



# Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information

---

*Testimony of*


Morgan Reed  
President  
ACT | The App Association

*Before the*

U.S. House of Representatives  
Committee on Energy and Commerce  
Subcommittee on Innovation, Data, and Commerce



1401 K Street NW  
Suite 501

 202.331.2130

 [www.ACTonline.org](http://www.ACTonline.org)

 @ACTonline

 /ACTonline.org

# I. Introduction

We applaud this Subcommittee for holding today’s hearing to examine the privacy risks—and the vast benefits—of activities involving the collection and processing of consumer data adjacent to the sector-specific federal privacy frameworks. Small businesses in the app economy lead the way in solving problems and protecting privacy in these areas.

ACT | The App Association is a global trade group for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. Today, the App Association represents an ecosystem valued at approximately \$1.8 trillion and supports 6 million American jobs. Our members propel the data-driven evolution of these industries and compete against larger firms in a variety of ways, including on privacy and security protections.

Policymakers are appropriately curious and concerned about the privacy and security implications of data collection and processing around the edges of the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA), and Family Educational Rights and Privacy Act (FERPA). Given that the United States lacks an overarching, comprehensive privacy framework, the gaps between what consumers see as “health,” “finance,” and “education” are real. At the same time, this Subcommittee has also acknowledged that digital health, financial technologies (FinTech), and digital education tools provide expanded access to higher quality, more cost-effective services across these critical industries. The activity taking place in the penumbras around these silos is some of the most dynamic and beneficial economic activity the world has to offer, but the privacy and security sensitivities are also accordingly higher. They are the best reason for Congress to enhance federal privacy protections.

The layered applicability of the Federal Trade Commission (FTC) Act, FERPA, and HIPAA to real-life economic activity is deceptively complex. A comprehensive, risk-based privacy framework—like the American Data Privacy and Protection Act (ADPPA, H.R. 8152, 117th)—is the best option before Congress to clarify these complications, better protect consumers in and between the penumbras around federal privacy silos, and advance American digital economy competitiveness on the global stage.

We recommend Congress take the following into consideration as the Subcommittee continues its legislative work on comprehensive privacy legislation:

1. Simply “expanding” HIPAA is a non-starter.
  - HIPAA is an interoperability regime, designed for an incredibly narrow set of “covered entities” providing healthcare services to patients. Expanding that list to all entities processing data with any connection to health—like grocery stores—would

turn the Department of Health and Human Services (HHS) and its sub-agency, the Office of Civil Rights (OCR), into a second FTC, but one with a staff of 72 already overseeing 6,000 annual complaints and convert much of the economy into an interoperable system required to maintain data for audit purposes.

2. Financial services go beyond GLBA and need a risk-based framework to better empower consumers.

- Like HIPAA, GLBA applies to a narrow, already-defined group of entities. But unlike HIPAA, GLBA currently lacks consumer data access requirements. The outcome is that the GLBA silo sometimes traps financial information, making it more difficult for consumers to understand and control their information. A risk-based framework can make it clear to the industry what can be done and spur innovation.

3. FERPA overlaps with the FTC Act and its child privacy requirements, resulting in uncertainty for parents, commercial industries, and educational institutions alike.

- Instead of augmenting the risks these overlaps present by imposing age verification requirements or increasing data collection with a “constructive knowledge” threshold, a federal privacy law should modernize verifiable parental consent (VPC) requirements currently in place.

## II. Health Insurance Portability and Accountability Act (HIPAA)

*HIPAA Background.* HIPAA and its concomitant Privacy Rule is one of the most misquoted or at least most misinterpreted laws on the books. Contrary to popular punditry, HIPAA is an interoperability regime, designed to help insurers, providers, and patients have access to electronic health records and support interoperability. Of course, Congress understood that enabling easier portability would create privacy concerns, but the “how” and “why” was left open so that Congress might pass a more comprehensive privacy law to deal with the issues. Specifically, when HIPAA first passed, it did not specify the kinds of privacy or security requirements the OCR should impose. Instead, the HIPAA statute included a “shot clock” provision implicitly authorizing what eventually became the Privacy Rule and the Security Rule, if Congress failed to authorize them directly within three years after HIPAA’s initial enactment (by August of 1999).<sup>1</sup> That provision required OCR to send a report to Congress in 1997 with recommendations on how legislation governing health information privacy should look. Preemptively addressing future legislative gridlock, the statute further provided that, “If legislation governing standards with respect to the privacy

---

<sup>1</sup> Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, Sec. 264, available at <https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>.

of individually identifiable health information . . . is not enacted by the date that is 36 months after the date of enactment of this Act, the Secretary . . . shall promulgate final regulations containing such standards.”<sup>2</sup> OCR finalized the Privacy Rule and Security Rule in 2003.

Congress should not defer entirely to agency rules like this again.

*Scope and summary of HIPAA.* HIPAA applies to two classes of entity: covered entities (CEs) and their business associates (BAs). Similar to the General Data Protection Regulation’s (GDPR’s) classification of “controllers” and “processors,” HIPAA directly applies to the “controller” analogue, CEs (health plans, providers that process insurance claims electronically, and clearing houses). This aspect of HIPAA’s scope is notable. Most consumers would be surprised to know that the main touchstone for HIPAA’s applicability to their health services is whether the provider processes insurance claims electronically. The “processors” in HIPAA parlance are BAs, which are only BAs to the extent they provide services on behalf of CEs but are liable for compliance with HIPAA via their contracts with CEs. Finally, HIPAA’s provisions apply to CEs’ and BAs’ activities with respect to protected health information (PHI), which includes personally identifiable information (PII) that is created or received by a healthcare provider, among other entities; relates to past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; and that either identifies the individual or “with respect to which there is a reasonable basis to believe the information can be used to identify the individual.”<sup>3</sup> The Privacy Rule generally allows CEs to use or disclose PHI for the purposes of “treatment, payment, and other routine healthcare operations.”<sup>4</sup> With some caveats, the Privacy Rule only allows any other use or disclosure of PHI if the CE obtains the patient’s written “authorization.”<sup>5</sup> Several administrative requirements also apply to CEs, including a requirement to provide individuals with written notices summarizing the Privacy Rule’s provisions and patients’ rights, along with contact information for someone at the CE who can handle privacy complaints and other communications. The Privacy Rule also requires CEs to designate a privacy official to develop and implement its policies and procedures and mandates disclosure—and therefore retention—of PHI for purposes of an OCR audit or investigation. Finally, CEs must obtain written assurance from BAs that they would use PHI only for the purposes permitted or required by contract, and “implement appropriate safeguards to prevent misuse of PHI.”<sup>6</sup>

