epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

UNBRIDLED AND UNDERREGULATED:

Removing FCRA and GLBA Exemptions from Privacy Laws to Hold Data Brokers Accountable

Unbridled and Underregulated:

Removing FCRA and GLBA Exemptions from Privacy Laws to Hold Data Brokers Accountable

July 2025

Authors:
Caroline Kraczon, Law Fellow
Justin Sherman, EPIC Scholar in Residence

Edited by:
John Davisson
Caitriona Fitzgerald

Acknowledgements:
The authors would like to thank Chi Chi Wu and Seth Frotman for their generous feedback on the paper. This project was supported by funding from Reset.

Key Terms

Consumer Reporting Agency (CRA) — Defined in the FCRA as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."[1]

Data Broker — A company that collects, aggregates, packages, or makes inferences about and then sells data, which often includes the personal data of consumers.

Data-Level Exemption — An exemption that only applies to activities regulated and authorized by a certain law rather than to an entire entity.

Entity-Level Exemption — An exemption that applies to an entire company if *any portion* of its business or activities are covered by a certain law.

Financial Institution — Defined broadly in the GLBA as "any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956,"[2] including consumer reporting agencies and a number of other non-bank companies such as auto dealers and check cashers.[3]

Specialty Consumer Reporting Agencies — Companies that sell credit reports for specific purposes, including employment background checks, subprime lending, tenant screening, medical insurance underwriting, guaranteeing consumers' checks and more.[4]

---

[1] 15 U.S.C. § 1681a(f).
[2] 15 U.S.C. § 6809(3).
[3] National Consumer Law Center, Fair Credit Reporting §§ 18.4.1.3 (10th ed. 2022), updated at www.nclc.org/library (citing Trans Union, L.L.C. v. Fed. Trade Comm'n, 295 F.3d 42, 48, 49 (D.C. Cir. 2002)).
[4] National Consumer Law Center, Fair Credit Reporting § 2.7.3 (10th ed. 2022), updated at www.nclc.org/library; Dan Rutherford, *You have a right to see specialty consumer reports too*, CFPB (Nov. 29, 2012), https://www.consumerfinance.gov/about-us/blog/you-have-a-right-to-see-specialty-consumer-reports-too/.

I. Introduction

Data brokers comprise a multi-billion-dollar industry of companies in the business of collecting, aggregating, packaging, making inferences about, and selling data, including the personal data of consumers. Data bought and sold within the data broker industry includes everything from demographic, financial, and political data to health information, data on children and teenagers, and geolocation and biometric data. The data brokers most well-known to consumers—within the broader, often invisible industry—are consumer reporting agencies that sell "credit reports" and "credit scores" on people to lenders, landlords, and other purchasers. Consumer reporting agencies (CRAs) are regulated by the 1970 Fair Credit Reporting Act (FCRA), a federal law which gives American citizens the right to access their credit reports once annually and to correct information that is inaccurate. Consumer reporting agencies also fall within the scope of the Gramm-Leach-Bliley Act (GLBA), which regulates financial institutions' use of personal information.

CRAs often sell much more than just credit reports. Prominent CRAs, for example, sell salary and employment information on hundreds of millions of U.S. consumers as well as health, location, and other information that goes far beyond what is traditionally included in a credit file. This raises two important yet under-discussed problems for policymakers, legislators, and consumers. First, all general state privacy laws exempt FCRA-covered data, even though the FCRA covers a much broader spectrum of personal information than consumers might expect. All general state privacy laws also contain an exemption for GLBA-covered entities or data. The protections included in the GLBA and the FCRA are different and often not as expansive as the protections and consumer rights included in general state privacy legislation. Legislators may not be aware that consumer reporting agencies engage in such widespread data brokerage—and may therefore unintentionally let these privacy-invasive and harmful activities off the hook from their state privacy law's rules. Second, it highlights the regulatory grey area in which data brokers often operate, which incentivizes data brokers to claim or disclaim the protections and obligations of different legal frameworks to best suit their purposes. Exemptions in state laws for GLBA- or FCRA-covered data or entities can exacerbate this regulatory arbitrage.

This paper proceeds in four parts. It examines the few regulations that govern some data broker business activities, including the GLBA and the FCRA. It then dives into the GLBA- and FCRA-based exemptions in various state privacy laws and how they allow privacy-invasive and harmful data brokerage activities to continue without adequate regulatory coverage. Next, the paper compares the consumer rights and protections included in the GLBA, the FCRA, and state privacy laws, evaluating the negative incentives created by the current legislative and regulatory structure governing data brokers.

Lastly, it offers recommendations for state legislators, federal legislators in Congress, and federal policymakers:

1. States with consumer privacy laws should evaluate any potential loopholes in the text and explore new legislation to close these gaps. States should remove GLBA and FCRA data-level or entity-level exemptions from consumer privacy laws so that consumers can both exercise their rights under the GLBA and FCRA without issue and receive protections against CRAs' other data activities (like selling demographic data and non GLBA- or FCRA-covered financial data).
2. Congress and legislatures in states without general consumer privacy laws should pass new laws without entity- or data-level GLBA or FCRA exemptions in the first place. Further, lawmakers should introduce legislation to clarify the coverage of CRAs under the FCRA—and strengthen the rules for consumers.
3. Lastly, federal agencies such as the CFPB, Federal Trade Commission (FTC) and Department of Justice (DOJ) should use their authority to strengthen rules to protect consumers from data brokers. For example, the CFPB should resuscitate its "Protecting Americans from Harmful Data Practices" rulemaking. The Bureau's 2024 proposal would clarify that many data brokers fulfill the definition of CRAs under the FCRA, meaning data brokers that are CRAs must comply with the FCRA. The CFPB and FTC should also bring enforcement actions against data brokers violating the law.

II. Consumer Reporting Agencies and Federal Regulation

The major CRAs today include Equifax, Experian, and TransUnion as well as many other companies engaging in GLBA- or FCRA-covered activities, whether they self-identify as CRAs or not.[5] Numerous public and private organizations can and do purchase or access consumers' credit data. These include lenders, employers and volunteer organizations, government agencies issuing public assistance, landlords and residential real estate management companies, banks, credit unions, payment processors, retail stores, companies marketing to lower-income consumers and subprime credit applications, debt buyers, debt collectors, insurance companies, telecommunications and utility companies, and gaming establishments and casinos.[6] Federal, state, and municipal law enforcement agencies can also obtain basic information from credit reports (e.g., name, former address, employer) without a warrant in many cases and can obtain more detailed information from CRAs with a court order or subpoena.[7]

The largest CRAs gather and sell enormous amounts of credit data on consumers. For example, Equifax operates a subsidiary CRA called "The Work Number" that gathers employment and salary

[5] *See, e.g.*, *List of consumer reporting companies*, Consumer Financial Protection Bureau, https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/consumer-reporting-companies/companies-list/ (last accessed Sept. 29, 2024).
[6] *2024 List of Consumer Reporting Agencies*, Consumer Financial Protection Bureau (2024) https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2024.pdf at 3-4.
[7] *Fair Credit Reporting Act,* Department of Justice, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/2349 (last accessed Sept. 29, 2024).

