CONSUMER FINANCIAL PROTECTION BUREAU | NOVEMBER 2024

State Consumer Privacy Laws and the Monetization of Consumer Financial Data

1700 G Street NW
Washington, D.C. 20552
(855) 411-2372

Consumer Financial Protection Bureau

Table of contents

1. Executive Summary

Companies across a range of industries are increasingly building business models premised on the monetization of consumer data. The consumer financial services marketplace is no exception. In recent years, financial institutions have become more engaged in advertising and sales, including by selling the data they have collected on the consumers who do business with them. These developments raise questions around whether data is being collected in ways that consumers may not fully understand or have not consented to, the extent to which consumers have meaningful choice in how their information is used, and whether their data is adequately protected.

Recently, several States have adopted new widely applicable consumer data privacy laws that are providing more consumers with more control over the nonpublic personal information that businesses have about them. These state laws add important new rights and protections on top of existing federal privacy law. This report examines that federal backdrop and the protections States are beginning to provide for consumers. This report then examines the perhaps unintended effect of the exemptions these state laws provide for financial institutions or data subject to the Gramm-Leach-Bliley Act and for activity to which the Fair Credit Reporting Act applies. These exemptions may pull numerous businesses outside of the coverage of these state laws, including banks, consumer reporting agencies, debt collectors, payment processors, credit card issuers, mortgage originators and servicers, and payday lenders, many of which may be capturing and monetizing consumer data. Conclusions from this analysis include the following:

- **States have recently passed new data privacy laws, but they have all included exemptions for financial institutions and financial data.** Several States have recently created new consumer protections to guide how companies collect and share consumer data. However, all of the state data privacy laws passed to date exempt financial institutions, financial data, or both if they are subject to the Gramm-Leach-Bliley Act. These state laws therefore decline to provide consumers the same rights over their financial data as the States are providing to the consumers who engage with other industries. All of the state data privacy laws also exempt activity subject to the Fair Credit Reporting Act, and may thereby overlook consumers' privacy interests in that data as well.

- **State policymakers should assess the tradeoffs associated with exempting financial institutions and financial data from new data privacy laws.** Exemptions from state data privacy laws can leave consumers at heightened risk with regard to their financial data. As implemented, the Gramm-Leach-Bliley Act has drawn criticisms for providing general notice to consumers about the types of sharing a financial institution engages in, and requiring consumers to affirmatively exercise their opt-out rights separately with each financial institution. In turn, providing state data privacy protections only for

nonfinancial markets effectively leaves consumers more exposed with respect to their sensitive financial data than they are in other areas of their economic life.

- **These protections are important because financial institutions are collecting large quantities of consumer data and building new business models around data monetization, and current federal protections have limits.** Firms in the consumer finance space are increasingly focusing on the monetization of consumers' financial data as a source of revenue, including by selling that data to third parties. Consumers place a high value on their financial data and their ability to control who has it and how it is used. States that have enacted new data privacy laws have created important protections, and—given the limitations in the current federal protections for financial data—States should consider whether removing or narrowing these exemptions is appropriate to ensure that consumer financial data is protected.

2. The federal financial data privacy framework

Existing federal regulations on financial data privacy have drawn significant scrutiny,[1] especially in light of pervasive digital surveillance—and financial institutions' increasing role as suppliers of consumer data. Financial institutions have always held extensive, detailed, personal records about consumers, which may include the purchases a consumer makes, the debts a consumer owes, and the balance in their accounts.[2] Today, when a consumer merely visits a website (even for their bank or credit card), numerous third parties can learn of the interaction, track the consumer across the web, and plaster individualized marketing across the pages the consumer subsequently views based on that data.[3] Given these modern technologies and only limited restrictions, financial institutions have the ability to—and in some cases may already be—collecting and making money off of the troves of data they possess about the most intimate details' of consumers lives. Many consumers may not even know that their financial data has the potential to be used in this way, and are unaware of the harms they can suffer as a result of that use.

2.1 Background

The Gramm-Leach-Bliley Act (GLBA), as implemented by regulation, provides important but limited federal protections for consumer financial data.[4] Before Congress passed the GLBA in late 1999, the primary federal protection for consumer data was the

[1] *See, e.g.*, Press Release, *McHenry Introduces New Legislation to Modernize Financial Data Privacy Laws* (Feb. 24, 2023), https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=408613; Press Release, *Ranking Member Waters Announces Passage of Democratic Legislation During Full Committee Markup* (Mar. 2, 2023), https://democrats-financialservices.house.gov/news/documentsingle.aspx?DocumentID=410193.

[2] *See, e.g.*, 146 Cong. Rec. S4828 (May 6, 1999) (statement of Sen. Sarbanes) ("Such information can include savings and checking account balances, CD maturity dates, security purchases and insurance payouts. Americans are becoming increasingly concerned about the issue."); *id.* at H11,537 (Nov. 4, 1999) (statement of Rep. Maloney) ("information on everything from account balances to credit card transactions").

[3] Stefan Larsson et al., *Notified but Unaware: Third-Party Tracking Online*, 1 Critical Analysis of Law 101, 118 (2021) (explaining that "[t]he modern web consists of an intricate network of actors who collect, purchase, convey, and convert data in various ways for a large number of purposes," and as a result, "third-party tracking is fundamentally present online," where "data-driven markets largely depend on the continuous collection, sharing and trade of consumers' personal data").

[4] Subtitle A of Title V of the Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (codified at 15 U.S.C. § 6801 *et seq.*); *see also* Regulation P, 12 C.F.R. pt. 1016. The Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, 124 Stat. 1376 (July 21, 2010) (Dodd-Frank) generally transferred privacy rulemaking authority under the GLBA from various other financial regulators to the CFPB. Dodd-Frank § 1093.