*The app economy is revolutionizing digital health.* Several App Association members serve patients via BA agreements with CEs. That puts their core activities under the scope of

---

<sup>2</sup> *Id.*, at Sec. 264(c)(1).

<sup>3</sup> 45 C.F.R. Sec. 160.103.

<sup>4</sup> 45 C.F.R. Sec. 164.506.

<sup>5</sup> 45 C.F.R. Sec. 164.508.

<sup>6</sup> CONG. RESEARCH SERV., HIPAA PRIVACY, SECURITY, ENFORCEMENT, AND BREACH NOTIFICATION STANDARDS 6 (updated Apr. 17, 2015), available at <https://crsreports.congress.gov/product/pdf/R/R43991>.

HIPAA. For example, Rimidi provides a remote physiologic monitoring and clinical decision support platform for patients and their caregivers to manage a variety of chronic conditions. Similarly, Podometrics provides a thermometric foot mat enabling caregivers to monitor patients at risk of developing diabetic foot ulcers (DFUs), identifying DFU development up to five weeks before they present clinically and preventing limb amputation. As digital health companies augmenting the caregiving services of healthcare providers, these member companies' activities are subject to HIPAA via BA agreements. Our member companies' digital health tools are only becoming more important for patients, consumers, and caregivers. With the current physician shortage of about 30,000 expected to increase to up to 124,000 by 2034;<sup>7</sup> healthcare costs spiking;<sup>8</sup> the efficacy of sensors and software that collect and analyze physiologic health data improving dramatically;<sup>9</sup> and the pandemic forcing patients to rely more generally on virtual care services, digital health tools are now an important fixture in American healthcare that can augment caregivers' reach and capabilities while controlling costs.

Some of our member companies provide services for clients and customers other than CEs subject to HIPAA, but nonetheless process sensitive PII with some connection to health. For example, App Association member Particle Health allows patients to receive and share their medical information digitally, seamlessly, and affordably. Importantly, Particle Health empowers consumers to make use of their health records both inside of the HIPAA umbrella and outside its borders. Particle Health's role in the digital health ecosystem is simple: Particle is the "Plaid of digital health."<sup>10</sup> If that comparison doesn't ring any bells, Plaid is the company that provides Venmo and other third-party financial services applications the programming interface to securely connect and transfer funds from a consumer's bank account to that specific payment app. Particle wants to serve the same function for digital health records, so that consumers have an easier, privacy-maximizing way to transfer their information from medical institutions to the various applications, platforms, and services they desire. Another company outside the scope of HIPAA, WeStrive, provides personal fitness trainers several digital tools to create programming for clients and monitor their progress. Consumers and trainers should be able to put sensitive health data to work with apps like WeStrive's, knowing that the law provides optimal privacy and security protections. WeStrive should not be thought of as failing to protect PII because bad actors in this space are culpable of privacy abuses,

---

<sup>7</sup> American Assoc. of Medical Colleges, "AAMC Report Reinforces Mounting Physician Shortage," press release (Jun. 11, 2021), available at <https://www.aamc.org/news-insights/press-releases/aamc-report-reinforces-mounting-physician-shortage>.

<sup>8</sup> "Lowering Unaffordable Costs: Legislative Solutions to Increase Transparency and Competition in Health Care," Hearing before the House Committee on Energy and Commerce, Subcommittee on Health, 118th Cong. (Apr. 26, 2023), available at [https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/lyse%20Schuman\\_Witness%20Testimony\\_04.26.23.pdf](https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/lyse%20Schuman_Witness%20Testimony_04.26.23.pdf).

<sup>9</sup> Aisha Malik, "Garmin launches a new FDA-cleared ECG app for the Venu 2 plus," TECHCRUNCH (Jan. 24, 2023), available at <https://techcrunch.com/2023/01/24/garmin-new-fda-cleared-ecg-app-venu-2-plus/>.

<sup>10</sup> See Matt Schwartz, "2020 Vision: Will Congress Have Foresight on Healthcare Privacy?" ACT | THE APP ASSOCIATION BLOG (Jan. 21, 2020), available at <https://actonline.org/2020/01/21/2020-vision-will-congress-have-foresight-on-healthcare-privacy/>.

which reporting sometimes unfairly implies is the case with all digital offerings outside HIPAA. A federal privacy framework would better enable WeStrive to earn consumers' trust.

*Health privacy abhors a vacuum.* Congress' decision in HIPAA to essentially defer entirely to HHS to create a health privacy regime has imposed avoidable costs on patients and would likely impose even greater costs on consumers in the general privacy context. As we noted in a letter to this Committee in 2021,<sup>11</sup> one of the most important reasons for Congress to enact a general privacy law is to enhance patients' privacy and security protections with respect to sensitive PII, especially as they relate to digital health activities outside the HIPAA umbrella. Congress' failure to act poses three related risks on this point: 1) that health privacy abuses are more likely to continue, undermining legitimate digital health offerings and weakening consumer trust; 2) that the FTC will continue to experience pressure to adopt overly expansive interpretations of its authority; and 3) that states will continue to take increasingly divergent approaches to health privacy outside the scope of HIPAA.