records on hundreds of millions of Americans. By 2022, Equifax reported that it had "over 535 million active and historic records from 2.5 million contributors to The Work Number."[8] Today, it currently advertises partnerships and integrations with payroll providers ADP, Alight, Avionte, OneSource, ProLiant, WorkDay, and Ultimate Software and boasts having more than 695 million records on consumer employment.[9]

Data brokerage is an alarmingly unregulated industry. Among the few laws and regulations that apply to many data brokers are the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, which both address privacy in the financial sector.

a. The Fair Credit Reporting Act

The FCRA applies to many data brokers, but not all, because not all entities that compile and sell information traditionally contained in consumer reports clearly fall under the FCRA as it is currently construed. For example, a mobile app that sells its users' data with the expectation that it will be used for the sole purpose of targeting advertisements may not be covered by the FCRA. However, a company selling the same data with the expectation that the purchaser of the data will consider the data while making a credit decision, for example, would be covered by the FCRA. While the FCRA was written to handle the growth of the credit bureau industry and the need for safeguards and consumer rights around credit reports, many of the data brokers covered under the statute engage in activities well beyond its original scope—creating urgent privacy questions for legislators and policymakers.

Congress passed the Fair Credit Reporting Act in 1970 to regulate the emerging credit reporting industry and advance the accuracy, fairness, relevance, proper use, and privacy of consumer data contained in credit reports.[10] The law covers "consumer reporting agencies," defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purposes of preparing or furnishing consumer reports."[11] Congress defined a "consumer report" as any written, oral, or other communication from a consumer reporting agency about a person's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" used or expected to be used or collected in whole or in part for the purpose of serving as a factor

[8] Justin Sherman, *Examining data broker Equifax's relationships with millions of employers*, Duke University Sanford School of Public Policy (Aug. 24, 2022) https://techpolicy.sanford.duke.edu/blogroll/examining-data-broker-equifaxs-relationships-with-millions-of-employers/.
[9] *Partner With Us*, The Work Number, https://theworknumber.com/partner-with-us (last accessed September 29, 2024).
[10] 15 U.S.C. §§ 1681-1681x.
[11] 15 U.S. Code § 1681a(f).

in credit or insurance decisions, employment decisions, and other covered activities.[12] Financial institutions and other decisionmakers were already regularly using consumers' credit reports to make lending decisions and more—prompting Congress to act.

The FCRA gives rights to consumers that include:

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "credit freeze" on your credit report with nationwide consumer reporting agencies, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.[13]

One of the most significant privacy safeguards in the FCRA is the limitation on access to consumer files. CRAs may only furnish consumer reports for one of the permissible purposes expressly set forth in the FCRA.[14] Some of the permissible purposes include furnishing a report in response to a court order or subpoena,[15] in accordance with the written instructions of the consumer,[16] or when the recipient intends to use the information for employment, insurance, credit, or other legitimate business purposes.[17] A CRA may only furnish a consumer's file to a third party if the CRA has reason to believe that the third party will use such information for one of the permissible purposes. This limitation prevents CRAs from sharing consumer reporting data for advertising and marketing purposes, for example. Strictly limiting the disclosure of consumer reports helps to protect privacy and to ensure that personal information is only disclosed to third parties who seek access to the data for certain legally defined purposes.

---

[12] 15 U.S. Code § 1681a(d).

[13] *A Summary of Your Rights Under the Fair Credit Reporting Act*, Consumer Financial Protection Bureau, https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf (last accessed September 29, 2024).

[14] 15 U.S. Code § 1681b(a).

[15] 15 U.S. Code § 1681b(a)(1).

[16] 15 U.S. Code § 1681b(a)(2).

[17] 15 U.S. Code § 1681b(a)(3).

Further, data brokers often collect and sell much of the same information as traditional CRAs without complying with the FCRA. The CFPB proposed new rules in December 2024 to clarify the scope of the FCRA. Noting that data brokers "routinely sidestep" the FCRA's requirements while engaging in the types of activities that the FCRA is meant to encompass,[18] the CFPB proposed language to clarify the extent of FCRA's coverage over data brokers.[19] The proposed rules would have clarified that data brokers which sell data about income, financial tier, credit history, credit score, or debt payments are necessarily consumer reporting agencies covered by the FCRA.[20] Though these proposed rules have since been withdrawn by the Trump Administration,[21] they would have better ensured that data brokers abide by all of the FCRA's consumer protections—including the above-described restriction on data brokers' ability to sell personal information.[22] Consumer reporting agencies, including many data brokers, have substantial impacts on consumers' access to basic services like housing and employment, their financial security, and their privacy and physical safety, making cohesive and comprehensive regulations essential for consumers.

b. The Gramm-Leach-Bliley Act

The GLBA was passed in 1999 in response to growing consolidation in the financial services industry. During the two decades prior to the GLBA's passage, the number of banks in the United States fell while the average size of banks increased.[23] Previously, different types of financial services were typically offered by different companies. For example, a bank might specialize in commercial banking or investment banking, but it may not offer both services. By the late 1990s, it was much more common for the same financial services company to offer a variety of financial services and products. As financial services companies grew in size and in the variety of services offered, they also began to collect and maintain more data about their customers.[24] The GLBA aimed to update financial services regulations to better fit the modern, integrated financial system. The law includes a variety of provisions, including provisions allowing more financial integration, limiting the size of banks' subsidiaries, and establishing Federal Reserve supervision authority over financial holding companies.[25]

---

[18] *CFPB Proposes Rule to Stop Data Brokers from Selling Sensitive Personal Data to Scammers, Stalkers, and Spies*, Consumer Financial Protection Bureau (Dec. 3, 2024), https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-stop-data-brokers-from-selling-sensitive-personal-data-to-scammers-stalkers-and-spies/.

[19] Protecting Americans from Harmful Data Broker Practices (Regulation V), Consumer Financial Protection Bureau, CFPB2024-0044 (Dec. 3, 2024).

[20] *Id.*

[21] Protecting Americans from Harmful Data Broker Practices (Regulation V); Withdrawal of Proposed Rule, Consumer Financial Protection Bureau, CFPB-2024-0044 (May 15, 2025).

[22] *Id.*

[23] *Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley)*, Federal Reserve History (Nov. 22, 2013), https://www.federalreservehistory.org/essays/gramm-leach-bliley-act.