1970 Fair Credit Reporting Act (FCRA).[5] The FCRA and the subsequent legislation that amended it restrict the "communication" by a consumer reporting agency (CRA) of information "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" that "is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for" credit, employment, insurance, or certain other purposes.[6] CRAs can only share such information for one or more of the "permissible purposes" enumerated in the FCRA.[7] The FCRA also institutes a robust framework to guide furnishers, CRAs, and users of consumer reports that continues to help ensure that information on consumer reports is kept accurate and remains private. Then and now, the FCRA is an important consumer privacy law protecting the sensitive personal information communicated on consumer reports.

Congress built upon this framework in the GLBA to impose restrictions on how financial institutions share the information they receive about consumers. The overall purpose of the GLBA was to relax prior federal law that had kept banks, insurance companies, and securities firms separate. Due to the GLBA, "bank holding companies" and "financial holding companies" could engage, directly and through their affiliates, in a wide variety of "financial activities" that extended far beyond traditional banking.[8] Congress defined "financial institution" to include any company in "the business of . . . engaging in financial activities,"[9] and required financial institutions to obey the GLBA's privacy restrictions.

2.2 Protections under federal privacy law

The GLBA broadly protects consumers' "nonpublic personal information," which generally includes all the information a financial institution receives about a consumer in the course of offering or providing a financial product or service to the consumer that is not already publicly available.[10] Further, nonpublic personal information remains protected even if it is combined with public information, such as when a company compiles "any list, description, or other grouping of consumers" based on the public and nonpublic information the company has collected.[11] Additionally, financial institutions

---

[5] Fair Credit Reporting Act, Title VI of Pub. L. 91-508, 84 Stat. 1114 (Oct. 26, 1970) (codified as amended at 15 U.S.C. § 1681 *et seq*.); *see also* Regulation V, 12 C.F.R. pt. 1022. Dodd-Frank generally transferred rulemaking authority under the FCRA to the CFPB. Dodd-Frank § 1088.

[6] 15 U.S.C. § 1681a(d).

[7] 15 U.S.C. § 1681b(a).

[8] 12 U.S.C. § 1843(k).

[9] 15 U.S.C. § 6809(3).

[10] 15 U.S.C. § 6809(4); 12 C.F.R. § 1016.3(p)–(q).

[11] 15 U.S.C. § 6809(4)(C); 12 C.F.R. § 1016.3(p)(1)(ii), (p)(2)(ii).

must implement appropriate technical safeguards to protect nonpublic personal information from tampering or destruction, inadvertent disclosure, and data breaches.[12]

Under the GLBA, subject to some exceptions, a financial institution generally cannot share nonpublic personal information with a nonaffiliated third party unless it "clearly and conspicuously discloses to the consumer . . . that such information may be disclosed to such third party," and provides the consumer a reasonable opportunity to opt out of that disclosure before such information is shared and after the financial institution has explained how the consumer can "exercise that nondisclosure option."[13] Further, the GLBA and its implementing regulations restrict the disclosure and reuse of nonpublic personal information by recipients of such information.[14] In that way, the GLBA and its implementing regulations protect consumers' nonpublic personal information wherever it goes, even when it is held by a company that is not a financial institution and not the affiliate of a financial institution.

Finally, the GLBA and its implementing regulations generally require each financial institution to deliver a notice describing its privacy policies and practices to (1) consumers whose information the financial institution may share and (2) consumers with whom it forms an ongoing customer relationship.[15] Financial institutions must deliver these notices to consumers before sharing information subject to an opt out right, and to customers both upon establishing the customer relationship and annually thereafter unless the privacy policy has not changed.[16] Financial institutions must also update their notices if they no longer accurately describe their policies and practices.[17] These notices are designed to enable consumers to easily compare the privacy policies and practices of different financial institutions, to choose who they want to trust with their information.[18]

However, the GLBA permits financial institutions to share information with their affiliates, and provides several exceptions that allow a financial institution to share nonpublic personal information with nonaffiliated third parties without offering consumers an opportunity to opt out of the sharing authorized by those exceptions, such

---

[12] 15 U.S.C. § 6801(b); FTC Safeguards Rule, 16 C.F.R. pt. 314; SEC Regulation S-P, 17 C.F.R. pt. 248; CFTC Safeguards Rule, 17 C.F.R. pt. 160.

[13] 15 U.S.C. § 6802(b)(1); *see also* 12 C.F.R. § 1016.10(a)(1).

[14] *See* 15 U.S.C. § 6802(c); 12 C.F.R. § 1016.11. While the Securities and Exchange Commission, Commodity Futures Trading Commission, and Federal Trade Commission also have rulemaking authority under the GLBA, *see* 15 U.S.C. § 6804(a)(1), for simplicity this report cites only to the CFPB's GLBA implementing regulation, Regulation P.

[15] 15 U.S.C. § 6803(a); 12 C.F.R. § 1016.4.

[16] 12 C.F.R. § 1016.5(e)(1)(ii).

[17] *See, e.g.*, 12 C.F.R. § 1016.8(a)(1).