Without specifically arming the FTC with the authority to enjoin privacy harms, evidence suggests adverse headlines will continue, although the Commission is making use of its current tools. The FTC's recent consent orders show that it has prioritized punishing privacy and security abuses by digital health companies that may run afoul of FTC Act prohibitions on unfair or deceptive acts or practices. The FTC sought to enjoin health services companies outside the scope of HIPAA from telling their customers that they were not sharing their PII but doing so anyways for advertising purposes. For example, in one complaint, the FTC alleges that a company, "recognizing the sensitivity of this health information, . . . repeatedly promised to keep it private and use it only for non-advertising purposes such as to facilitate consumers' therapy,"<sup>12</sup> but then shared some PII with third parties for advertising. In another case, the FTC alleged that a period tracking app told its users that no PII would be shared with third parties but used software development kits (SDKs) that shared their PII with several advertisers.<sup>13</sup> Advertising and marketing are critical to making digital health tools accessible for consumers and patients, but it is equally important that digital health providers adhere to privacy representations as well as customer expectations.

At the same time, the FTC is also seeking to expand its current tools absent a new privacy law that would enhance penalties and clarify its authority specific to privacy and security. For example, although privacy experts have always distinguished between purposeful disclosures and data breaches, the FTC recently interpreted its Health Breach Notification

---

<sup>11</sup> Letter from Morgan Reed, president, ACT | The App Association, to Hon. Frank Pallone, chairman, House Committee on Energy and Commerce, and Hon. Cathy McMorris Rodgers, Republican leader, House Committee on Energy and Commerce, Re: Fed. Trade Comm'n Settlement with Flo (Feb. 17, 2021).

<sup>12</sup> Fed. Trade Comm'n, *BetterHelp, Inc.*, FTC No. 202316, Complaint (released Mar. 2, 2023), available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/2023169-betterhelp-complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/2023169-betterhelp-complaint.pdf).

<sup>13</sup> Fed. Trade Comm'n, *Flo Health, Inc.*, FTC No. 1923133, Complaint (released Jan. 13, 2021), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc>.

Rule (HBNR) as a privacy rule. As then-Commissioner Wilson noted in a dissent, the statement expansively and awkwardly interprets a few aspects of the rule, including the definition of vendors of “personal health records” (PHRs), to which the rule applies.<sup>14</sup> She argued further that interpretations of a rule that differ in such a way from the text of its provisions typically require an administrative rulemaking procedure so that an agency can consider comments from the public. More fundamentally, the core of the HBNR is a requirement to notify affected consumers in case of a “breach of security,” defined as “acquisition of [PHR identifiable health information] without the authorization of the individual.”<sup>15</sup> There are two problems with applying this rule when a company purposely transfers data to a third party. First, such transfer is generally done under color of authorization by the affected consumer—in other words, the company has (erroneously but deliberately) inferred the consumer’s authorization for its transfer. Characterizing the willful transfer by a company to a third party as a “breach of security”—which typically involves a malicious attack by a third party that thwarts the company’s security measures—is at least an odd fit. The second problem with the interpretation is that it merely requires notice to the consumer for purposely transferring the data, instead of punishing the act of transferring the data. Going forward, a company could potentially comply with the broadly interpreted HBNR by simply notifying consumers after the fact that it has given their health information to Facebook. It could still be liable under Section 5 of the FTC Act as well, and that is the proper *current* law to apply in this scenario. But better than either option would be a privacy law that empowers the Commission to pursue and punish instances of purposeful onward transfer of health PII that is inconsistent with a company’s own representations, the context of its relationship with the affected consumers, or data minimization requirements.

For a few years, states have steadily adopted new comprehensive privacy laws that differ in various ways from each other. However, in the wake of the Supreme Court of the United States’ (SCOTUS’) decision in the *Dobbs v. Jackson Women’s Health Org.*, the gap between state approaches to privacy is widening at an accelerated pace. For example, Washington recently enacted a new consumer health privacy law, the Washington My Health My Data Act,<sup>16</sup> and a few other legislatures like Connecticut’s and Maryland’s are considering similar measures. Despite that legislators mainly sought to protect consumers against investigations into access to reproductive health services that are legal in Washington, the law does not address law enforcers’ access to reproductive health data. Instead, it broadly proscribes collection, processing, or transfer by commercial actors of an exceptionally broad class of information that may relate to an individual’s health. As noted above, even HIPAA allows for the collection, transfer, and processing of PHI for treatment, payment, and other routine operations. The My Health My Data Act prohibits any collection

---

<sup>14</sup> Fed. Trade Comm’n, Policy Stmt. On Breaches by Health Apps and Other Connected Devices, Dissenting Stmt. Of Comm’r Christine S. Wilson, FTC No. P205405 (Sept. 15, 2021), *available at* [https://www.ftc.gov/system/files/documents/public\\_statements/1596356/wilson\\_health\\_apps\\_policy\\_statement\\_dissent\\_combined\\_final.pdf](https://www.ftc.gov/system/files/documents/public_statements/1596356/wilson_health_apps_policy_statement_dissent_combined_final.pdf).

<sup>15</sup> 16 C.F.R. Sec. 318.2(a), 318.3(a).

