular regulatory universe will continue to have no meaningful privacy obligations.

---

[10] See Robert Gellman, *Protect consumer privacy: Repeal GLBA's privacy provisions* (July 2020), https://iapp.org/news/a/protect-consumer-privacy-repeal-the-glbas-privacy-provisions.

[11] 88 Federal Register 74845.

[12] 88 Federal Register 74799

To address any possible contrary existing requirement, the Bureau should adopt the simple rule that the Health Insurance Portability and Accountability Rule includes. Under HIPAA, the federal health privacy rule does not preempt any existing more stringent state law.[13] The HIPAA rule explains what a more stringent state law means in the context of health care, and it would not be difficult to use that model to define what a more stringent state (or other) law means in a financial context.

We hope that the Bureau can find a way to improve privacy across all financial institutions, either in this rulemaking or another.

**III. Targeted marketing**

There are two minor issues that we want to raise. First, in §1033.421(a)(2)(ii), the proposed rule essentially prohibits the use of consumer data for "targeted marketing." We support that provision, but we do not think that the idea of targeted marketing is clear enough.

Targeted marketing is typically based on personal characteristics of the individual who sees the ad, or perhaps even identifiable information. Thus, the advertiser may know a range of information, from personal data, to less identifiable generic data that the recipient is a 47-year-old male who owns a house and likes baseball.

But ever-evolving alternatives to targeted marketing are emerging– contextual marketing, for example, may also rely on known information about an individual. The known information may be that the recipient of the ad is a user of a particular platform providing a service that the individual uses. It is not clear whether that ad is targeted or not.
Another evolving alternative to traditional digital targeted marketing is marketing using advanced analytics techniques, including AI, which do not require precise identification of an individual to create precise marketing profiles and targeting. Data can in fact be targeted even when in an encrypted state, which may in effect nullify targeted marketing rules written with other forms of targeting in mind. Unless the rule (or the accompanying commentary) explains just what constitutes targeted marketing, there may be unnecessary confusion.

Second, in §1033.421(a)(2)(iii), the proposed rule prohibits the "sale of covered data." We support that provision, but we suggest that the language be broadened to prohibit the "sale, rental, exchange, or other transfer or use of covered data not otherwise authorized under this rule." Data can be provided to (or made available for the use of) a third party in ways that do not constitute a "sale." These items can be readily solved with language-level changes.

[13] See 45 C.F.R. 160.202.

## IV. Poverty and digital financial services

Poverty does not need to be a hindrance to inclusion in digital financial services, as can be seen in the India use case. Further, poverty must not be a barrier to the provision of privacy rights. We note that there is not a discussion of poverty in the NPRM, and how CFPB plans to ensure inclusive access to digital financial services as well as privacy to those living in poverty. In the United States, the prevailing discussions about privacy rarely contemplate the poor. Poverty is often perceived as something that the developing world suffers from, not the U.S.[14] Nevertheless, the reality on the ground is that poverty can indeed impact the experience of privacy, and can create meaningful negative disparate impacts.

Data governance, privacy, and poverty are each in their own right multifactorial, complex issue areas which require nuanced legislative approaches. When these areas intersect, great caution is required, as well as ongoing monitoring of legislative impacts. The ideal is to craft careful laws which are rigorously analyzed so as to not create harms for vulnerable people or groups of people, and that will affirmatively create systemic protections for all people, including those who are economically vulnerable. These laws would then ideally be equally administered, allowing all people an equal possibility of enjoying good compliance and the ability to easily effectuate their rights.

However, an unwelcome pattern is emerging from the data regarding how privacy and poverty intersect; that is, there is a distinct fiscal component to privacy. This can be seen in a number of ways, including in some specific use cases, where geographic areas with more fiscal capacity for implementation of privacy regulations tend to have better privacy practices on the ground. This means in practice that people living in poverty may experience less robust privacy protections in comparison with others who have more financial capacity.

The underlying factors contributing to these challenges are complex. One factor is the high cost of privacy implementation and compliance.[15] It is not surprising that wealthier jurisdictions in the U.S. would tend to have better privacy implementations for federal and state privacy laws. Another contributing factor is that much of the recent privacy legislation in the United States— particularly at the state level — is written without enough attention to the economic vulnerabilities of the people who need legal protections. Far too often, privacy legislation has not paid attention to how the legislation will specifically interact with people living in poverty.