[18] 15 U.S.C. § 6803(e)(2)(C); *see also Final Model Privacy Form Under the Gramm-Leach-Bliley Act*, 74 Fed. Reg. 62890, 62912 (Dec. 1, 2009) (stating that "two key objectives of the model form are that (1) consumers can understand an institution's information sharing practices and (2) they may more easily compare financial institutions' sharing practices and policies across privacy notices").

as when such sharing is required by law, is necessary to effect a transaction the consumer requested, or even to allow the financial institution to market its own products and services to the consumer.[19] The GLBA also provides an exception for certain activity governed by the FCRA and its implementing regulations, such as furnishing information to consumer reporting agencies (CRAs) and using information in consumer reports.[20]

2.3 Critiques of federal privacy protections

Although the GLBA was groundbreaking in 1999 and provides important protections today, limitations in the framework implemented under it have been identified. For example, the GLBA focuses on informing consumers so they can opt *out*, but an opt-*in* approach that prohibits businesses from sharing information until the consumer affirmatively agrees could be more protective of consumers' sensitive information.[21] Additionally, at present, consumers who do not want their information to be shared have to separately inform each financial institution of their desire to opt out, because there is not yet a single reliable mechanism for broadly opting out across all financial institutions. Further, when consumers were given notice and a reasonable opportunity to opt out but did not do so, the financial institution and its affiliates can broadly use and share the consumers' nonpublic personal information without violating the GLBA, so long as they do so consistent with what the financial institution's privacy policy disclosed.[22]

The Government Accountability Office has also expressed concerns that some financial institutions are abusing Regulation P's model notice option to mask just how much data they collect on consumers and all the ways they allow that information to be used, including by firms far removed from the products and services the financial institution provides.[23] This also raises questions of whether financial institutions have done

---

[19] *See* 15 U.S.C. § 6802(b)(2), (e).

[20] 15 U.S.C. §§ 6802(e)(6), 6806.

[21] *See, e.g.*, Samuel Levine, Director, FTC Bureau of Consumer Protection, Remarks at the Reidenberg Lecture at Fordham Law School, *Toward a Safer, Freer, and Fairer Digital Economy* (Apr. 17, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/20240417-Reidenberg-Lecture-final-for-publication-Remarks-Sam-Levine.pdf; David Walrath, *Privacy and Information Disclosure: An Economic Analysis of the Gramm-Leach-Bliley Act*, 24 POLICY PERSPECTIVES 55, 61 (2017), https://doi.org/10.4079/pp.v24i0.17602. Economists have noted that financial institutions will almost always have more knowledge about what they do with consumer data than consumers do, creating "information asymmetry" that may mean that placing the burden on financial institutions to identify and mitigate risks to consumers would be a more efficient approach than obligating consumers to continually take action to guard the consumer's data. Walrath, *supra* at 58.

[22] *See* 15 U.S.C. § 6803(c); 12 C.F.R. § 1016.6 (detailing the information to be included in privacy notices).

[23] U.S. Gov't Accountability Office, *Consumer Privacy: Better Disclosures Needed on Information Sharing by Banks and Credit Unions,* at 10–21 (Oct. 2020), https://www.gao.gov/assets/d2136.pdf; *see also* Edward J. Janger & Paul

sufficient diligence to even know where the information they share goes after they share it. And consumers understandably may face "information fatigue" from receiving notices from so many financial institutions and communicating their preferences in response.[24]

M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1257–59 (2002), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=319144; *see also* Loretta Garrison et al., *Designing Evidence-Based Disclosures: A Case Study of Financial Privacy Notices*, 46 J. CONSUMER AFFAIRS 204, 227–31 (2012), https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1745-6606.2012.01226.x (explaining development of the model form).

[24] Dan Murphy et al., *Financial Data: The Consumer Perspective* (June 30, 2021), https://finhealthnetwork.org/wp-content/uploads/2021/04/Consumer-Data-Rights-Report_FINAL.pdf (in one study, only 20% of consumers reported that they read most or all of their primary financial institution's privacy policy, and relatively few believed they had successfully communicated their preference to opt-out to their primary financial institution).

3. The need for data privacy in the financial sector

Businesses collect several forms of data that consumers generate when they access financial products and services.[25] This "financial data" can include information that consumers disclose to financial institutions, such as details of their income, expenses, and account balances.[26] Lenders offering paycheck advance products, for example, sometimes collect as many as 140 datapoints on consumers in the course of providing that service.[27] Financial data can also include information that financial institutions compile using third-party products and services, such as a consumer's credit score or a consumers' web browsing history tracked through cookies, pixels, beacons, and related technology.[28] Further, financial data can include the insights about a consumer's behavior that their financial transactions reveal, such as details about what products and services consumers utilize, how much they are spending on these products and services, and where consumers are purchasing them.[29] Hence, this data can be used for purposes that go significantly beyond traditional banking functions.

Consumers place a high value on their financial data and are particularly concerned about maintaining the privacy of that data.[30] For example, in a 2021 survey, 89% of

---

[25] *See* 15 U.S.C. § 6809(4)(a); 12 C.F.R. § 1016.3(q)(1).

[26] *See* 15 U.S.C. § 6809(4)(a)(i)–(ii); 12 C.F.R. § 1016.3(q)(1)(i)–(ii), (q)(2)(i)(B); *see also* Required Rulemaking on Personal Financial Data Rights, at 65 (Oct. 22, 2024), https://files.consumerfinance.gov/f/documents/cfpb_personal-financial-data-rights-final-rule_2024-10.pdf.

[27] Caitlin Harrington, *Workers Are Trading Staggering Amounts of Data for "Payday Loans*," WIRED (Mar. 23, 2022, 8:00 a.m.), https://www.wired.com/story/payday-loan-data/ ("These can include shifts worked, time off, earnings and promotions history, health care and retirement contributions, even reputational markers like on-time rate or a gig worker's star rating and deactivation history.").

[28] *See* 12 C.F.R. § 1016.3(q)(2)(i)(F) (explaining that "personally identifiable financial information" under Regulation P includes "[a]ny information [a financial institution] collect[s] through an internet 'cookie'").

