epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

February 27, 2023

The Honorable Patrick McHenry, Chair
The Honorable Maxine Waters, Ranking Member
U.S. House Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

Dear Chair McHenry and Ranking Member Waters:

We write to you regarding tomorrow's markup of the Data Privacy Act of 2023 proposed by Chairman McHenry.[1] EPIC appreciates your attention to the need for improved privacy protections in the financial services sector. However, this bill's reliance on an outdated system of notice-and-choice does not meaningfully protect privacy and is out of step with recent developments in privacy legislation.

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC is a leading advocate for consumer privacy, including in the financial sector, and has appeared before this Committee on several occasions.[3]

The Bill's Focus on "Notice and Choice" is Outdated

The Data Privacy Act unfortunately relies on an outdated system that does little to protect privacy by extending the notice-and-choice provisions of the Gramm-Leach-Bliley Act (GLBA). GLBA requires financial institutions to provide their customers with privacy notices. This notice-and-choice regime, in which consumers are expected to read extensive privacy policies, makes it impossible for consumers to meaningfully protect their privacy. Even if consumers had the time to read every privacy policy and statement, they would in most cases come away with woefully incomplete information. Such policies tend to be vague and expansive, designed to protect a company from liability rather than inform privacy-conscious consumers.

[1] Amend. in the Nature of a Substitute to H.R.1165, the "Data Privacy Act of 2023," https://docs.house.gov/meetings/BA/BA00/20230228/115381/BILLS-118-HR1165-M001156-Amdt-12.pdf.
[2] EPIC, *About EPIC*, https://epic.org/about/.
[3] *See, e.g, Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing before the Subcomm. on Fin. Inst. and Consumer Credit of the H. Comm. on Fin. Services* (testimony of Marc Rotenberg, EPIC Exec. Dir.) 116th Cong (2018), https://epic.org/documents/examining-the-current-data-security-and-breach-notification-regulatory-regime/; *Examining the EU Safe Harbor Decision and Impacts for Transatl. Data Flows: Hearing before the Subcomm. on Commn'c and Tech. of the H. Comm. on Fin. Services* (testimony of Marc Rotenberg, EPIC Exec. Dir), 114th Cong. (2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf.

Notice and choice simply does not work. We have all received these notices in the mail – a pamphlet from our bank or credit card company explaining all the ways they disclose our data to other entities. Under GLBA, the notice must give consumers the option of opting-out of a limited amount of data sharing. But in reality, very few consumers read these notices or exercise their opt-out option. Even though the Data Privacy Act provides a new deletion right for consumers, this 1) still puts the burden on consumers to protect their privacy; and 2) is not a meaningful right as so few consumers will be aware it exists. The Data Privacy Act assumes that consumers have the time, knowledge, and know-how to read company legalese and exercise their rights. This framework simply hasn't worked.

Rather than move past this outdated notice-and-choice system, the Data Privacy Act simply adds another layer of notice – notice must now be given at the point of collection rather than just at the point of disclosure. This is out of step with the progress made by the House Energy & Commerce Committee last Congress on the American Data Privacy and Protection Act ("ADPPA"). Sponsored by Democratic and Republican leaders on the Committee, ADPPA takes the burden of protecting privacy off the consumer and instead imposes a data minimization standard[4] that requires businesses to limit the collection, use, and retention of personal information to what is reasonably necessary to provide the product or service the consumer has requested.[5] This is very different than the purported "data minimization" provosions of the Data Privacy Act that simply require that institutions limit their collection of personal data for the purposes they list in their "privacy policies" – policies that no one reads. Under this standard, companies would be permitted to collect and use data for purposes that are not consistent with what a reasonable consumer would expect, so long as they disclose the purpose and get consent. This gives incredible leeway to companies to determine the purposes for which they can collect data.

On the contrary, ADPPA's baseline requirement that companies must limit their data collection to what is reasonably necessary and proportionate "to provide or maintain a product or service requested by the individual" (or pursuant to certain enumerated purposes) means that data collection will more closely match consumer's expectations. This is the standard that the Committee on Financial Services should be imposing on entities subject to the GLBA.

The Committee on Financial Services simply should not advance a bill in 2023 that uses a notice-and choice-regime, particularly when paired with a preemption provision that prevents states from enacting stronger protections. The standard has changed. The Committee should not advance legislation that purports to be a privacy bill unless it includes a data minimization standard similar to what is set forth in the bipartisan American Data Privacy and Protection Act.

Data Aggregators Should Not be Added to GLBA Without Stronger Privacy Protections

The Data Privacy Act would add "data aggregators" to the types of financial institutions covered by GLBA. "Data aggregators," more commonly known as "data brokers," buy, aggregate, disclose, and sell billions of data elements on Americans with virtually no oversight. For these

[4] EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.
[5] American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. Title I (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

companies, consumers are the product, not the customer. Most consumers do not even know that data brokers exist, as they have no direct relationship with them. This comes at huge cost to individual privacy and our national security.[6] Data brokers have sold data on military personnel to foreign adversaries[7] and facilitated elder scams.[8] Foreign governments seeking personal data on Americans can simply purchase it from a data broker – no cyberattack needed.

Given the lack of regulation of this industry, it would seem to be a step in the right direction to include data brokers as covered entities under the GLBA. Unfortunately, that is not the case. Adding data brokers to GLBA simply allows them to evade stricter regulations, whether from existing state privacy laws or stronger national standards that may come into effect in the coming years. The so-called privacy protections in GLBA are so weak that some consumer advocates have called for their repeal and said that "In some ways, the GLBA is worse for consumers than nothing."[9] This is due to the success that entities regulated by the GLBA have had in lobbying state lawmakers to exempt them from stronger state privacy laws. Any data collected pursuant to GLBA is exempt from the California Consumer Privacy Act. In the other four states that have passed comprehensive privacy laws (Colorado, Virginia, Connecticut, and Utah), entities governed by GLBA are exempted entirely, even for data that is not covered by the law. This is why data aggregators would like to be covered by GLBA, as proposed in this bill – such coverage exempts them from stronger privacy laws. The Committee should not include data aggregators under GLBA coverage unless the privacy protections in this bill are substantially improved and set a higher standard than existing state laws.

We ask that this letter be entered in the record. EPIC looks forward to working with the Committee on these issues.

Sincerely,

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Deputy Director

---

[6] *Promoting Competition, Growth, and Privacy Protection in the Technology Sector: Hearing Before the Subcomm. on Fiscal Responsibility and Economic Grown of the Sen. Comm. on Finance* (testimony of Justin Sherman, Duke University) (Dec. 2021), https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf.
[7] Suzanne Smalley, *Brokers' sales of U.S. military personnel data overseas stir national security fears*, CyberScoop (Apr. 2022), https://cyberscoop.com/data-brokers-national-security-risk/.
[8] U.S. Dept. of Justice, "List Brokerage Firm Pleads Guilty To Facilitating Elder Fraud Schemes," Justice.gov, (Sept. 2020), https://www.justice.gov/opa/pr/list-brokerage-firm-pleads-guilty-facilitating-elder-fraud-schemes.
[9] Robert Gellman, *Protect consumer privacy: Repeal GLBA's privacy provisions*, IAPP Privacy Perspectives (Jul. 30, 2020), https://iapp.org/news/a/protect-consumer-privacy-repeal-the-glbas-privacy-provisions/.