---

[14] Poverty is defined by UNICEF as living in a household that earns less than 50% of the national median. https://www.unicef.org

[15] Aly McDevitt, *CCPA Compliance costs expected to reach $55B,* Compliance Week, January 2020. https://www.complianceweek.com/data-privacy/ccpa-compliance-costs-projected-to-reach-55b/27847.article

Regrettably, the intersection of privacy and poverty is not well studied in part because there is not enough emphasis on requirements for collecting data on the effectiveness of privacy regulations in the United States, leaving regulators and the public blind as to impacts unless independent studies are completed. Even with existing data gaps, however, it is still possible to see the emerging signs from the existing data that especially at the sub-national or state level in the United States, privacy protections do not protect those living in poverty as well as they protect those who are not.

This discussion in these comments is not a comprehensive examination of the topic of privacy and poverty, but rather an introduction to the ways in which this problem is expressing itself in the United States, and how some solutions are already being put forward. Poverty and privacy is a profoundly under-researched area in the United States; WPF urges the Bureau to ensure that as it makes new rules, that it includes documenting this area with qualitative and quantitative data.

WPF has studied and area of privacy and poverty in the United States in depth, and we do have associated data. We acknowledge that our data relates to the implementation of a non-financial sector regulation, however, we include this case study here as privacy and poverty data is very difficult to come by, and there are applications to the financial sector that can be gleaned from this work. This case study relates to FERPA implementation. FERPA stands for the *Family Educational Rights and Privacy Act*.[16] FERPA gives parents and students three key rights:

> **Right of Access (Inspect and Review)**. Parents of students and eligible students have the right to access their educational records held by educational institutions and by State educational agencies.[17]
>
> **Right to Correct Records (Request Amendment(s))**. Parents and eligible students can challenge the content of their educational records and to seek to amend records.
>
> **Right to Restrict Release of Records**. Parents and eligible students can elect to restrict the release of their educational records to third parties, with some exceptions.[18]

---

[16] *The Family Educational Rights and Privacy Act of 1974*, 20 U.S.C §1232g; 34 CFR Part 99.

[17] State educational agencies include, for example entities such as State departments of education, for example, the Virginia Department of Education, or the Montana Office of Public Instruction. For more on State educational agencies' roles, see the Council of Chief State School Officers (CCSSO.) See in particular: *The State Education Agency's Role in Supporting Equitable Student-Centered Learning*, CCSSO, November 10, 2019. Available at: https://ccsso.org/resource-library/state-education-agencys-role-supporting-equitable-student-centered-learning.

[18] Exceptions to the consent restrictions are set out in §99.31, and include 16 specific exceptions where disclosure of student educational records are allowed without consent.

The *right to restrict disclosure* pertains to information known as *directory information*.[19] FERPA protects the sensitive information held in a school record; this data may not be disclosed without prior consent. But schools can still choose to publicly release certain categories of information about students without prior consent. This type of student data is called *directory information.* If a student wants to restrict disclosure of their directory information, they must file a FERPA opt out form.

What constitutes *directory information* does not adhere to a specific national list of data types. Rather, it is decided at the local level because schools have been given broad discretion to designate the categories of information they may disclose or release as *directory information*. The FERPA rules contain a simple test: directory information cannot be considered harmful if it is disclosed, nor can it be considered an invasion of privacy if it is disclosed.

In 2017, the World Privacy Forum set out to study and document FERPA implementations in a cross-section of U.S. public schools. The final report, *Without Consent: An analysis of student directory information practices in U.S. schools, and impacts on privacy*, was four years in its research.[20] The methodology included systematic analysis of more than 5,000 schools in 101 U.S. school districts, and 102 postsecondary schools across the U.S. The sampling of the approximately 5,000 schools represents under 1 percent of the approximately 105,298 educational institutions that are covered under FERPA.

The methodology was carefully balanced to ensure diversity of demographic, geographic, and economic factors. In 2020, after four full passes through the research data set, the data were finalized. The data showed a systemic interaction between poverty and privacy across the U.S. regarding FERPA implementation. One area where the poverty divide could be seen particularly clearly was in a simple FERPA implementation task: was a FERPA opt-out form, which is required to be given to a school to opt out of disclosure of directory information, posted on the school's website? Without ready availability of a FERPA form, opt out becomes very challenging for students and parents.