[29] *See* 15 U.S.C. § 6809(4)(a)(ii)–(iii) ("nonpublic personal information" includes all "personally identifiable financial information" about a consumer "resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution"); 12 C.F.R. § 1016.3(q)(1)(ii)–(iii) (defining "personally identifiable financial information" to include information "[a]bout a consumer resulting from any transaction involving a financial product or service between [the financial institution] and a consumer" as well as any information the financial institution "otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer").

[30] *See, e.g.*, Consumer Reports, *American Experiences Survey, December 2023 Omnibus Results*, at 18–19 (Jan. 2024), https://article.images.consumerreports.org/image/upload/v1704482298/prod/content/dam/surveys/Consumer_Reports_AES_December-2023.pdf (more than 75% of respondents said it was "very important" to them that they know "exactly which companies can access [their] banking data" and that their permission be required before banking data can be shared with another company; while 69% felt it was "very important" to "limit[] the purposes for which banks can share [their] banking data, for example, for financial services but not for advertising").

respondents expressed the belief that it should be illegal "for [their] current bank or credit union to give other companies access to personal data about [them] unless [consumers tell the bank to provide it]"; and 94% of respondents stated that they would not like their "current bank or credit union to give other companies access to personal data" so those other companies could "market products and services to [those consumers]."[31] It is not clear if consumers realize how many financial institutions are currently undertaking these practices. Similarly, a recent survey suggested that Americans are more concerned about the security of their financial data than even their medical records.[32]

At the same time, consumers are also increasingly gravitating toward the use of digital tools across their financial lives, from accessing banking services via apps to making payments through products offered by tech companies.[33] Mobile banking became much more widely adopted as a result of the pandemic, reaching 95% of consumers age 18-25, 90% of consumers under 40, 85% of consumers in their 40s, and 60% of consumers age 56-75.[34] Similarly, the Federal Reserve Bank of Atlanta recently found that 70% of consumers had made at least one payment via mobile phone or tablet in the preceding year, and 72% had adopted online or mobile payment services such as PayPal, Venmo, or Cash App by 2023.[35] Another survey found that more than two-thirds of consumers have linked a financial application to their checking account.[36] Consumers' use of these digital financial tools creates unprecedented opportunities for companies to collect large quantities of various types of data concerning Americans' economic lives and behaviors.

The ramifications of the rapid growth of digital payments and financial services are only beginning to present themselves. A variety of stakeholders, including consumer

---

[31] Murphy, *supra* at 10.

[32] Centrify, Consumer Trust Survey, *The Corporate Cost of Compromised Credentials* (2016), https://web.archive.org/web/20170430003505/https://www.centrify.com/resources/centrify-2016-thought-leadership-survey/ (while 78% of Americans ranked "credit card or bank statements" as their top fear of being compromised by hacking or a data breach, only 46% ranked "health and medical records" so highly).

[33] *See, e.g.*, Murphy, *supra* at 12; Ron Shevlin, *Mobile Banking Adoption in the United States Has Skyrocketed (But So Have Fraud Concerns)*, FORBES (July 29, 2021), https://www.forbes.com/sites/ronshevlin/2021/07/29/mobile-banking-adoption-has-skyrocketed-but-so-have-fraud-concerns-what-can-banks-do/.

[34] Shevlin, *supra*.

[35] Fed. Res. Bank of Atlanta, Research Data Report, *2023 Survey and Diary of Consumer Payment Choice*, at 4, 7, 16 (June 3, 2024), https://www.atlantafed.org/-/media/documents/banking/consumer-payments/survey-diary-consumer-payment-choice/2023/sdcpc_2023_report.pdf.

[36] Murphy, *supra* at 12.

advocates[37] and members of Congress,[38] have raised concerns about how information collected by financial institutions is used. Financial institutions are increasingly sharing purportedly deidentified individual information with advertisers, and seeking to hire from companies experienced in leveraging data to better make use of their own data hoards.[39] Others are developing their own products and services to make use of consumer information. For example, Chase and PayPal have launched advertising platforms that companies can use to reach consumers based on data that the financial companies themselves collect on consumer behavior,[40] and several of America's largest banks have launched digital wallet products that may be used to collect consumer data to direct customers toward higher-margin offerings.[41] These digital products follow the example of many Big Tech companies, which have offered various digital wallet and payment services that have opened new frontiers in data collection and monetization.[42]

Consumers may not be aware that financial companies are collecting their data, or that it can be sold. For example, four-in-five respondents to a 2021 survey reported being unaware that fintech apps use third-party providers to gather consumers' financial data, and only about one-in-four knew that data aggregators could sell consumers' personal financial data.[43]

The enormous value of consumer data continues to fuel an increasing appetite for more data on consumers.[44] While access to this information can improve companies' offerings and help consumers find the products and services most suited to their needs,

---

[37] *See, e.g.*, Ed Mierzwinkski, *We oppose a weak federal privacy bill because it would take away state consumer protections* (Feb. 9, 2023), https://pirg.org/updates/we-oppose-a-weak-federal-privacy-bill-because-it-would-take-away-state-consumer-protections/.

[38] *See, e.g.*, Letter from Chairwoman Maxine Waters to the Federal Financial Institutions Examination Counsel on behalf of the House Financial Services Committee, at 5 (Nov. 29, 2021), https://democrats-financialservices.house.gov/uploadedfiles/11.29_ai_ffiec_ltr_cmw_foster.pdf.

[39] *See, e.g.*, Iain Withers & Lawrence White, *Dollars in the detail; banks pan for gold in 'data lakes'*, Reuters (June 21, 2019), https://www.reuters.com/article/us-banks-data/dollars-in-the-detail-banks-pan-for-gold-in-data-lakes-idUSKCN1TM0JG/.