[24] *Id.*

[25] *Id.*

Most relevant to this paper is Title V of the GLBA, which covers the privacy of consumer information held by financial institutions. The GLBA governs "nonpublic personal information," meaning personally identifiable financial information that is not publicly available, held by financial institutions.[26] "Financial institution[s]" are defined broadly in the GLBA as "any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956."[27] Consumer reporting agencies are within the scope of financial institutions covered by the GLBA, as are a number of other non-bank companies such as auto dealers and check cashers.[28]

The GLBA's privacy protections rely on notice requirements. Financial institutions must provide a notice to consumers about their privacy policies and practices[29] and a notice about how consumers may opt out of disclosure of their nonpublic personal information to nonaffiliated third parties.[30] Regulation P, promulgated by the CFPB pursuant to its authority under the GLBA, provides specific requirements for financial institutions' disclosures to consumers, aiming to ensure that disclosures are clear, comprehensive, and conspicuous.[31]

The GLBA's notice requirements do not provide strong privacy protections to consumers. Given the length and complexity of privacy disclosures, it would be virtually impossible for consumers to read and understand all of the privacy notices provided to them by financial institutions.[32] Even if consumers did read them, consumers are not empowered to negotiate terms with financial institutions. The sole substantive right for consumers is the ability to opt out of nonexempt disclosures of nonpublic personal information to a nonaffiliated third party.[33] Otherwise, if a consumer is uncomfortable with a company's privacy policy, the only option for the consumer is not to use the company's services. However, choosing not to use the services provided by financial institutions would be nearly impossible for modern consumers because these companies provide a number of essential services, including banking services, insurance policies, mortgages and other loans, and credit reporting.

Further, the GLBA contains a number of broad exemptions to its disclosure and opt-out requirements. First, financial institutions are not required to provide privacy or opt-out disclosures

---

[26] 15 U.S.C. § 6809(4).
[27] 15 U.S.C. § 6809(3).
[28] National Consumer Law Center, Fair Credit Reporting §§ 18.4.1.3 (10th ed. 2022), updated at www.nclc.org/library (citing Trans Union, L.L.C. v. Fed. Trade Comm'n, 295 F.3d 42, 48, 49 (D.C. Cir. 2002)).
[29] 15 U.S.C. § 6803.
[30] 15 U.S.C. § 6802.
[31] National Consumer Law Center, Fair Credit Reporting §§ 18.4.1.8 (10th ed. 2022), updated at www.nclc.org/library.
[32] Tim Samples, Katherine Ireland, Caroline Kraczon, *TL;DR: The Law and Linguistics of Social Platform Terms-of-Use*, 39 Berk. Tech. L. J. 47 (2024).
[33] National Consumer Law Center, Fair Credit Reporting §§ 18.4.1.8.1 (10th ed. 2022), updated at www.nclc.org/library.

when sharing a consumer's financial information in connection with processing or servicing a consumer's transaction.[34] Second, the GLBA includes a long list of specific exempt disclosures, including disclosures to CRAs in accordance with the FCRA, disclosures of information from a consumer report from a CRA, and disclosures to law enforcement agencies, to name just a few.[35] Third, financial services institutions are exempt from opt-out disclosure requirements when information is disclosed to nonaffiliated third parties providing certain services to the institution.[36]

Beyond disclosure requirements, the GLBA also includes certain data security requirements. The FTC Safeguards Rule, which was promulgated pursuant to the GLBA, provides specific data security safeguards for financial institutions, and it also requires covered entities to notify consumers if their financial information was breached.[37]

c. Well Beyond Credit Information

Some of the largest CRAs today sell personal data about consumers that goes far beyond the scope of credit information. This includes data on purchases, browsing histories, network data, geolocation data, and inferred preference and characteristic data on hundreds of millions of U.S. persons. The "Big Three" nationwide CRAs (Equifax, Experian, and TransUnion) by themselves sell a tremendous amount of data in addition to credit reports.

Equifax advertises "data, insights, and efficiencies" for the healthcare industry, including "clear, reliable information about patients and their ability and propensity to pay."[38] Experian advertises marketing data to automobile dealers, stating that for its North American Vehicle Database "information is loaded within 48 hours of receipt from state Departments of Motor Vehicles," which is offered alongside "a robust combination of vehicle history, vehicles in operation, credit, market, and online/offline behavioral data" needed to get "comprehensive views" of the market.[39] TransUnion offers an IP tracking service—which it describes as a fraud mitigation tool—that helps purchasers with "clearly understanding the origin and legitimacy of web traffic," including identifying the use of VPNs and corporate network anonymizers, by collecting "IP data from countries across five continents" incorporated with "partner data from countries with mobile

---

[34] 15 U.S.C. § 6802(e)(1).
[35] 15 U.S.C. § 6802(e).
[36] 15 U.S.C. § 6802(a)(2).
[37] *Id.*; *FTC Safeguards Rule: What Your Business Needs to Know*, Federal Trade Commission (Dec. 2024), https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.
[38] *Healthcare*, Equifax, https://www.equifax.com/business/healthcare/ (last accessed May 6, 2025) [https://web.archive.org/web/20250709151230/https://www.equifax.com/business/healthcare/].
[39] *Auto Dealer Services*, Experian, https://www.experian.com/automotive/auto-dealer-services (last accessed May 6, 2025) [https://web.archive.org/web/20250709151141/https://www.experian.com/automotive/auto-dealer-services].

networks."[40] All three of these CRAs offer facial recognition technology (i.e., biometrics analysis) for companies to identify and verify the identities of users,[41] with Experian most recently purchasing behavioral analytics firm NeuroID in August 2024 to provide "a new layer of insight into digital behavioral signals and analytics observed for both new and returning users throughout the customer lifecycle, including account openings, logins, and transactions."[42] The list goes on, well beyond what is typically expected from a credit reporting business.

[40] *TruValidate IP Intelligence Solutions*, Transunion, https://www.transunion.com/solution/truvalidate/digital-insights/ip-intelligence (last accessed May 6, 2025) [https://web.archive.org/web/20250709151427/https://www.transunion.com/solution/truvalidate/digital-insights/ip-intelligence].

[41] *Equifax Biometrics*, Equifax, https://www.equifax.com.au/business-enterprise/products/equifax-biometrics (last accessed May 6, 2025) [https://web.archive.org/web/20250709151418/https://www.equifax.com.au/business-enterprise/products/equifax-biometrics]; *Identity proofing*, Experian, https://www.experian.com/business/solutions/identity-solutions/identity-proofing (last accessed May 6, 2025) [https://web.archive.org/web/20250709151458/https://www.experian.com/business/solutions/identity-solutions/identity-proofing]; *Document Verification and Facial Biometrics*, Transunion, https://www.transunion.co.uk/product/document-verification-facial-biometric (last accessed May 6, 2025) [https://perma.cc/F2N4-BP9T].

[42] *Experian acquires behavioral analytics pioneer NeuroID*, Experian plc (Aug. 13, 2024), https://www.experianplc.com/newsroom/press-releases/2024/experian-acquires-behavioral-analytics-pioneer-neuroid [https://web.archive.org/web/20250709151753/https://www.experianplc.com/newsroom/press-releases/2024/experian-acquires-behavioral-analytics-pioneer-neuroid].