<sup>16</sup> My Health My Data Act, Wash. House, HB 1155, 68th Leg. (2023).

or transfer of consumer health data, with only two exceptions: 1) with consent of the consumer for “a specified purpose” and 2) to the extent *necessary* to provide a product or service the consumer has requested.<sup>17</sup> The prohibitions in this law appear to restrict WeStrive from improving its product to benefit consumers, or create a new data-driven feature that helps trainers and consumers reach their fitness or health goals. We agree with policymakers that the law should not allow app developers to create profiles on people using their sensitive PII in ways that contravene the context of the relationship they have with consumers or fail to gain their consent. However, only allowing two narrow bases for collection and transfer of consumer health data—including non-health information which can be used to extrapolate health-related information—would limit consumers’ access to digital health tools. The answer to privacy and security risks involving consumer health data should not be to drastically limit consumers’ ability to make use of them and incidentally sweep in non-health digital services in the process. The approach in ADPPA strikes a more reasonable balance that would punish privacy and security harms arising from collection and processing of health information—and impose reasonable data minimization requirements that mitigate unnecessary risks associated with the creation and maintenance of profiles—while allowing for product improvements, context-driven communications, and basic operations.

*Information blocking rules.* As part of the 21st Century Cures Act, Congress required HHS (via its National Coordinator for Health IT Policy or ONC) to prohibit entities subject to HIPAA from blocking a patient’s access to their own protected health information (PHI). The information blocking rules add further pressure on Congress to regulate privacy outside the scope of HIPAA because if they work as intended, they should empower patients to transfer their own PHI outside the HIPAA umbrella. CEs and BAs that collect and process PHI on behalf of patients worry about their own liability for transferring PHI to entities not subject to HIPAA, even at their patients’ request. Entities subject to HIPAA tend to lack a detailed understanding of—and underestimate—the FTC’s and state attorney generals’ (AGs’) enforcement practices regarding health privacy, but their concerns are not unjustified. Despite our Connected Health Initiative’s (CHI’s) suggestion for ONC to require privacy and security attestations by health apps receiving PHI on behalf of patients under the information blocking rules, ONC declined to adopt such a requirement. Requiring health apps and device companies to make those attestations would have equipped consumer protection enforcers with statements that could be matched against the companies’ own conduct, setting up deception claims against companies behaving inconsistently with their representations. But ultimately, attestations would be a stopgap measure until Congress can enact a risk-based general privacy law that would prevent and penalize collection and processing activities involving health information that impose costs in excess of their benefits.

*HIPAA is a bad fit for digital health tools provided directly to consumers.* For example, some of the most important aspects of a general privacy bill are the requirements to respond to various kinds of consumer requests. One such requirement mandates that

---

<sup>17</sup> *Id.*, Sec. 5.



covered companies respond to verified consumer requests to delete PII pertaining to them. Although this protection should be limited by legitimate business or legal interests associated with maintaining PII, it is an important one in the general economy. However, the policy interest in allowing patients to request their healthcare providers to delete health information about them is generally weaker, while the policy interest in blocking such requests is stronger. A patient may want to delete addiction information about themselves in their health records, but that information may save their lives in the future. Thus, a central aspect of a strong consumer privacy regime probably should not even be a feature of patient privacy as applied to HIPAA CEs and BAs. Specific provisions aside, a regime like HIPAA designed around the patient-provider relationship is not well suited to consumer products. The main purpose of HIPAA is to ensure interoperability between health providers so that a patient can port their health records across providers. Thus, HIPAA is supposed to be a bulwark against the incentive for providers to block access by the patient in order to keep the patient's business, as well as the disincentive to invest anything in making health records accessible or readable by other providers. Consumer-facing products and services with health-related aspects are fundamentally different and appropriately require an approach more along the lines of what this Subcommittee is pursuing taking a risk-based approach to privacy and security protections. For this reason, we strongly support updated language in ADPPA that would clarify that PHI is exempt from ADPPA's requirements.

To the extent Congress wants to intervene to ensure interoperability between digital health services outside of HIPAA, we would recommend cosponsoring and forwarding the Better Interoperability for Devices (BID) Act (H.R. 1557). The BID Act would require the Food and Drug Administration to make recommendations to Congress as to how it could better allow for interoperability between medical devices inside and outside the HIPAA umbrella.

*Federal consumer privacy law must enable healthcare research and necessary processing activities on behalf of consumers.* Comprehensive privacy bills like ADPPA will likely include data minimization provisions. One aspect of the HIPAA framework that is appropriate for digital health tools outside of HIPAA is an allowance for those services to conduct health research and process payments and other healthcare functions on behalf of customers. To the extent federal legislation imposes data minimization restrictions on covered companies, they should appropriately allow for the use of covered data for research, especially "peer-reviewed scientific, historical, or statistical research," that "adheres to all relevant laws" governing such research, as ADPPA provides.<sup>18</sup> It is essential for a comprehensive federal privacy bill not to inadvertently hamstring legitimate medical research that currently benefits consumers and patients.

---

<sup>18</sup> American Data Privacy and Protection Act, Sec. 1(b)(10) (H.R. 8152, 117th Cong.).

### III. Gramm-Leach-Bliley Act (GLBA)

*GLBA Scope.* GLBA applies to “financial institutions,” which the regulation defines as entities engaged in any activity that is “financial in nature,” or is “incidental to such financial activities as described” in the Bank Holding Company Act.<sup>19</sup> The FTC is the primary data security regulator of financial institutions under GLBA, which imposes security requirements, disclosure limits, and transparency requirements. GLBA authorizes two separate rulemakings, the Safeguards Rule (vested solely in the FTC) and the Privacy Rule (which four separate federal agencies maintain and enforce, divided up by entity type).<sup>20</sup> GLBA distinguishes between “consumers” and “customers” of financial institutions. Consumers are individuals who interact with a financial institution, while customers are consumers who have an ongoing relationship with the financial institution.<sup>21</sup> For example, a person who applies for a loan from a financial institution—and therefore submits sensitive, non-public PII—is a consumer; but they only become a customer if they have an ongoing relationship with the financial institution.