[40] Chase, Chase Media Solutions (last visited Sept. 6, 2024), https://www.chase.com/mediasolutions/home; Patrick Coffee, *PayPal Is Planning an Ad Business Using Data on Its Millions of Shoppers*, Wall St. J. (May 28, 2024), https://www.wsj.com/articles/paypal-is-planning-an-ad-business-using-data-on-its-millions-of-shoppers-cc5e0625.

[41] *E.g.*, Stephanie Hughes, *Banks want in on digital wallets – and the consumer data that comes with them*, MARKETPLACE (Jan. 23, 2023), https://www.marketplace.org/2023/01/23/banks-want-in-on-digital-wallets-and-the-consumer-data-that-comes-with-them/.

[42] Adam J. Levitin, *Pandora's Digital Box: The Promise and Perils of Digital Wallets*, 166 U. PA. L. REV. 305 (2018), https://scholarship.law.upenn.edu/penn_law_review/vol166/iss2/1.

[43] Clearinghouse, *2021 Consumer Survey: Data Privacy and Financial App Usage*, at 6 (Dec. 2021), https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/2021-TCH-ConsumerSurveyReport_Final.

[44] Julie E. Cohen, *Law for the Platform Economy*, 51 U. CAL. DAVIS L. REV. 133 (2017), https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-1_Cohen.pdf.

it also creates new opportunities for scammers and predatory actors to take advantage of consumers, especially those who are particularly vulnerable or where the insights that companies derive can enable manipulative business practices.[45] For example, such data can be used to structure more effective "dark patterns" that steer consumers into products they do not want or cannot afford. Even worse, data may empower companies to generate dark patterns that mislead consumers into approving greater access to even more sensitive information.[46] Further, large-scale data collection can produce discriminatory outcomes, such as when platforms use algorithmic targeting to advertise products and services only to particular demographic groups.[47] This kind of surveillance can also result in "dynamic" pricing that increases costs for consumers.[48] Finally, increased data surveillance may create opportunities for companies to violate consumers' privacy and inflict other harms on young people,[49] workers,[50] and society as a whole in many aspects of peoples' lives and decision-making.[51]

---

[45] Staff Report for Chairman Rockefeller, Senate Committee on Commerce, Science, and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (Dec. 18, 2013), https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a.

[46] Samuel Levine, Director, FTC Bureau of Consumer Protection, Keynote at the Cybersecurity and Privacy Protection Conference at Cleveland-Marshall College of Law, at 7 (May 19, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks-Samuel-Levine-Cleveland-Marshall-College-of-Law.pdf.

[47] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016); *cf. CFPB v. Townstone Fin., Inc.*, 107 F.4th 768, 776 (7th Cir. 2024) ("An analysis of the text of the [Equal Credit Opportunity Act] as a whole makes clear that the text prohibits not only outright discrimination against applicants for credit, but also the discouragement of prospective applicants for credit.").

[48] Michael S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J. L. TECH. 309 (2017), https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech309.pdf.

[49] *See* FTC, *The Future of the COPPA Rule* (Oct. 7, 2019), https://www.ftc.gov/news-events/events/2019/10/future-coppa-rule-ftc-workshop.

[50] Kathryn Zickuhr, *Workplace surveillance is becoming the new normal for U.S. workers* (Aug. 18, 2021), https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/.

[51] Levine (2022), *supra*.

4. State-level data privacy efforts

States have recently been active in passing consumer data privacy laws.[52] Eighteen States passed new statutes between January 2018 and July 2024.[53] Although there are nuances within and differences between each of these laws, many of them provide several important rights for consumers, often for the first time. Generally, these laws govern the "controller" of nonpublic personal information, which is "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."[54] These state laws also impose certain obligations on "processors," who do not control the data but who handle or store it.[55]

Like the GLBA, all of the state laws require that businesses notify consumers about their rights under the state law, and most require that businesses regularly assess that they have appropriate cybersecurity measures in place. Similarly, these state laws do not impose obligations on publicly available information, and generally do not govern deidentified or pseudonymous information that cannot readily be traced back to the specific consumer.

Importantly, all of the state laws enacted to date include the following three new rights, modeled after the European Union's General Data Protection Regulation:

Right of access. In these eighteen States, consumers have the right to ask whether a business has collected their nonpublic personal information, and the consumer can generally obtain from the business a description of the categories of the collected information.[56] In some circumstances, the consumer can follow up to look at the underlying data directly.[57] Some States impose limits on this access to protect especially

---

[52] Members of Congress have also introduced various proposed federal consumer data privacy bills, but none of these bills have yet been enacted. *See, e.g.*, Online Privacy Act of 2023, H.R. 2701 (Apr. 19, 2023), https://www.congress.gov/bill/118th-congress/house-bill/2701; American Data Privacy and Protection Act, H.R. 8152 (117th Cong.) (June 21, 2022), https://www.congress.gov/bill/117th-congress/house-bill/8152; Consumer Online Privacy Rights Act, S.3195 (117th Cong.) (Nov. 4, 2021), https://www.congress.gov/bill/117th-congress/senate-bill/3195; *see also* Cong. Res. Serv., Overview of the American Data Privacy and Protection Act, H.R. 8152 (Aug. 31, 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10776 (comparing proposed legislation).

[53] California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Texas, Utah, and Virginia.

[54] *E.g.*, Va. Code § 59.1-575 (defining "controller").

[55] *E.g.*, Tex. Bus. & Com. Code § 541.104 (describing the obligations of "processors").