---

[19] "Schools may disclose, without consent, 'directory' information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. **The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school**." [*Emphasis added*] US Department of Education, Family Compliance Office Home, *Family Rights and Privacy Act*, Available at: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[20] Pam Dixon, Bob Gellman, John Emerson, *Without Consent: An analysis of student directory information practices in U.S. schools, and impacts on privacy.* World Privacy Forum, 15 April 2020. https://www.worldprivacyforum.org/2020/04/without-consent/

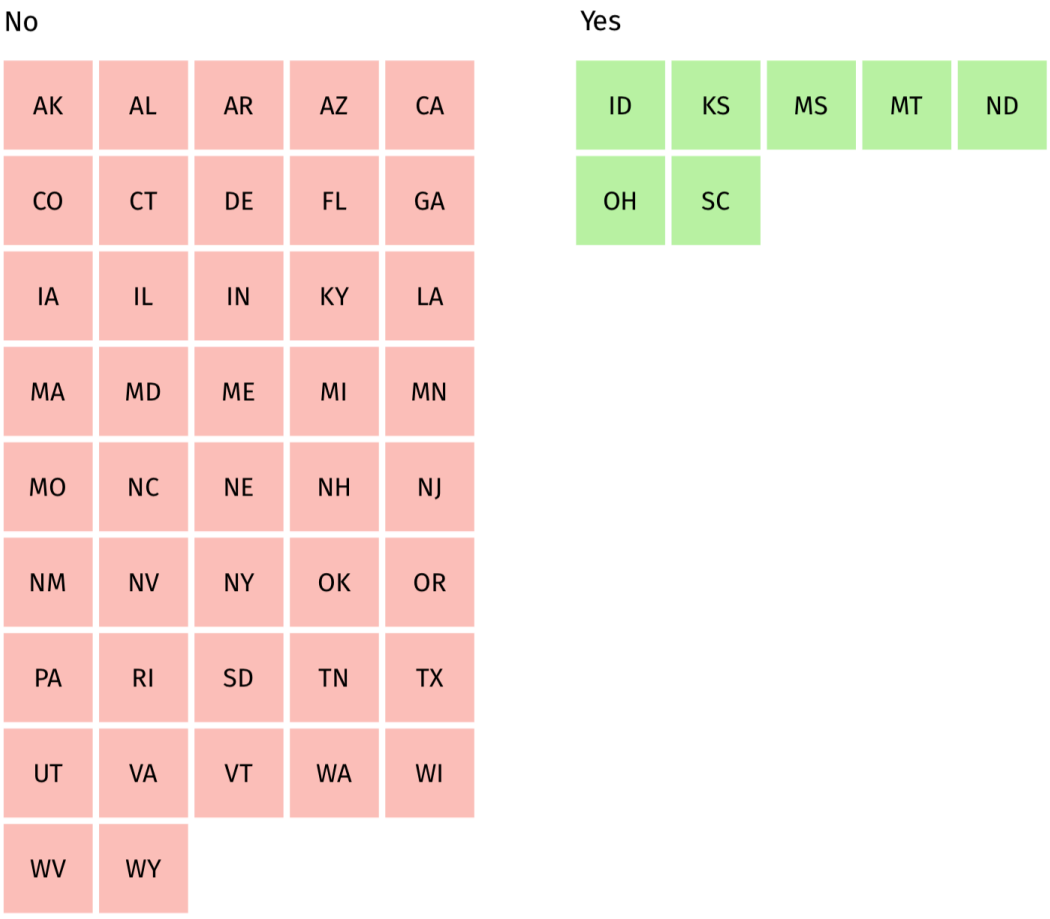
**At the primary / secondary district level, aggregate, the research found that:**

- **13.8 percent** of **rural** school districts posted FERPA opt out forms online at the school district level.

The rural school districts were statistically among the poorer school districts studied. The 13.8 percent figure is extremely low. Less than 14 percent of rural schools studied offered a FERPA opt out online.