*The FinTech app economy.* The app economy activity in and around the scope of GLBA is robust. Our FinTech member companies are solving emerging and long-intractable problems for consumers. For example, Goalsetter provides a financial education platform for children, which allows kids to receive allowance or monetary gifts from friends, parents, and relatives, and/or spend money through the Goalsetter debit card. Another kids’ digital wallet company, REGO, has gone so far as to patent the COPPA compliant opt-in protections in its Mazoola mobile wallet for kids.<sup>22</sup> Both of these FinTech apps put parents in charge and empower kids to learn financial literacy. With studies indicating that just over half of Americans are considered financially literate and only 24 percent of millennials understand basic financial concepts,<sup>23</sup> App Association members and companies like them are leveraging the power of smart devices and platforms to address this issue in privacy-protective ways.

Just as patients sought a remedy for better access to their records through the information blocking rules, concerns about customers’ access to and portability of their financial information have punctuated financial services policy debates. The App Association filed comments on the Consumer Financial Protection Bureau’s (CFPB’s) statutorily required

---

<sup>19</sup> 16 C.F.R. Sec. 314(b); Sec. 314(h)(1).

<sup>20</sup> 16 C.F.R. Sec. 314; 16 C.F.R. Sec. 313.

<sup>21</sup> 16 C.F.R. Sec. 314.2(b); Sec. 314.2(c).

<sup>22</sup> See MAZOOOLA: A KIDS MOBILE WALLET POWERED BY PRIVACY, available at <https://mazoola.co/>.

<sup>23</sup> Kevin P. Chavous, “A Hand Up Or A Handout? Tackling America’s Financial Literacy Crisis,” FORBES (Feb. 3, 2022), available at <https://www.forbes.com/sites/stopaward/2022/02/03/a-hand-up-or-a-handout-can-we-tackle-americas-financial-literacy-crisis/?sh=2258745fe251>.

Section 1033 rulemaking<sup>24</sup> highlighting the need for more meaningful access by customers to their own financial information. As we noted in our letter, “[t]he opportunities for consumers in the open market are enormous. FinTech applications can improve consumer access to credit using data points that traditional lenders overlook; they can allow consumers to budget and receive personalized tips in real time; and they can send consumers sophisticated analytics tailored specifically to them and their goals.”<sup>25</sup>

Unfortunately, “the current data access regime involves a mixture of informal credentials-based access agreements and formalized, token-based access agreements. This system is complicated to navigate for both consumers and third parties and often allows traditional financial institutions to impose their will regardless of consumer welfare.”<sup>26</sup> These unnecessary levels of friction resulted in some FinTech companies playing fast and loose with consumer expectations, opting to “scrape” data from their banking screens in order to populate their apps.<sup>27</sup> Even though this was typically done to effectuate what the developers assumed was their customers’ intent, it never involved actual notification to the consumer and consent, because it was done outside the managed lines of communication and contract. Just as the information blocking rules require electronic health records (EHR) companies to adopt open application programming interfaces (APIs), we also recommended that financial institutions enable safe, secure access—with appropriate data security and privacy guardrails—by customers to their own financial data via open APIs. Having established the overwhelming policy interests in enabling consumers to access their own financial information and transfer it outside the GLBA umbrella, an equally important task is to ensure consumers continue to benefit from optimal privacy and security protections outside the scope of GLBA. The answer must be a federal, risk-based privacy framework.

## IV. Family Educational Rights and Privacy Act (FERPA)

---

<sup>24</sup> Letter from Morgan Reed, president, ACT | The App Ass’n, to Hon. Rohit Chopra, Dir., Consumer Financial Protection Bureau, Re: Comments of ACT The App Association on the Consumer Financial Protection Bureau’s *Request for Information Regarding Consumer Access to Financial Records*, Docket No. CFPB-2016-0048, 81 Fed. Reg. 83806 (Feb. 21, 2023).

<sup>25</sup> *Id.* (citing AITE-NOVARICA, *ALTERNATIVE DATA ACROSS THE LOAN LIFE CYCLE: HOW FINTECH AND OTHER LENDERS USE IT AND WHY*, (2018), available at [https://www.experian.com/assets/consumerinformation/reports/Experian\\_Aite\\_AltDataReport\\_Final\\_120418.pdf?elqTrackId=7714eff9f5204e7ca8517e8966438157&elqaid=3910&elqat=2](https://www.experian.com/assets/consumerinformation/reports/Experian_Aite_AltDataReport_Final_120418.pdf?elqTrackId=7714eff9f5204e7ca8517e8966438157&elqaid=3910&elqat=2); PWC, *GLOBAL FINTECH REPORT 2019: CROSSING THE LINES - HOW FINTECH IS PROPELLING FS AND TMT FIRMS OUT OF THEIR LANES*, (2019), available at <https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2019.pdf>.)

<sup>26</sup> *Id.*

<sup>27</sup> Benjamin Pimentel, “Banks and fintechs agree: It’s time for screen scraping to go. So what’s next?” *PROTOCOL* (Oct. 5, 2021), available at <https://www.protocol.com/fintech/idx-financial-data>.

*Scope of FERPA.* FERPA's scope is not as narrow as it seems, and the gap it leaves is made smaller by the FTC's proactive approach. Similar to HIPAA and GLBA, FERPA also applies primarily to a specific class of entity—educational agencies and institutions—and a subset of personal information, “education records.” The definition of education records, in turn, is tied to whether educational agencies or institutions are directing the processing or collection<sup>28</sup> and includes any information “directly related to a student.” The two pillars of FERPA are 1) a requirement for schools allow parents access and review of their children's education records; and 2) a prohibition on schools from releasing students' education records without written consent of their parents, unless one of several exceptions apply.<sup>29</sup> Notably, FERPA's requirement to allow students' parents to access education records distinguishes it to some extent from other federal privacy silos and from state laws that apply adjacent to the federal laws. Observing shortcomings in the access requirements in GLBA and HIPAA, policymakers have sought to perfect the requirements in those contexts in ways that have not materialized as clearly under FERPA.