[56] *E.g.*, Cal. Civ. Code § 1798.110.

[57] *E.g.*, Cal. Civ. Code § 1798.110(c)(5).

sensitive information, such as requiring the business to remove any Social Security Number from the materials provided in response to an access request.[58]

Right to delete. All eighteen States also give consumers the right to instruct a business to delete the nonpublic personal information it has about the consumer.[59] There are typically some limitations to this right.[60] (Notably, another California law that requires the registration of data brokers allows a consumer to make a single request to a state agency that will result in all California-registered data brokers deleting the information they have about that consumer.[61])

Right to data portability. The final right that all eighteen States included in their laws is the right of the consumer to request that the business give the consumer's data to the consumer in a way that the consumer can easily hand over to another business.[62] The intent of this provision is to make it easy for a consumer to switch providers. After transferring the consumer's data, it is as if the new provider has had a relationship with the consumer for a long period of time. (The CFPB has similarly focused on the benefits of empowering consumers to switch financial providers as part of its work to implement Section 1033 of the Consumer Financial Protection Act through the Personal Financial Data Rights Rule.[63])

In addition, many of the States included the following additional rights and protections in their new privacy laws:

Right to correct. Sixteen States, in addition to access and deletion rights, enable consumers to request that a business fix inaccurate information it holds about the consumer.[64] Such laws focus on allowing the consumer to help the business correct

---

[58] *E.g.*, Minn. Stat. § 325O.05(4)(i)(1).

[59] *E.g.*, Va. Code § 59.1-577(A)(3).

[60] For example, a business is generally not required to undertake costly efforts to find and delete information, and most States do not make the business responsible for ensuring that downstream recipients of the information actually delete it once they communicate the consumer's deletion request to those recipients. Further, several States affirmatively allow businesses to hold onto information for particular purposes despite the deletion request, such as to improve its products and services, and to make sure the business continues to honor the consumer's privacy preferences going forward.

[61] *See* Cal. Civ. Code § 1798.99.86. Further, where a data broker cannot process the request, it must at a minimum treat the request as an opt out from the sale or sharing of personal information. *Id.* § 1798.99.86(c)(1)(B) (citing Cal. Civ. Code § 1798.120).

[62] *E.g.*, Colo. Rev. Stat. § 6-1-1306(1)(e); Utah Code § 13-61-201(3).

[63] *E.g.*, Required Rulemaking on Personal Financial Data Rights, *supra* at 5.

[64] *E.g.*, Conn. Gen. Stat. § 42-518(a)(2).

errors in the important information the business holds for itself or might share with others.[65]

Right to opt* in *before the business processes sensitive data. Departing from the opt-out approach they apply to personal data more generally, fifteen States require that the consumer opt *in* before the business is allowed to collect or use "sensitive" data about the consumer.[66] One category of data many of these laws consider sensitive is geolocation data precise enough to allow someone to track their movements in the physical world or discern their street address.[67] Several States define this threshold as any geolocation data that is more precise than a radius of 1,750 feet.[68] Several States also treat as especially sensitive any nonpublic personal information about minors, although different States set varying age thresholds.[69]

Right to opt out of targeted advertising. Many States give consumers the right to opt out of the business' use of the consumer's nonpublic personal information for the purpose of targeted advertising that follows them across websites and online services.[70] When consumers opt out under these provisions, the business can no longer provide the consumer's history of transactions with the business to an advertising company to inform what ads its online advertising algorithms present to that consumer.

Right to opt out of the sale of personal data. Some States give consumers the right to opt out of the business selling their nonpublic personal information.[71] In some ways, this protection extends far beyond an advertising opt out, because the business can no longer earn revenue from providing others with access to the data it holds about the consumers who choose to opt out, regardless of whether the buyer will use the data for advertising or for other purposes.

Protection from retaliation. Several States affirmatively prohibit businesses from treating consumers differently because they are exercising these rights.[72] However, in certain circumstances, a business can refuse to transact with a consumer when the product or service cannot work without information sharing. Some States also allow

---

[65] *See, e.g.*, Va. Code § 59.1-577(A)(2) ("taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data").

[66] *E.g.*, 6 Del. Code § 12D-106(a)(4).

[67] *E.g.*, Colo. Rev. Stat. § 6-1-1303(17.5).

[68] *E.g.*, Tex. Bus. & Com. Code § 541.001(21), (29)(D).

[69] *E.g.*, 6 Del. Code § 12D-106(a)(7).

[70] *E.g.*, Utah Code § 13-61-201(4)(a).

[71] *E.g.*, Iowa Code § 715D.3(1)(d).

[72] *E.g.*, Mont. Code § 30-14-2812(2)(e).

businesses to compensate consumers for allowing access to their data by providing differently priced offerings.

Prompt response times. Most States require businesses to respond promptly to consumers' data requests and impose a time limit, often 45 days.[73]

Data minimization obligation. Most States' laws encourage businesses to collect only the nonpublic personal information they really need in order to provide the products and services they are offering the consumer.[74] This is a particularly helpful protection in the face of data breaches, because data a company does not take in will not be revealed in a data breach.[75]

Specific consent required. Some state laws also seek more affirmative consent, generally providing that a consumer's agreement to lengthy, generalized terms and conditions does not satisfy a state law requirement to obtain consent from the consumer.[76]

[73] *E.g.*, Or. Rev. Stat. § 646A.576(5)(a).

[74] *E.g.*, Mont. Code § 30-14-2812(1)(a).

[75] Samuel Levine (2022), *supra* at 11, https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks-Samuel-Levine-Cleveland-Marshall-College-of-Law.pdf ("information that is never collected can't be compromised").