Based on their privacy policies, Equifax,[43] Experian,[44] and TransUnion[45] reserve the right to—and in some cases do—sell or share the following types of data:

Data Type	Equifax — Sold or Shared?	Experian — Sold or Shared?	TransUnion — Sold or Shared?
Personal identifiers	YES	YES	YES
Demographic information	YES	YES	YES
Commercial transaction data	YES	YES	YES
Internet or other network activity	YES	YES	YES
Professional or employment data	YES	YES	YES
Geolocation data	YES[46]	YES	YES
Education data	YES	YES	NO

Specifically, Equifax, Experian, and TransUnion state in their privacy policies that they sell or share a wide variety of personal information with third parties.

- Equifax states that it may use, disclose, sell, and share name and contact information, identifiers, demographic information, payment information, financial information, commercial information, internet or other similar network activity, professional or employment-related information, education information, inferences drawn from personal data, public records information, and photos with third parties.[47]

[43] *Equifax Privacy Statement*, Equifax https://www.equifax.com/privacy/privacy-statement/ (last updated June 2025) [https://web.archive.org/web/20250709151821/https://www.equifax.com/privacy/privacy-statement/#SourcesOfPersonalData].

[44] *U.S. Consumer Data Privacy Policy*, Experian, https://www.experian.com/privacy/us-consumer-data-privacy-policy (last updated June 27, 2025) [https://web.archive.org/web/20250709152057/https://www.experian.com/privacy/us-consumer-data-privacy-policy].

[45] *TransUnion LLC Privacy Notice*, TransUnion.com, https://www.transunion.com/privacy/transunion (last updated July 1, 2025) [https://perma.cc/FC9T-VFDW].

[46] Interestingly, Equifax does not list the collection of geolocation data under the "Personal Data Collected" section of its privacy statement. However, under the "Categories of Personal Information Collection" subsection of its "California Residents Privacy Statement and Notice at Collection," Equifax states that it has collected in the last 12 months (as of June 2025) "geolocation data," sourced "directly from you," as well as from "devices and browsers," "employers," "financial institutions," "consumer credit customers," "third-party data providers," "business customers," "government agencies and contractors," and "public records."

[47] *Equifax Privacy Statement*, Equifax https://www.equifax.com/privacy/privacy-statement/ (last updated June 2025) [https://web.archive.org/web/20250709151821/https://www.equifax.com/privacy/privacy-statement/#SourcesOfPersonalData].

- Experian states that it sells or shares personal and online identifiers, commercial transaction information ("such as records of personal property or products or services purchased, obtained or considered, vehicle information, insurance claims, insurance underwriting information"), internet or other network activity information ("such as browsing history, search history, interactions with a website, email, application, or advertisement"), geolocation data (including "precise geolocation"), professional or employed-related information, education information, and inferences of personal characteristics and preferences drawn from personal data.[48]
- TransUnion states that it sells or shares personal identifiers, protected class characteristics, commercial information, internet or other electronic network activity, geolocation data, professional or employment information, and inferences drawn from other personal information.[49]

The companies' handling of biometric data is not listed in the table above because the statements the companies provide are more difficult to pin down. Equifax says that it "may share biometric information with other service providers for use in the verification services" but otherwise "will not disclose face geometry or other biometric information to third parties without first obtaining additional consent."[50] Experian says that it has collected biometric information (such as call recordings, retina/fingerprint scans, or facial recognition data) in the last 12 months from consumers for the purposes of "fraud and identi[t]y theft prevention and protection" and "to detect and protect against security incidents," but has not sold or shared this data.[51]

Lower down in its privacy policy, however, Experian states (under the discussion of "sensitive personal information") that it has not processed a consumer's biometric data for the purpose of uniquely identifying a consumer in the last 12 months.[52] It does indeed appear, based on Experian's statements, that it is collecting consumers' biometric data—but it is difficult to understand how Experian would be collecting data such as face images or fingerprint scans in ways that are not meant to uniquely identify individual people, when (a) biometric data is typically easily linkable to a specific person and (b) the stated purpose is fraud prevention, which would imply the data is

---

[48] *U.S. Consumer Data Privacy Policy*, Experian, https://www.experian.com/privacy/us-consumer-data-privacy-policy (last updated June 27, 2025) [https://web.archive.org/web/20250709152057/https://www.experian.com/privacy/us-consumer-data-privacy-policy].

[49] *TransUnion LLC Privacy Notice*, TransUnion.com, https://www.transunion.com/privacy/transunion (last updated July 1, 2025) [https://perma.cc/FC9T-VFDW].

[50] *Equifax Privacy Statement*, Equifax https://www.equifax.com/privacy/privacy-statement/ (last updated June 2025) [https://web.archive.org/web/20250709151821/https://www.equifax.com/privacy/privacy-statement/#SourcesOfPersonalData].

[51] *U.S. Consumer Data Privacy Policy*, Experian, https://www.experian.com/privacy/us-consumer-data-privacy-policy (last updated June 27, 2025) [https://web.archive.org/web/20250709152057/https://www.experian.com/privacy/us-consumer-data-privacy-policy].

[52] Id.

being used to match a person's claimed identity against their identity stored somewhere else.[53] TransUnion, for its part, is clearer—stating that it collects biometric information (for "customer service and quality control" and "to verify your identity") and does not sell or share it but discloses it "for a business purpose" to "biometrics analytics providers" and "government agencies."[54]

As detailed above, the "Big Three" CRAs collect extensive personal information going far beyond data that consumers would expect to be included on a credit report. However, the scope of credit reporting data collection and sharing goes far beyond the "Big Three." A number of other companies operate as CRAs, including specialty CRAs. These companies sell credit reports for specific purposes, including employment background checks, subprime lending, tenant screening, medical insurance underwriting, and more.[55] Specialty CRAs share credit reports containing sensitive personal information, but consumers may not even know that specialty credit reports about them exist.[56]

It is common for privacy laws or regulations to be passed and then adapted to keep up with technological changes. However, many new state privacy laws in the U.S. have missed this dynamic in the data brokerage industry—and as a result have created major gaps for consumer privacy and protection.

III. State Privacy Laws

As of July 1, 2025, 19 states have passed general privacy laws. In general, these laws provide consumers more transparency into how companies collect, use, and share their personal data. The laws also give consumers more control over their personal data, though that control puts the onus on the consumer to take action.

These state privacy laws differ in scope and coverage, but most include similar protections for consumers. The following provisions are included in all 19 laws:[57]

---

[53] As of May 2025, Experian has updated its privacy policy to state that the sensitive personal information disclosures only pertain to certain states. "This chart below reflects Experian's data practices with regard to Sensitive Personal Information in states other than Colorado, Connecticut, Delaware, Indiana, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah and Virginia."

[54] *TransUnion LLC Privacy Notice*, TransUnion.com, https://www.transunion.com/privacy/transunion (last updated July 1, 2025) [https://perma.cc/FC9T-VFDW].

[55] National Consumer Law Center, Fair Credit Reporting § 2.7.3 (10th ed. 2022), updated at www.nclc.org/library.

[56] Dan Rutherford, *You have a right to see specialty consumer reports too*, CFPB (Nov. 29, 2012), https://www.consumerfinance.gov/about-us/blog/you-have-a-right-to-see-specialty-consumer-reports-too/.