Notably, just as the HIPAA Privacy Rule refers to contractual entities working on behalf of CEs as BAs, the U.S. Department of Education's (ED's) rules promulgated under FERPA also create categories analogous to “business associate.” The statutory provisions Congress enacted do not explicitly contemplate third-party companies providing digital education services using education records. However, schools routinely release education records to third-party education services companies—without incurring the requirement to obtain parental consent for disclosure—via the statutory exception allowing schools to provide such records to “school officials.” ED's regulations spell out the relationship more concretely. To qualify for the school officials exception, schools must determine whether a third party “(1) performs an institutional service or function for which the agency or institution would otherwise use employees; (2) is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) is subject to the requirements of Sec. 99.22(a) governing use and redisclosure of personally identifiable information from education records.”<sup>30</sup>

*The app economy is thriving in education technology.* Thinkamigo is an educational app company focused on getting kids excited about writing. Their app, Story Dice, helps give kids ideas for stories, while their apps Lists for Writers and Story Spark help kids lay out their story, build out their characters and plot points, and give them the tools they need to improve their overall writing and story structure. Through contracts with school districts, Thinkamigo provides these tools for students in the school context, which puts their activities under the scope of FERPA. But to the extent that the apps are available to kids and parents directly, COPPA and the FTC Act are the federal laws covering their privacy practices. Another member company, TORSH, provides a platform for teachers'

---

<sup>28</sup> 20 U.S.C. Sec. 1232g(a)(4)(A). Education records are materials that “contain information directly related to a student” and “are maintained by an educational agency or institution or by a person acting for such agency or institution.”

<sup>29</sup> 20 U.S.C. Sec. 1232g(a)(1)(A); 20 U.S.C. Sec. 1232g(b)(1).

<sup>30</sup> 34 C.F.R. Sec. 99.31(a)(1)(i)(B).

professional development, enabling streamlined review, analysis, and management of classroom video clips.<sup>31</sup> The ability for schools to rely on digital tools like TORSH's is critical and increasingly important as we exit the pandemic.

*COPPA applies to entities subject to FERPA.* It is difficult to address FERPA requirements without also covering the FTC Act and one of its subsections, COPPA, which regulates collection of PII about children under 13. There is no explicit carve-out from the FTC Act or COPPA for entities subject to FERPA. In fact, the FTC is adamant that COPPA applies readily to education technology companies, even when they are subject to FERPA via contractual relationships with schools.<sup>32</sup> However, COPPA rules do attempt to account for potential conflicts or incongruities between the two regimes. For example, COPPA's requirement for companies to obtain verifiable parental consent (VPC) prior to collecting PII from children does not apply "to the extent permitted under other provisions of law," (presumably, including FERPA's provisions).<sup>33</sup> This could lead to the two regimes applying slightly unevenly or confusingly, even though there might be good reasons for their overlapping structure, but the FTC has addressed the issue. Under FERPA, schools need not obtain parental consent for disclosing children's education records to educational apps on contract with the school. The FTC has clarified in a frequently asked questions (FAQ) section that an education technology company may rely on "consent obtained from the school under COPPA instead of the parent,"<sup>34</sup> when such collection is for the "use and benefit of the school and for no other commercial purpose."<sup>35</sup> Conversely, if the same children (if they are 12 or younger) sought to use the same educational apps outside the school context, the app must obtain VPC directly from those children's parents.<sup>36</sup> Thus, while the edges around sector-specific privacy laws may seem less regulated, in this case, more regulatory privacy barriers arguably exist under the FTC framework than under the sector-specific law.

The FTC's COPPA guidance for education technology companies emphasizes that students should not have to trade access to digital education services for their privacy.<sup>37</sup> This messaging addresses rapidly developing privacy concerns over the past three years, especially among parents, as the COVID-19 pandemic caused schools to move to a virtual model leaning heavily on digital tools. Parents worried that their children's mandatory use

---

<sup>31</sup> TORSH, POWER PACKED FEATURES DRIVE RESULTS, available at <https://www.torsh.co/features/>.

<sup>32</sup> Fed. Trade Comm'n, Policy Stmt. of the Fed. Trade Comm'n on Education Tech. and the Children's Online Privacy Protection Act (May 19, 2022), available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf) (FTC EdTech Policy Statement).

<sup>33</sup> 16 C.F.R. Sec. 312.5(c)(6)(iv).

<sup>34</sup> Fed. Trade Comm'n, Complying with COPPA: Frequently Asked Questions, N. COPPA AND SCHOOLS, Question N.1, (Jul. 2020), available at <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%20SCHOOLS>.

<sup>35</sup> *Id.*, at N.2.

<sup>36</sup> 15 U.S.C. Sec. 6501(9); Sec. 6502(b)(1)(A)(ii); 16 C.F.R. Sec. 312.5.

<sup>37</sup> FTC EdTech Policy Statement at 4, "Children should not have to needlessly hand over their data and forfeit their privacy in order to do their schoolwork or participate in remote learning, especially given the wide and increasing adoption of ed tech tools."

of those services would expose their children to undue privacy and data security risks, in an environment where no in-person alternative was available. Against this backdrop, the FTC sought to remind consumers and parents that the FTC Act—including COPPA—still applies to education technology companies. Most notably, the FTC reminded education technology companies that COPPA’s prohibitions on 1) conditioning access to a service on a child disclosing more information than is reasonably necessary for the child to participate in an activity; 2) engaging in commercial activities like marketing, advertising, or other commercial activities unrelated to the provision of the school-requested service; 3) retaining PII about a child longer than reasonably necessary to fulfill the reason for which it was collected; and 4) failing to have procedures to maintain the confidentiality, security, and integrity of children’s PII, *still apply* to education technology companies, even when they also comply with FERPA.