[76] *E.g.*, Cal. Civ. Code § 1798.140(h).

5. State exemptions for financial institutions and financial data

As promising as the new rights and protections in these state laws are, their reach is limited by the exemptions in those laws. Every one of the new state privacy laws discussed above includes exemptions tied to the GLBA. In addition, all of the state laws exempt the communications that furnishers, CRAs, and users of consumer reports make in compliance with the FCRA and its implementing regulations.[77]

The California Consumer Privacy Act is the only one of the eighteen state laws to focus its GLBA exemption solely on the data governed by the GLBA.[78] The remaining state laws expressly exempt both the data governed by the GLBA as well as financial institutions subject to the GLBA, and fifteen States also exempt the affiliates of those financial institutions.[79]

TABLE 1: STATE DATA PRIVACY LAW EXEMPTIONS FOR GLBA FINANCIAL INSTITUTIONS AND DATA

State	Citation	GLBA Exemptions		
		Data subject to the GLBA	GLBA Financial Institutions	Affiliates of GLBA Financial Institutions
California	Cal. Civ. Code § 1798.145(e)	X		
Colorado	Colo. Rev. Stat. § 6-1-1304(2)(j)(II), (2)(q)	X	X	X
Connecticut	Conn. Gen. Stat. § 42-517(a)(6)	X	X	

[77] Cal. Civ. Code § 1798.145(d); Colo. Rev. Stat. § 6-1-1304(2)(i); Conn. Gen. Stat. § 42-517(b)(11); 6 Del. Code § 12D-103(c)(7); Ind. Code § 24-15-1-2(9); Iowa Code § 715D.2(3)(m); Ky. Rev. Stat. § 367.3613(3)(j); Md. Code, Com. Law § 14-4603(b)(7); Minn. Stat. § 325O.03(2)(a)(8); Mont. Code § 30-14-2804(2)(k); Neb. Rev. Stat. § 87-1104(11); N.H. Rev. Stat. § 507-H:3(II)(k); N.J. Stat. § 56:8-166.13(f); Or. Rev. Stat. § 646A.572(2)(j); R.I. Gen. Laws § 6-48.1-10(f); Tex. Bus. & Com. Code § 541.003(11); Utah Code § 13-61-102(2)(j); Va. Code § 59.1-576(C)(10).

[78] Cal. Civ. Code § 1798.145(e) ("This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations.").

[79] *E.g.*, Md. Code, Com. Law § 14-4603(a)(3) ("This subtitle does not apply to: A financial institution, an affiliate of a financial institution, or data that is subject to Title V of the federal Gramm-Leach-Bliley Act and regulations adopted under that act.").

State	Citation	GLBA Exemptions		
		Data subject to the GLBA	GLBA Financial Institutions	Affiliates of GLBA Financial Institutions
Delaware	6 Del. Code § 12D-103(b)(2), (c)(14)	X	X	X
Indiana	Ind. Code § 24-15-1-1(b)(2)	X	X	X
Iowa	Iowa Code § 715D.2(2)	X	X	X
Kentucky	Ky. Rev. Stat. § 367.3613(2)(b)	X	X	X
Maryland	Md. Code, Com. Law § 14-4603(a)(3)	X	X	X
Minnesota[80]	Minn. Stat. § 325O.03(2)(a)(9), (2)(a)(16)	X	X	X
Montana	Mont. Code § 30-14-2804(1)(e)	X	X	X
Nebraska	Neb. Rev. Stat. § 87-1103(2)(b)	X	X	X
New Hampshire	N.H. Rev. Stat. § 507-H:3(I)(e)	X	X	
New Jersey	N.J. Stat. § 56:8-166.13(b)	X	X	X
Oregon[81]	Or. Rev. Stat. § 646A.572(2)(k)(A), (2)(*l*)	X	X	X
Rhode Island	R.I. Gen. Laws § 6-48.1-10(a)	X	X	X
Texas	Tex. Bus. & Com. Code § 541.002(b)(2)	X	X	
Utah	Utah Code § 13-61-102(2)(k)	X	X	X
Virginia	Va. Code § 59.1-576(B)	X	X	

[80] Minnesota limits its definition of financial institution to "a state or federally chartered bank or credit union, or an affiliate or subsidiary that is principally engaged in financial activities." Minn. Stat. § 325O.03(2)(a)(16).

[81] Oregon limits its definition of financial institution to those defined by the Oregon Bank Act, and limits affiliates to those who are "only and directly engaged in financial activities." Or. Rev. Stat. § 646A.572(2)(*l*).

The GLBA exemptions in these state laws sharply circumscribe the effect of the state laws, and result in providing new protections with respect to data collected by nonfinancial institutions while leaving data collected by financial institutions behind.[82] These exemptions reach far beyond just exempting banks. Under the GLBA, the term "financial institution" broadly encompasses a wide variety of businesses engaged in financial activities including lending, transferring money or securities, financial advisory services, asset management, consumer reporting, debt collection, loan servicing, various transactional services, and in many circumstances acting as a service provider for companies engaged in these activities.[83] Given financial institutions' rapid investment in expanding their own data monetization and absent stronger federal protections, States should consider whether they wish to continue to exempt these activities from the consumer rights and protections their comprehensive state privacy laws provide.

[82] Washington enacted a similar law limited in scope to personal health information, which also exempts the GLBA and the FCRA. Wash. Rev. Code § 19.373.100(2)(a), (c).

[83] *See* 12 U.S.C. § 1843(k)(4); 12 C.F.R. §§ 225.28, 225.86.

6. How State law can provide additional protections

Federal law offers States opportunities to provide consumers with additional protections for financial data.