[57] *US State Privacy Legislation Tracker*, IAPP (Jun. 17, 2025), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [hereinafter "IAPP State Privacy Legislation Tracker"].

- Right of access: Consumers have the right to ask businesses if they have collected their information and to request a description of the types of data collected and/or to obtain the collected data.
- Right to delete: Consumers have the right to request that businesses delete their personal information.
- Right to portability: Consumers may request their data from businesses in a portable format so that consumers can switch to another provider.
- Right to opt out of sales: Consumers may opt out of the sale of their personal information.
- Notice and transparency requirements: Businesses must provide notice and transparency to consumers about certain data practices and privacy programs.

However, general state privacy laws often do not provide adequate privacy protections to consumers. These laws put very few obligations on the companies collecting and using data to protect privacy, instead putting the onus on consumers in the form of opt-out rights. None of the state privacy laws include a private right of action that would allow consumers to bring suits against companies that violate the privacy rights granted by the laws.[58] The state privacy laws currently in place provide some privacy protections for consumers, but they are far from perfect. Stronger state privacy laws would include protections such as robust data minimization obligations on companies, strict regulations on the use of sensitive data, strong civil rights protections, powerful enforcement and regulatory tools, and a private right of action.[59]

Further, as discussed in the next Part, all of the state privacy laws passed thus far exempt entities when they engage in activities that are regulated and authorized by the FCRA or the GLBA, and every state except California, Connecticut, Minnesota, Montana, and Oregon also includes a GLBA entity-level exemption. As previously discussed, the FCRA and GLBA cover a number of large entities that collect, use, and share enormous amounts of deeply personal consumer information. Failing to hold FCRA- and GLBA-covered entities to the same standard as other entities under state privacy laws represents a significant gap in privacy protections for consumers.

IV. Privacy Law Exemptions for FCRA- and GLBA-Covered Entities

a. State Privacy Law FCRA and GLBA Exemptions

[58] The California Consumer Privacy Act does include a private right of action allowing consumers to sue a business when there has been a data breach, but the private right of action does not extend to other consumer rights. Cal. Civ. Code § 1798.150.

[59] Caitriona Fitzgerald, Kara Williams, and R.J. Cross, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, EPIC & U.S. PIRG Education Fund (Feb. 2024), https://epic.org/state-of-privacy-2025 (This report assigns a letter grade to state privacy laws by evaluating the privacy protective provisions included in the laws. Half of the 14 states evaluated received an "F," and no states received an "A.") [hereinafter "The State of Privacy Report"].

All 19 of the general state privacy laws that have passed as of July 1, 2025 include exemptions for data or entities regulated by the FCRA and the GLBA. All of the FCRA exemption provisions are "data-level" exemptions rather than "entity-level" exemptions, meaning that each exemption only applies to activities regulated and authorized by the FCRA rather than to an entire entity. To qualify for the FCRA exemption, an entity must fulfill the FCRA's definition of a "consumer reporting agency," and the data being collected, sold, or otherwise shared must fulfill the FCRA's definition of a "consumer report," both detailed in Part II(a) of this paper. However, if the same entity collects or shares data that does not fulfill the FCRA's definition of a consumer report, then it must comply with state privacy laws.

All 19 general state privacy laws also include an exemption for GLBA-covered data, and every state except California, Connecticut, Minnesota, Montana, and Oregon also includes a GLBA entity-level exemption. All 19 states include exemptions for data collection, processing, and sharing that is regulated and authorized by the GLBA. In the 14 states with entity-level GLBA exemptions, a company is exempt from the state privacy law if ***any portion*** of its business or activities are covered by the GLBA.

The table below shows that every general state privacy law includes an FCRA and GLBA data-level exemption, and that most states also exempt GLBA covered entities entirely. The provisions providing those exemptions are included in the table below.

General State Privacy Law FCRA and GLBA Exemptions

State	FCRA Data-Level Exemption	GLBA Data-Level Exemption	GLBA Entity-Level Exemption	FCRA Exemption Citation	GLBA Exemption Citation
California	X	X		Cal. Civ. Code § 1798.145(d)	Cal. Civ. Code § 1798.145(e)
Colorado	X	X	X	Colo. Rev. Stat. § 6-1-1304(2)(i)(II)	Colo. Rev. Stat. § 6-1-1304(2)(j)(II), (2)(q)
Connecticut	X	X		Conn. Gen. Stat. § 42-517(b)(11)	Conn. Gen. Stat. § 42-517(a)(6)
Delaware	X	X	X	6 Del. Code § 12D-103(c)(7)	6 Del. Code § 12D-103(b)(2), (c)(14)
Indiana	X	X	X	Ind. Code § 24-15-1-2(9)	Ind. Code § 24-15-1-1(b)(2)
Iowa	X	X	X	Iowa Code § 715D.2(3)(m)	Iowa Code § 715D.2(2)
Kentucky	X	X	X	Ky. Rev. Stat. § 367.3613(3)(j)	Ky. Rev. Stat. § 367.3613(2)(b)
Maryland	X	X	X	Md. Code, Com. Law § 14-4603(b)(7)	Md. Code, Com. Law § 14-4603(a)(3)
Minnesota	X	X		Minn. Stat. § 325O.03(2)(a)(8)	Minn. Stat. § 325O.03(2)(a)(9), (2)(a)(16)
Montana	X	X		Mont. Code § 30-14-2804(2)(k)	Mont. Code § 30-14-2804(1)(f)
Nebraska	X	X	X	Neb. Rev. Stat. § 87-1104(11)	Neb. Rev. Stat. § 87-1103(2)(b)
New Hampshire	X	X	X	N.H. Rev. Stat. § 507-H:3(II)(k)	N.H. Rev. Stat. § 507-H:3(I)(e)
New Jersey	X	X	X	N.J. Stat. § 56:8-166.13(f)	N.J. Stat. § 56:8-166.13(b)
Oregon	X	X		Or. Rev. Stat. § 646A.572(2)(j)	Or. Rev. Stat. § 646A.572(2)(k)(A), (2)(l)
Rhode Island	X	X	X	R.I. Gen. Laws § 6-48.1-3(e)(11)	R.I. Gen. Laws § 6-48.1-10(a)
Tennessee	X	X	X	Tenn. Code Sec. 47-18-3210(a)(16)	Tenn. Code Sec. 47-18-3210(a)(2)
Texas	X	X	X	Tex. Bus. & Com. Code § 541.003(11)	Tex. Bus. & Com. Code § 541.002(b)(2)
Utah	X	X	X	Utah Code § 13-61-102(j)(i)(C)	Utah Code § 13-61-102(2)(k)
Virginia	X	X	X	Va. Code § 59.1-576(C)(10)	Va. Code § 59.1-576(B)

Four states—California, Vermont, Texas, and Oregon—have also passed data broker registry laws. Though these laws differ in scope, they generally require third-party data brokers (i.e., companies selling personal data that they did not collect from their own customers or users) to register with a state agency, to allow consumers to request that data brokers delete their data or stop collecting and selling their data, and to comply with data security requirements. Vermont's Data Broker Act contains no exemption for FCRA- or GLBA-regulated entities or activities. California, Texas, and Oregon's data broker registration laws include FCRA data-level exemptions, meaning that data brokers must comply with these laws except to the extent they are engaging in activities regulated by the FCRA and are in compliance with the FCRA. California and Oregon also include a GLBA data-level exemption, and Texas includes a GLBA entity-level exemption.