The FTC’s and ED’s separate jurisdiction over different kinds of entities help illustrate how they fit together. The FTC has jurisdiction over commercial entities—not schools—while ED has jurisdiction over schools receiving federal education funds. Thus, ED’s enforcement mechanism is limited to punishing schools—not education technology companies directly—by withholding their federal education funds. Similarly, the FTC Act does not authorize the FTC to enjoin schools from activities that result in consumer harm related to privacy and security. Where ED’s jurisdictional limits suggest a gap in protections may exist, the FTC’s guidance and policy statements make a strong case that federal privacy enforcers are holding education technology companies and schools accountable for privacy and security practices. Nonetheless, we have two suggestions as you consider updates to the FTC Act when it comes to children’s and students’ privacy:

1. Any amendments to or expansion of COPPA’s protections to cover children up to 17 years old **should also modernize VPC requirements**. We have written extensively about the issues VPC present by shifting the onus for privacy protections to parents and consumers rather than companies providing services.<sup>38</sup> Expecting parents to provide credit card information, driver’s license scans, or to call a 1-800 number to verify their identity for each online service with which their children interact is asking a great deal of today’s parents. As the FTC itself has alluded to, parents now have little choice but to enable their children to make beneficial use of digital services. Requiring multiple redundant copies of their PII to exist in all corners of the internet their children may need to venture becomes a less workable concept with each passing day.
2. Any general consumer privacy legislation addressing kids’ **privacy should avoid imposing age verification requirements or requirements that would require similar levels of data collection** to “verify” or “assure” a child’s identity for age verification

---

<sup>38</sup> Letter from Morgan Reed, president, ACT | The App Association, to Hon. Maria Cantwell, chair, Senate Committee on Commerce, Science, and Transportation, and Hon. Ted Cruz, ranking member, Senate Committee on Commerce, Science, and Transportation, Re: Feedback/suggestions for improvement regarding the Kids Online Safety Act (KOSA) (S. 3663, 117th), available at <https://actonline.org/wp-content/uploads/2023-03-01-ACT-KOSA-letter-Senate-Commerce-and-Sponsors-FINAL.pdf>.

purposes. Similar to the issue described above, requiring detailed PII profiles on children to exist in multiple parts of the ecosystem with every company providing services a child may access introduces more serious privacy and security risks than are necessary. In fact, such requirements may conflict with other privacy provisions of a federal bill, especially those that apply to more sensitive classes of information like biometric indicators.<sup>39</sup> We also discussed this in testimony last year in the context of a privacy bill possibly moving COPPA to a “constructive knowledge” regime, which would require covered companies to compile much more granular profiles on children.<sup>40</sup>

## V. Conclusion

Each of the federal privacy silos that exist today present unique challenges for this Subcommittee to consider as you continue to work on a comprehensive privacy bill. Although COPPA applies to entities covered by FERPA, and the FTC Act overlays HIPAA, the sector-specific laws apply more narrowly than is often appreciated, causing gaps to appear wider than they are. As is often the case, the truth about activity around the federal privacy silos is both less shocking and more interesting than it appears at first glance. These market activities happen to be some of the most important areas for consumers and job creation in the United States and are therefore worth preserving and strengthening with a federal data privacy and security law. We look forward to continuing to work with this Subcommittee on federal privacy reform in the 118th Congress.

---

<sup>39</sup> Eric Goldman, “Do Mandatory Age Verification Laws Conflict with Biometric Privacy Laws? – Kuklinski v. Binance,” TECH. AND MARKETING L. BLOG, Apr. 8, 2023, *available at* <https://blog.ericgoldman.org/archives/2023/04/do-mandatory-age-verification-laws-conflict-with-biometric-privacy-laws-kuklinski-v-binance.htm> (“The invasiveness of [age verification] requirements could overwhelm and functionally moot most other efforts to protect consumer privacy.”).

<sup>40</sup> “Protecting America’s Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security,” Hearing before the House of Representatives Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce (comments of Graham Dufault, sr. dir. for public policy, ACT | The App Association).

# Appendix:

## The App Economy in Your District

### Majority

#### **Chair: Bilirakis, FL-12**

Since 2011, Tampa-based Thinkamingo is a husband-and-wife team working together to build family-friendly, education-focused mobile apps. Their apps range from interactive dice meant to take young writers to inspired storytellers to imagination-driven spy kits complete with virtual disguises, including a voice changer!

#### **Vice Chair: Walberg, MI-05**

Located in Jackson, Lean Rocket Lab is a coworking space and accelerator supporting businesses of all types by providing office space, education, mentorship, and pathways to funding for companies in a variety of industries. Their Manutech Incubator program and i4.0 Accelerators focus on startups creating devices and the software that powers them in manufacturing, transportation, data analytics, healthcare, and more.

#### **Bucshon, IN-08**

Located in Evansville and founded in 2016, anu is working to help people grow their own food through technology in order to create a more sustainable world and allow people to increase their food independence. With 11 employees, anu is building hydroponic farming systems that can grow anything from lettuce and other vegetables to any number of fruits or spices.

#### **Duncan, SC-03**

Topography Digital is a full-service software development company that focuses on providing services for small and medium-sized companies across industries looking to build or grow their digital presence or offerings. Their services include web and app development, drone programming, and cloud optimization.