As the CFPB has previously explained, the FCRA authorizes States to create laws that are not inconsistent with the FCRA—including state laws that are more protective of consumers—so long as they are not with respect to certain narrow subject matters listed in the FCRA.[84] As described above, the state data privacy laws considered in this report vary, but as they are generally more protective (and hence not inconsistent) with the FCRA and do not address the narrow subject matters listed in FCRA section 625(b), they would generally fall outside the scope of FCRA's preemption provision.

The GLBA's general preemption provision preempts inconsistent state law "only to the extent of the inconsistency."[85] Congress was especially clear that States have a role to play in protecting data privacy by adding an express provision that a state law is generally not "inconsistent" with the GLBA when the protection the state law "affords any person is greater than the protection provided" by the GLBA.[86] Again, as described above, the state data privacy laws considered in this report vary, but as they generally are more protective than the GLBA, they can avoid preemption by the GLBA.[87]

Further, under the National Bank Act, a state consumer financial law is preempted if the state law discriminates against national banks as compared to state banks or if the state law "prevents or significantly interferes with the exercise by the national bank of its

---

[84] CFPB, *The Fair Credit Reporting Act's Limited Preemption of State Laws*, 87 Fed. Reg. 41042 (July 11, 2022) ("State laws that are not 'inconsistent' with the FCRA—including State laws that are more protective of consumers than the FCRA—are generally not preempted."); *see also* 15 U.S.C. § 1681t.

[85] 15 U.S.C. § 6807(a).

[86] *See* 15 U.S.C. § 6807(b). This provision states that the CFPB may "determine[]," "after consultation" with any other agency that has enforcement authority, that the state law provides greater protection, either "on [the CFPB's] own motion or upon the petition of any interested party." *Id.*; *see also* 12 C.F.R. § 1016.17(b). States are welcome to consult the CFPB about seeking such a determination with respect to their state data privacy laws.

[87] The GLBA provides the CFPB with authority to determine if state laws are preempted: "For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter, *as determined by the Bureau of Consumer Financial Protection, after consultation with the agency or authority with jurisdiction under section 6805(a) of this title of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party*." 15 U.S.C § 6807(b) (emphasis added). Accordingly, States may consult the CFPB regarding whether their state data privacy laws offer greater protection than the GLBA and Regulation P.

powers" under the standard announced in *Barnett Bank of Marion County v. Nelson*.[88] The Office of the Comptroller of the Currency (OCC) must consult the CFPB before the OCC preempts multiple state laws that have substantively equivalent terms to a law that the OCC is preempting.[89] It appears unlikely that provisions like the state data privacy laws considered in this report prevent or significantly interfere with the exercise by national banks of their powers. Such laws are more akin to a state contract, property, or debt collection law that would generally not be preempted than to a law regulating a banking-specific subject matter that may be preempted in appropriate circumstances.[90]

States should keep the limited scope of these standards in mind in crafting their state laws to ensure they offer the rights and protections to all the consumers they wish to reach. In doing so, States should also be aware that maintaining a GLBA exemption may inadvertently continue to exempt furnishers, CRAs, and users of consumer reports, who may also qualify as "financial institutions" subject to the GLBA.[91] Further, States might craft their FCRA exemptions to not excuse entities from their state laws with respect to all of those entities' conduct merely because they are furnishers, CRAs, or users of consumer reports.[92]

---

[88] 12 U.S.C. § 25b(b)(1) (citing *Barnett Bank of Marion County v. Nelson,* 517 U.S. 25 (1996)).

[89] 12 U.S.C. § 25b(b)(3)(B).

[90] *See Cantero v. Bank of America*, 144 S. Ct. 1290, 1300 (2024) (citing *National Bank v. Commonwealth*, 76 U.S. 353, 361–63 (1870), in which the Court determined that a Kentucky tax law was not preempted because it did not impede the national bank's banking operations and "produced no greater interference with the functions of the bank than any other law governing businesses" much like "generally applicable state contract, property, and debt-collection laws").

[91] *E.g.*, *Trans Union LCC v. FTC*, 295 F.3d 42, 48 (D.C. Cir. 2002) (citing 12 C.F.R. § 225.28(b)(2)(v)) (holding that CRAs are generally financial institutions subject to the GLBA).

[92] *Compare* R.I. Gen. Laws § 6-48.1-10(f) (exempting any "consumer reporting agency as defined by 15 U.S.C. § 1681a(f)"), *with* Conn. Gen. Stat. § 42-517(b)(11) (exempting certain activity related to consumer reports but "only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*.").

7. Conclusion

Many States have recently enacted new data privacy laws that give consumers greater protection and more control over the information businesses hold about them, including the right to find out what data the business has, to ask the business to delete that data, and to facilitate consumers taking ownership of their own data to transfer it to a different company the consumer would prefer to use instead. However, the potential benefit of these state laws will not reach many consumer financial products and services because the States have exempted from coverage the data and financial institutions subject to the GLBA or the FCRA.

States should consider whether they would like to provide the same protections to the financial sector that they are providing consumers in other parts of their economic lives. Research suggests that consumers are particularly concerned about the privacy of their financial information, even as financial institutions increasingly look to make more use of the data they hold without much input from consumers. The rapid growth of business models that rely on the systematic capture and monetization of consumer data poses risks for consumers, especially in the financial sector.

State data privacy laws can play an important role in buttressing existing federal data privacy protections so that consumers are adequately informed and have a meaningful say in how their nonpublic personal information is shared and used. The GLBA and the FCRA give States latitude to offer consumers greater protections than what those federal laws provide for consumers. Absent action to enhance federal privacy protections, States may need to amend privacy laws to adequately protect consumers' personal financial data.