State Data Broker Registry Laws' FCRA & GLBA Exemptions

State	Law	FCRA Exemption Language	GLBA Exemption Language
California	Delete Act Sec. 1(c)	"An entity to the extent that it is covered by the federal Fair Credit Reporting Act"	"An entity to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations."
Vermont	Data Broker Act	No exemption	No exemption
Texas	Data Broker Act Sec. 509.003(b)	"A consumer reporting agency or other person or entity that furnishes information for inclusion in a consumer credit report or obtains a consumer credit report, but only to the extent the person or entity engages in activity regulated or authorized by the Fair Credit Reporting Act (15 U.S.C. Section 1681et seq.), including the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer 's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living."	"A financial institution subject to Title V, Gramm-Leach-Bliley Act"
Oregon	HB 2052 Sec. 1(c)(B)	"A consumer reporting agency, as defined in 15 U.S.C. 1681a(f), a person that furnishes information to a consumer reporting agency, as provided in 15 U.S.C. 1681s-2, or a user of a consumer report, as defined in 15 U.S.C. 1681a(d), to the extent that the consumer reporting agency, the person that furnishes information to a consumer reporting agency or the user of a consumer report engages in activities that are subject to regulation under the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq."	"A financial institution, an affiliate or a nonaffiliated third party, as those terms are defined in 15 U.S.C. 6809, to the extent that the financial institution, affiliate or nonaffiliated third party engages in activities that are subject to regulation under Title V of the GrammLeach-Bliley Act, 15 U.S.C. 6801 to 6809, and regulations adopted under Title V of the Gramm-Leach-Bliley Act."

b. Federal Privacy Bill FCRA and GLBA Exemptions

The American Privacy Rights Act (APRA), the most recently proposed comprehensive federal privacy bill, also contained FCRA and GLBA exemptions.[60] The FCRA and GLBA exemptions included in APRA were data-level exemptions, similar to the exemptions for FCRA and GLBA covered data included in general state privacy laws. The text of APRA heavily referenced the text of the American Data Privacy and Protection Act (ADPPA), which was a comprehensive federal privacy bill introduced in 2022.[61] ADPPA passed out of committee, but it was never ultimately passed into law.

Given how past Congressional privacy bills inform future ones (like ADPPA informing APRA), it is likely that FCRA or GLBA exemptions may be carried forward into future proposals. This introduces similar questions and concerns about consumer privacy and about companies' incentives to comply with consumer safeguards. Data-level exemptions are better for privacy than entity-level exemptions, in that they cover more CRA data brokerage (of non-FCRA- or GLBA-covered data). But they may still incentivize companies to represent or shift their data collection activities to avoid coverage under a future federal privacy law, relying on exemptions and regulatory gaps that legislators did not anticipate or intend to create.

V. Analysis

a. Data Brokers' Coverage Claims and Mismatched Compliance Incentives

Whether businesses are covered by privacy laws should not be left up to the businesses themselves. Ambiguities in the current regulatory system have afforded some companies the space to speciously claim that they are not subject to the FCRA or the GLBA, either by mischaracterizing their own data activities or posting boilerplate language on their websites to the effect of "do not use this data for credit reporting purposes as defined under the FCRA."

Pasting a sentence or two into a website footer or terms of service page to disclaim coverage from the FCRA is relatively commonplace, especially for many "people search" data brokers (those that compile public records and other data, digitize them, link them to specific people, and then post the data online for search and sale by a person's name, phone number, and so on). For example, the people search data broker PeopleFinder.com advertises for sale, among many other data points, consumers' home addresses, phone numbers, traffic records, and criminal records. Some of this data meets the FCRA's description of what can constitute a "consumer report," as criminal records alone would constitute information—in the FCRA's words—about someone's "character,"

[60] H.R. 8818, 118th Cong. (2024).
[61] H.R. 8152, 117th Cong. (2022).

"general reputation," and "personal characteristics." However, PeopleFinder.com puts a disclaimer at the bottom of its website that reads:

> PeopleFinder.com powered by Intelius does not provide consumer reports and is not a consumer reporting agency as defined by the Fair Credit Reporting Act (FCRA). This site must not be used to determine an individual's eligibility for credit, insurance, employment, housing or any other purpose covered by the FCRA. Please visit GoodHire for all your employment screening needs.[62]

The people search data broker Spokeo similarly advertises that it collects six billion "consumer records," 600 million court records, 89 million business records, and information related to more than 120 social networks. It says its "informative reports" available for sale include contact information, "personal details," "location history," "wealth data," "family and associates," criminal records, and "social media accounts." Once again, several of these categories—such as "wealth data" and "criminal records"—would line up with the kinds of data under the FCRA that constitute a credit report. Yet, Spokeo includes a disclaimer on its website footer that reads:

> Spokeo is not a consumer reporting agency as defined by the Fair Credit Reporting Act (FCRA). Do not use this site to make decisions about credit, employment, tenant screening, or any purpose covered by the FCRA.[63]

PeopleFinder.com states that it collects and shares financial information,[64] and consumer reporting agencies are within the scope of GLBA.[65] However, PeopleFinder.com includes the following GLBA disclosure in their Terms of Use:[66]

> In addition to the above restrictions, the Websites, the Related Services and Materials and the Background Information Services may not be used for the following purposes: . . . To use for purposes covered by federal statutes such as Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), Driver's Privacy Protection Act, the Children's Online Privacy Protection Act (COPPA), and/or all similar laws on the state level.

General statements on the bottom of a website or within terms of use—saying that someone buying data which could easily be used for GLBA or FCRA-related purposes should not do so—should not

---

[62] PeopleFinder.com, https://web.archive.org/web/20250313171616/https://www.peoplefinder.com/ (last accessed March 13, 2025).
[63] Spokeo.com, https://web.archive.org/web/20250327155115/https://www.spokeo.com/ (last accessed March 27, 2025).
[64] PeopleFinder.com, https://web.archive.org/web/20250313171616/https://www.peoplefinder.com/ (last accessed March 13, 2025).
[65] National Consumer Law Center, *supra* note 24.
[66] *Id.*

be sufficient to avoid GLBA or FCRA coverage.[67] But the presence of these disclaimers suggest that the data sellers are behaving as if their data buyers are listening to their suggestions. Beyond raising questions about whether the brokers actually invest in any mechanisms to try to investigate their buyers' compliance, it heightens the risk that said data brokers are not providing legally required rights to consumers as a result.