#### **Dunn, FL-02**

TechFarms, founded in 2015 and located in Panama City Beach, has a singular mission: create a more technology-focused and vibrant entrepreneurial ecosystem in northwestern Florida. The team at TechFarms has created a collaborative coworking space for local business owners with the goal of lifting up the whole community.

#### **Lesko, AZ-08**

Founded in 2019, LiteraSeed is an early-stage digital health startup creating a visual way for patients to share their symptoms with their doctors. The product, called a “visual symptom report,” focuses on helping those patients whose first language is not English and those with lower literacy levels to communicate with their doctors and better understand their medical records.



**Pence, IN-06**

Located in Muncie and founded in 1987, Accutech provides software solutions and services to those in the financial industry. Accutech's solutions include a wealth management platform, mobile applications that make opening an account easy, as well as a business intelligence dashboard.

**Armstrong, ND-At Large**

North Dakota-based Bushel built a digital ecosystem that powers APIs, apps, websites, and digital payment solutions to support agribusinesses and build digital infrastructure for the agriculture industry. Supporting more than 2,000 grain facilities with 40% grain origination in the United States and Canada, the Bushel platform strengthens relationships between grain processing facilities and farmers by enabling both to complete transactions quickly, safeguard important data, share information faster, and create a more complete picture of businesses.

**Allen, GA-12**

Zapata Technology is a veteran-owned Augusta-based cybersecurity company that provides critical cyber-secure infrastructure for the defense industry. Their products, offered globally, support persons in active duty with cybersecurity penetration testing, cloud computing and analytics, systems engineering and data integration, and custom software development.

**Fulcher, ID-01**

Located in Coer d'Alene, Chief Architect Software provides automated residential home design and interior decorating software for architects, builders, and designers. Through their suite of software products, industry professionals can create construction drawings and floor plans, get 3D renderings of interior spaces and elevations, and 360-degree panoramic renderings of whole buildings to better understand and craft design schemes unique to each building project.

**Harshbarger, TN-01**

Located in Kingsport, Code & Color is a digital marketing firm that offers software and design services and helps businesses grow through creative design. Their main services are clustered into marketing, design, websites, and mobile apps.

**Cammack, FL-03**

Founded in 2001, Atmosphere Apps is based in Gainesville and is a custom software development shop that works with clients through the design, development, maintenance, and integrations with other popular technologies. Atmosphere Apps also maintains their client's apps long after development ensuring the apps are always up to date with OS versions and compliance standards. While initially focused on clients in the health sector, Atmosphere is expanding its client base to include sales, media, and travel industries.

**McMorris Rodgers, WA-05**

Founded in 2017, Gestalt is a 31-person team working to bring healthcare into the 21<sup>st</sup> century by replacing microscopes and glass slides with automated, electronic, and digital workflows. They provide services related to pathology in the medical field to professionals as well as those in education or academic research from their HQ in Spokane

## **Minority:**

### **Ranking Member: Schakowsky, IL-09**

The one-woman team at Kidz Learn Applications has been developing iOS and Android mobile apps that provide educational content to children for the past decade. Kidz Learn Applications has developed over 20 apps with lessons ranging from math to vocabulary and even created a guide for educational, kid-friendly places in New York City for a day of fun for kids and adults alike.

### **Castor, FL-14**

Located in Tampa nearly 200 employees, Accusoft, originally founded as Pegasus Imaging Corporation in 1991, focuses primarily on content processing through image and document cleanup while providing APIs and barcode collection through mobile apps. They also provide digital conversion tools that turn paper document and paper-based processes (often found in legal, financial, and health transactions) into customized digital processes based on each client's unique needs.

### **Dingell, MI-06**

Founded in 2017 and headquartered in Kalamazoo, with two other offices in the state, SPARK Business Works is a custom software development and design firm. They help businesses of any size create an effective online presence that aims to improve each client's unique needs for the connected customer experience.

### **Kelly, IL-02**

Based in Kankakee and founded in 2020, Pathfinder is a full-service creative marketing agency that helps their clients tell stories through web and mobile solutions. With 24 currently employed, their offerings include web development, graphic design, photography, and other digital marketing offerings.

### **Blunt Rochester, DE**

Located in Wilmington, MightyCall is a cloud-based communications and customer service platform founded in 2013. Their virtual phone system is designed specifically for small businesses and remote teams making it easy for teams to connect from anywhere through mobile and desktop apps. Their apps provide unique features like call availability windows, scheduling services, and the ability to mask personal cell numbers, given that privacy is a core pillar of MightyCall's service.

### **Soto, FL-09**

Originally founded as "Yelling Across Cubicles"—because it was essentially built as a digital walkie-talkie to be used in the workplace—Yac was founded in 2019 in Kissimmee. Since then, Yac has grown to include other functionalities including asynchronous meetings, voice messages, screen sharing and shareable links, all focused on making remote work more collaborative.

### **Trahan, MA-03**

Founded in 1997 and located in Maynard, Fisheye Software focuses on building enterprise-level software that makes complex systems easier to understand. They provide services to a number of clients, both in the government and commercial systems, contributing to anything from data archiving to air traffic control or missile defense systems.

**Clarke, NY-09**

Since Stellar Health's founding in 2018, this Manhattan-based healthcare technology company has rapidly grown to over 200 employees and is providing connected health solutions to patients everywhere. Stellar Health helps deliver providers targeted recommendations to enable "value-based" improvements to care and financial performance to hospitals. This means that through Stellar Health's services, patients receive care faster and at a lower cost throughout the care chain.

**Pallone, NJ-06**

DealerApp Vantage, located in Piscataway, is the nation's leading native mobile app development company that specializes in automotive dealers. They have mobile app solutions aimed to fit all budgets and sizes, from small, single rooftop dealerships to some of the largest auto groups in the United States.