**Primary / Secondary School Districts: Is the Is the FERPA opt out form available on the school district web site?**

Rural School Districts

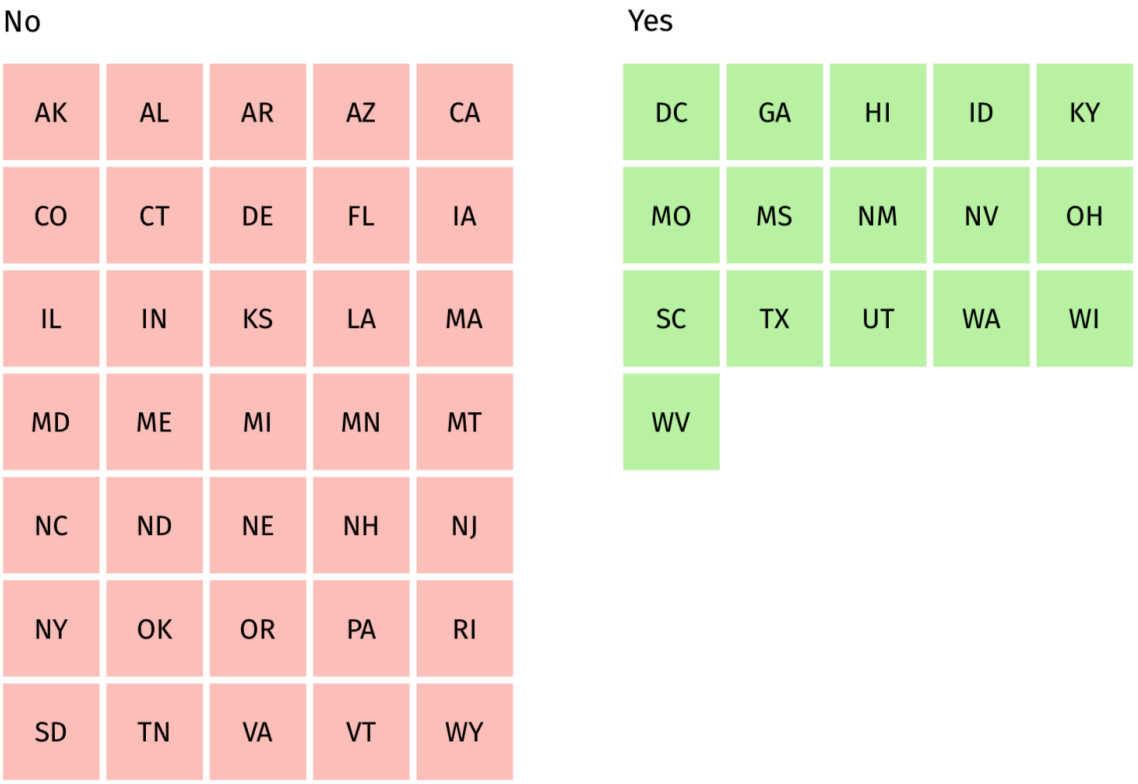



- **31 percent** of **urban** school districts posted FERPA opt out forms online at the school district level.

The urban school districts were statistically among the wealthier school districts studied. The 31 percent figure is still low, but shows significant improvements from the rural schools in aggregate.

**Primary / Secondary School Districts: Is the Is the FERPA opt out form available on the school district web site?**

Urban School Districts




The overall study and findings were extensive, but this particular set of data was particularly illustrative of the "FERPA poverty divide."

Much of today's work around state level student privacy legislation has focused on platforms and technology vendors.[21] This is fine, but the basics of facilitating better FERPA implementation has been ignored, in part because there are data gaps. The *Without Consent* report was the first major report to document FERPA directory information practices as they intersected with privacy across U.S. schools. The data

[21] *Education Bill Tracking,* National Conference of State Legislatures, https://www.ncsl.org/research/education/education-bill-tracking-database.aspx

shows us that some very simple legislative tweaks could help these students. For example, legislation that requires school to post FERPA opt out forms online would be helpful to students. Some of the other options the research found included some schools requiring parents and older students to write their own opt out letter.[22] The likelihood of parents and students writing an opt-out letter from scratch is quite low. Having the simple provision of a FERPA opt out available online at all times would help.