These kinds of scenarios underscore the problem with entities self-labeling their own coverage under a privacy law like the GLBA and the FCRA—and with unnecessary legal ambiguities about which data-selling entities must comply with which provisions under which circumstances. Privacy laws and regulations must be clear about which data brokers are covered under the FCRA and the GLBA and the penalties for noncompliance with the law.

Lawmakers must also remember the importance of the incentives for data brokers. If general state privacy laws, and even state data broker deletion laws, are not clear about which entities are covered, how state-level coverage relates to federal laws like the FCRA, and the rights that brokers must provide to consumers as a result, there is a greater risk that data brokers will be incentivized to claim (accurately or not) that they are regulated by the FCRA to avoid compliance with a state law. For instance, consider a state that passes a data deletion law for data brokers that completely exempts FCRA-covered entities. A data broker, like one of the aforementioned people search websites, could remove its website footer language about not being FCRA-covered—and likely get away with changing little about its business practices—in a superficial attempt to avoid providing consumers with broader data deletion rights. However, if any portion of a data broker's business qualifies it as a financial institution under GLBA, then the data broker is entirely exempt from almost all of the general state privacy laws currently on the books.

This is just one example, but it demonstrates how these exemptions can create unintentional incentives and workarounds for data brokers to avoid honoring the privacy rights granted to consumers by law. When evaluating state data broker registry laws, privacy experts have lamented how the often small penalties for non-registration give the shadiest companies little reason to register at all. Including GLBA and FCRA exemptions in state privacy laws creates similar unintended incentives for companies to attempt to skirt regulation.

b. Policy Problems Related to Exemptions Included in Other Privacy Laws

Some state and federal sector-specific privacy laws also include entity- or data-level exemptions. Below are several examples of privacy lawsuits that have implicated entity-level exemptions. In these cases, individuals brought suits against entities for violating privacy rights provided by state or federal laws. However, the privacy laws in question include entity-level exemptions that

[67] National Consumer Law Center, Fair Credit Reporting §§ 2.3.5.1, 2.5.4.3 (10th ed. 2022), updated at www.nclc.org/library.

ultimately denied individuals the protection of those laws. Looking at these lawsuits demonstrates how including FCRA and GLBA exemptions in privacy laws may introduce harmful regulatory gaps that are counter to the policy objectives of those laws.

For example, Illinois' Biometric Information Privacy Act (BIPA) includes an exemption for entities regulated by the GLBA. Since BIPA's passage, several cases have arisen in which universities claim that they are financial institutions covered by the GLBA because they offer and administer student loans.[68] In each of the cases discussed below, students brought BIPA suits against their universities based on the universities' use of remote test proctoring software that utilized facial recognition technology, gaze monitoring, microphone recordings, eye monitoring, facial detection tools, and more to surveil students while they took tests remotely.

The universities' arguments have met with mixed success. For example, in *Powell v. DePaul University*,[69] a judge in the Northern District of Illinois dismissed a BIPA suit against DePaul University on the grounds that DePaul is a financial institution covered by the GLBA, making it exempt from the BIPA. However, in both *Harvey v. Resurrection University*[70] and *Fee v. Illinois Institute of Technology*,[71] judges declined to grant motions to dismiss, concluding that whether the universities are financial institutions was a factual question that could not be resolved at the motion to dismiss stage. In *Patterson v. Respondus*,[72] the court also denied the motion to dismiss, rejecting the claim that defendant universities qualified as GLBA covered financial institutions based on the allegations presented by plaintiffs at that stage in the case. As the court explained, entity exemptions such as the GLBA exemption included in the BIPA could have significant impacts on the overall reach of privacy laws like the BIPA, especially if the exemptions are interpreted broadly to include entities who are covered by another law based only on a small portion of their activities.[73]

To take an example from another statutory context, the Health Insurance Portability and Accountability Act (HIPAA), which protects health privacy, includes an exemption for entities covered by the Family and Educational Rights and Privacy Act (FERPA),[74] which protects the privacy of educational records. However, the privacy protections included in FERPA are not as stringent as those provided in HIPAA. For example, a student at the University of Oregon, referred to as Jane Doe in the case, filed a lawsuit under Title IX against her university after being

[68] Jonathan Louis Newmark & Austin Collier, *Banking on an Exemption: Do Universities Qualify as Financial Institutions Exempt from the Illinois Biometric Information Privacy Act?*, Goodwin Privacy Blog (Jan. 3, 2023), https://www.goodwinprivacyblog.com/2023/01/03/banking-on-an-exemption-do-universities-qualify-as-financial-institutions-exempt-from-the-illinois-biometric-information-privacy-act/.
[69] Powell v. DePaul Univ., No. 21-C-3001, 2022 U.S. Dist. LEXIS 201296 (N.D. Ill. Nov. 4, 2022).
[70] Harvey v. Resurrection University, No. 21-cv-3203, 2022 WL 3716213 (N.D. Ill. Aug. 29, 2022).
[71] Fee v. Illinois Institute of Technology, No. 21-cv-02512, 2022 WL 2791818 (N.D. Ill. Jul. 15, 2022).
[72] Patterson v. Respondus, Inc., 593 F. Supp. 3d 783 (N.D. Ill. 2022).
[73] *Id* at 819.
[74] 34 C.F.R. § 160.103.

sexually assaulted by other students.[75] During discovery in the case, the university's attorneys were able to obtain notes from Jane Doe's therapy sessions at a university health facility. If Doe saw a therapist off campus, her health records would have been governed by HIPAA. In that case, the university's attorneys would have needed consent or a court order to obtain Doe's health records, and it is unlikely that they would have been able to access the therapy notes at all. However, since she saw a therapist at a university health facility, FERPA governed the privacy of the health information at issue because HIPAA exempts entities covered by FERPA. FERPA permits universities to disclose student information internally and externally, and it makes no distinction between health information held by student health facilities and attendance records taken by professors. Because FERPA governed, the university's lawyers were easily able to obtain detailed notes about Doe's therapy sessions.

In these cases, students were not afforded the same privacy protections as others because some of the data their respective universities handled was covered by a federal law, allowing the entire entity to skirt compliance with BIPA and HIPAA. When passing these laws, legislators likely did not intend to exclude college students from protection. However, the inclusion of entity exemptions—and the expansive interpretations of those exemptions by courts—resulted in universities skirting responsibility for violating the privacy of their students.

When lawmakers enact privacy laws, they should take these cases as cautionary tales and avoid introducing exemptions that may be construed far more than intended. This was the message of a recent Consumer Financial Protection Bureau report, which details how financial institutions' collection and sale of personal information threatens consumer privacy, discusses weaknesses in Federal privacy laws that cover financial institutions, and recommends that states with privacy laws should remove or narrow FCRA and GLBA exemptions.[76] A separate report by the Connecticut Attorney General's office encourages Connecticut lawmakers to scale back entity-level exemptions in the CTDPA for nonprofits and entities covered by GLBA and HIPAA.[77] The report states that the exemptions put Connecticut residents at a disadvantage, hinder the state's Attorney General from upholding CTDPA's protections, and limit Connecticut's ability to join other states in consumer protection enforcement actions against large entities.[78] Connecticut's experience serves as a warning to other states that are considering passing privacy legislation not to include expansive exemptions in state privacy laws.