It is important that legislators and others interested in privacy understand that people — and children — living in poverty need specific consideration as privacy laws are crafted. Fortunately, there are organizations who systematically and rigorously study and document poverty in the United States, including child poverty. The American Institutes for Research documented in its report, *America's Youngest Outcasts: A report card on child homelessness*, that 1 in 30 children are homeless in the United States.[23] Other research has put this number closer to 1 in 16 as of 2018.[24] In a 2022 report, UNICEF has stated that child poverty is growing at a record pace.[25] The U.S. Census Bureau's *Supplemental Poverty Measure* tracks poverty in detail across the U.S.[26] The data shows unambiguously that poverty, including child poverty, is not an imagined condition. Children and people who live in poverty deserve to be considered in legislative discussions with much more intention, and with more federal, state, county, and municipal-level data to document where there are greater potentials for disparate impacts.

Of the data the World Privacy Forum studied for its *Without Consent* report, by far the most troubling came from the National Center for Education Statistics, which tracks, among other statistics, homelessness and its impacts on the education of children. Very young students — those in Kindergarten, 1st, 2nd, and 3rd grades — are among those who experience homelessness. Out of 1,351,120 homeless students in the U.S. in 2016-2017, fully 460,937 of these students were in grades K-3. [27] Parents of these students will be the ones who have to exercise FERPA rights. People who live in poverty have equal privacy rights under FERPA and other laws, and both deserve and need assistance and consideration in effectuating those rights.

---

[22] *Without Consent*, p. 104.

[23] *America's Youngest Outcasts: A report on child homelessness,* AIR, November 2014. https://www.air.org/resource/report/americas-youngest-outcasts-report-card-child-homelessness

[24] PovertyUSA. https://www.povertyusa.org/facts

[25] *Prospects for Children in 2022*, UNICEF. https://www.unicef.org/globalinsight/media/2471/file/UNICEF-Global-Insight-Prospects-for-Children-Global-Outlook-2022.pdf

[26] *Supplemental Poverty Measure,* U.S. Census Bureau, https://www.census.gov/topics/income-poverty/supplemental-poverty-measure.html

[27] *Digest of Education Statistics*, NCES. Available at: https://nces.ed.gov/programs/digest/d18/tables/dt18_204.75a.asp.

**Other intersectional work on privacy and poverty**

CGAP, the Consultative Group to Assist the Poor,[28] focuses on poverty, most often in developing countries. David Medine, a respected privacy expert and scholar, created a body of pioneering work on privacy and poverty during his tenure at CGAP, which concluded in 2020. Of this work, arguably among the most important is his work on consent, and how it does not protect privacy in the context of poverty. In his report, *Beyond Consent: Why new approaches to data protection and privacy are needed*,[29] Medine discusses the Western consent-driven model, and compares it with a model that provides systemic privacy protections that do not rely on consent. In his summary of the problem, he writes:

> As digital financial services gain popularity in developing countries, more and more governments are working on data protection and privacy legislation. But there's a problem. Most of the laws under consideration rely on consumer consent as a basic cornerstone, a model that clearly is insufficient to protect consumer rights in today's highly complex world where data is mined, monetized and resold. It's time to consider a new data paradigm, one that puts more responsibility onto the service providers instead of consumers.[30]

In a further article, Medine notes that limiting data to legitimate purposes, establishing a fiduciary relationship between providers and consumers, and appointing learned intermediaries to help consumers are more systemic approaches that would build privacy into data flows. In suggesting limiting data to legitimate purposes, Medine adds a particularly important systemic element.[31]

**The need for measurement of effectiveness of privacy laws in the poverty context**

The entire point of this digression into education privacy has been to provide a factual basis for the intersection between poverty and privacy. Other intersections exist, including in the financial sector. However, in the United States, there is a lack of metrics regarding privacy laws in general, but in particular, there is scant data regarding poverty and privacy. This includes data about the effectiveness of privacy laws as they

---

[28] CGAP https://www.cgap.org

[29] David Medine, *Beyond Consent: Why New Approaches to Data Protection and Privacy for the Digital Age Are Needed*. CGAP, Webinar. 13 June 2019.