---

[75] Lynn M. Daggett, *The Myth of Student Medical Privacy*, 14 Harv. L. & Pol'y Rev. 467 (2020).
[76] *State Consumer Privacy Laws and the Monetization of Consumer Financial Data*, Consumer Financial Protection Bureau (Nov. 2024), https://files.consumerfinance.gov/f/documents/cfpb_state-privacy-laws-report_2024-11.pdf.
[77] Report to the General Assembly's Law Committee Pursuant to Public Act 22-15 "An Act Concerning Personal Data Privacy and Online Monitoring," State of Connecticut Office of the Attorney General (Feb. 1, 2024), https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf.
[78] *Id.*

c. Consumer Rights: The FCRA vs. The GLBA vs. State Privacy Laws with FCRA Exemptions

When a state-level privacy law includes an exemption for data or entities regulated by another law, ideally the other law would provide similar or more stringent privacy protections, especially when the other law covers sensitive personal information. The FCRA covers data held by consumer reporting agencies. As explained in Part II of this paper, that data includes a massive amount of deeply sensitive personal information related to finances, employment history, credit history, arrest records, family members, bankruptcies, and much more. The FCRA does include privacy protections and consumer rights related to covered data, but the FCRA does not have the same protections as current state privacy laws. The GLBA provides even weaker privacy protections than the FCRA.

The protections and rights afforded by the FCRA, the GLBA, and state privacy laws are covered in more detail in Parts II and III of this paper, but the comparisons in the table below demonstrate some of the important differences between the protections and rights afforded to individuals.

Consumer Data Rights in the FCRA vs. the GLBA vs. General State Privacy Laws

Type of Consumer Right	The FCRA	The GLBA	General State Privacy Laws
Limitations on third-party access to data	Entities covered by the FCRA may only disclose data contained in credit reports if they have a permissible purpose to do so.[79] Consumers also have the right to place a credit freeze on reports from the "nationwide" consumer reporting agencies, which prohibits them from releasing information in consumers' credit reports without their permission.[80]	A financial institution must provide notice and an opportunity to opt out before sharing nonpublic financial information with nonaffiliated third parties, subject to a number of exceptions.[81]	All general state privacy laws allow consumers to opt out of the sale of their personal data.[82]

[79] 15 U.S.C. § 1681b.
[80] 15 U.S.C. § 1681c-1(i).
[81] 15 U.S.C. § 6802(b).
[82] IAPP State Privacy Legislation Tracker.

Right to delete or correct data	The FCRA requires CRAs to correct or delete inaccurate, incomplete, or unverifiable information, and consumers have the right to dispute incomplete or inaccurate information.[83]	Not included.	All general state privacy laws give consumers the right to request that businesses delete their personal information.[84]
Right of access	The FCRA gives consumers the right to know what is in their file and to request their credit score.[85]	Not included.	All general state privacy laws give consumers the right to ask businesses if they have collected their information and request a description of the types of data collected or obtain the collected data entirely.[86]
Right of portability	Not included.	Not included.	All general state privacy laws give consumers the right to request their data from businesses so that consumers can switch to other providers.[87]
Notice and transparency	CRAs must tell consumers if information in their credit file has been used against them, and consumers have the right to access their credit file.[88]	Financial institutions must provide privacy[89] and opt-out[90] notices to consumers, subject to a number of exceptions.	All general state privacy laws require businesses to provide notice to consumers about certain data practices and privacy programs.[91]

When legislators pass state privacy laws, they do so to provide strong privacy protections for their constituents. Legislators may include exemptions to ensure that entities are not overly burdened with layers of privacy compliance. However, given the breadth and sensitivity of data held by entities that are regulated by the GLBA and the FCRA, exempting GLBA- or FCRA-covered data or entities seriously limits the effect of state privacy laws. This is particularly true as states begin to incorporate stronger protections such as meaningful data minimization rules that go far beyond privacy protections included in the GLBA and the FCRA.[92] The GLBA and the FCRA

[83] 15 U.S.C. § 1681i.
[84] IAPP State Privacy Legislation Tracker.
[85] 15 U.S.C. § 1681j.
[86] IAPP State Privacy Legislation Tracker.
[87] IAPP State Privacy Legislation Tracker.
[88] 15 U.S.C. § 1681s-2(a)(7).
[89] 15 U.S.C. § 6803.
[90] 15 U.S.C. § 6802(b).
[91] IAPP State Privacy Legislation Tracker.
[92] For example, the Maryland Online Data Privacy Act (MODPA) includes strong privacy protections, including data minimization requirements and use limitations, a prohibition on the sale of sensitive data, civil rights protections, and a ban on targeted advertising to minors.

do not provide the same privacy protections and consumer rights as state privacy laws currently in effect in many states. States unduly limit privacy protections for their constituents when they exempt GLBA- or FCRA-covered data or entities, which include entities that engage in the collection and sale of personal information on a massive scale. Individuals deserve the same protections for personal data held by entities covered by the GLBA or the FCRA as they enjoy for personal data held by other entities.

VI. Recommendations

As more state privacy laws are passed and more federal privacy bills are proposed, these challenges related to GLBA and FCRA coverage, data brokerage, and expanding consumers' rights over their data will persist. To proactively tackle these issues, we recommend:

1. States with consumer privacy laws should evaluate any potential loopholes in the text and explore new legislation to close these gaps. States should remove GLBA and FCRA data-level or entity-level exemptions from consumer privacy laws so that consumers can both exercise their rights under the GLBA and FCRA without issue and receive protections against CRAs' other data activities (like selling demographic data and non GLBA- or FCRA-covered financial data).
2. Congress and legislatures in states without general consumer privacy laws should pass new laws without entity- or data-level GLBA or FCRA exemptions in the first place. Further, lawmakers should introduce legislation to clarify the coverage of CRAs under the FCRA—and strengthen the rules for consumers.
3. Lastly, federal agencies such as the CFPB, Federal Trade Commission (FTC) and Department of Justice (DOJ) should use their authority to strengthen rules to protect consumers from data brokers. For example, the CFPB should resuscitate its "Protecting Americans from Harmful Data Practices" rulemaking. The Bureau's 2024 proposal would clarify that many data brokers fulfill the definition of CRAs under the FCRA, meaning data brokers that are CRAs must comply with the FCRA. The CFPB and FTC should also bring enforcement actions against data brokers violating the law.

The data broker industry's continued collection, aggregation, and sale of personal data violates individual privacy and creates risks to physical safety, financial wellbeing, cybersecurity, and national security. Better understanding how data brokers regulated by the GLBA and the FCRA gather and sell data—and in particular, how they gather and sell non-credit reporting data—will give consumers, legislators, and policymakers a fuller picture of the risks and allow them to work towards more comprehensive solutions. Consumers deserve robust privacy protections and rights over their own data, regardless of the type of business collecting and processing that information. Legislators should not limit those protections with unnecessary and overly broad exemptions.