[30] *Id.*

[31] David Medine, Gayatri Murthi. *Three data protection principles that go beyond consent,* CGAP, 7 January 2019. https://www.cgap.org/blog/3-data-protection-approaches-go-beyond-consent

impact the poor, including children. It is remarkable to truly understand this lack of measurement. Compare the lack of metrics regarding privacy regulation impacts to those metrics regarding the impacts of face recognition systems. In the area of face recognition systems, NIST undertook a rigorous 2-year study of vendors' algorithms to study algorithmic bias, which NIST called "demographic effects."[32] NIST indeed found meaningful evidence of problems. If NIST had not conducted this important study, the public would not have the empirical data to back up claims of a variety of perceived problems with face recognition systems. The NIST study has caused significant impetus for new regulations, as well as a push for vendor improvements.[33]

Due to the lack of metrics, studies, and robust data regarding the practical functioning effectiveness of privacy statutes, no one really knows for sure what privacy laws are having which specific consequences on consumers living in poverty. WPF requests that the Bureau use its considerable knowledge base to conduct the same kind of study regarding GLB that WPF conducted regarding FERPA. Privacy laws already on the books need to undergo rigorous testing and measurement as implemented, as well as analyses that inform the public if the laws are ineffectual for the poor, or if there is a disparate impact.

**What policymakers need to do to create improvements in the privacy - regulatory intersection**

No regulation will provide perfection. But we can all do better. WPF respectfully suggests the following ideas for your consideration:

- Policies must address root issues. *Will this regulation work for the poorest constituents?* The development of any privacy interventions should only be conducted with the presence of those living in poverty (or who have lived in poverty ) as stakeholders.
- Ensure that the effectiveness of privacy legislation is measured and studied in an ongoing manner. Results should be published publicly.
- Civil society's role and voice needs to be strengthened in multistakeholder and regulatory processes.
- Rigorous studies that provide empirical data regarding the many unknowns about what kinds of privacy solutions are effective / ineffective / neutral for those living in poverty need to be undertaken.
- Privacy laws that rely on consent as a primary basis for privacy protection need to be analyzed for utility in all contexts and other options that create more systemic protections should be considered.

---

[32] Patrick Grother, Mei Ngan. *FVRT: Demographic Effects*, NIST, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[33] *United States: Biometric Laws and Pending Legislation Bill Tracker,* Mondaq. May 2021. https://www.mondaq.com/unitedstates/privacy-protection/1068486/us-biometric-laws-pending-legislation-tracker. For vendor improvements discussions, see generally the Biometric Institute, http://www.biometricsinstitute.org.

- Codes of conduct to implement legislation should be considered. (Voluntary consensus standards, using the OMB A-119 standard,[34] which ensures fair procedures and non-dominance of any one stakeholder.) Poverty experts, consumers, poverty advocates, and other key poverty stakeholders must be at the table.

It is important to acknowledge that privacy protections as they exist today may not be serving people living in poverty. To move beyond this, it will require extensive and ongoing work to begin measuring privacy impacts on the poor. Changes in legislative approaches are also necessary. But it will be very difficult to make progress without first documenting what precisely the problems are. To assist with this, at the very least, each state should establish a commission to study privacy and poverty at the state, county, and municipal levels.

Poverty is an issue for the developing world; it is also an issue here, in the U.S. It is appalling that there are more than one million homeless students in the U.S., and that nearly half of these students are in grades K-3.[35] People who live in poverty have equal privacy rights under U.S. privacy laws, from FERPA to other regulations such as GLB. It is essential that these laws are not just laws on the books, but vibrant law "on the ground" that effectuates meaningful privacy for all people. But to know if they work, we have to talk to the people they are intended to protect.

We note again that GLB does not assist much here, and even where it offers assistance, it is often a challenge for consumers to find the time or know about how to effectuate a GLB opt out. GLB is not an adequate solo vehicle for consumer privacy protections in digital financial services. We further posit that poverty and inclusion need to be taken into consideration more clearly in this NPRM.

The World Privacy Forum again thanks the Bureau for this opportunity to comment on the proposed rule. We understand that we have cast our net across multiple topics; it is our hope that this information proves helpful. WPF stands ready to assist.

Respectfully submitted,

Pam Dixon
Executive Director, World Privacy Forum

---

[34] Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, OMB Circular A-119, https://obamawhitehouse.archives.gov/omb/circulars_a119

[35] *Digest of Education Statistics*, NCES. Available at: https://nces.ed.gov/programs/digest/d18/tables/dt18_204.75a.asp.