Articles + Publications | November 15, 2024

# CFPB Publishes Report on State Privacy Law Exceptions for Financial Information

**WRITTEN BY**

Kim Phan | Ronald Raether, Jr. | Robyn W. Lin

On November 12, the Consumer Financial Protection Bureau (CFPB) released a new report titled, "State Consumer Privacy Laws and the Monetization of Consumer Financial Data." The report provides an overview of the state comprehensive privacy laws, such as the California Consumer Privacy Act, enacted in recent years, and analyzes the various exemptions in these state privacy laws for certain federal financial privacy laws, such as the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA). The CFPB concludes that these state privacy laws should reconsider these exemptions and go further to protect consumer financial information in the absence of additional federal privacy protections.

**Insufficient Federal Privacy Protections**

The report expresses concern that federal privacy protections established under laws such as the GLBA and FCRA are insufficient. It claims that many financial institutions are collecting and using large quantities of consumer financial information to create new products and offer new services. For example, lenders offering paycheck advance products may be collecting "as many as 140 datapoints on consumers in the course of providing the services," and financial institutions can collect behavioral data from consumers relating to their use of digital banking tools. The report further observes that such data can be used for advertising, data sales, and other purposes that "go significantly beyond traditional banking functions." The CFPB presents no data from studies or other evidence in the report to support its position that GLBA and FCRA are insufficient to protect consumers. To the extent that the CFPB believes that these federal laws need to be amended, the CFPB should ask for such amendments through Congress rather than attempting to direct the activity of state legislatures. Alternatively, the CFPB could take action through the rulemaking authority granted to the CFPB under both GLBA and FCRA.

**Exemptions for Financial Information Under State Privacy Laws**

The report observes that state privacy laws offer various exemptions for financial institutions. The CFPB claims that such exemptions result in consumers being unable to avail themselves of the privacy rights otherwise established under these state privacy laws. The report concludes that the potential benefits of these state privacy laws will not reach consumer financial information subject to GLBA and FCRA exemptions. The CFPB calls on states to limit the scope of such financial exemptions "to ensure they offer the rights and protections to all the consumers they wish to reach."

Other state laws are already beginning to require businesses to state the types of personal information they collect that may be governed by different privacy laws. Recently passed regulations under California's data broker law will require data brokers to specify the types of personal information they collect that are regulated by other laws such as the GLBA and FCRA.

**Next Steps**

The CFPB suggests that states should consider amending existing privacy laws to further protect financial information. Such amendments may soon be proposed in the wake of the report. Additional states considering enacting their own state privacy laws may also modify existing legislative language in response to the report.

In light of the current federal and state regime, financial institutions should continue to maintain good data hygiene and related compliance practices. If operational practices allow, a financial institution may consider voluntarily extending the various privacy protections implemented on the state level to all of the consumer personal information collected, used, maintained, or disclosed by those financial institutions. However, any such action by financial institutions could present legal, operational, and business risks.

Before extending any rights, financial institutions should consider the following operational concerns:

1. **Potential to Create Inconsistent Standards Across Regulated Data Types.** Depending on resources, it may be difficult to standardize requirements across various data sets. Some laws may require certain handling procedures that differ from other laws. For example, the FCRA may require different handling procedures compared to the CCPA.

2. **Risk of Inconsistent Practices Leading to FTC Scrutiny Under UDAP Principles.** Inconsistent application of voluntary privacy practices can lead to consumer confusion and potential harm. For example, the Federal Trade Commission (FTC) enforces laws against unfair or deceptive acts or practices (UDAP). Depending on how a business publicly commits to handling personal information (such as committing to provide rights to personal information regardless of the statutory regime it is governed by), if these practices are not carried out in practice, the FTC may investigate and decide the business has misled consumers in violation of UDAP.

3. **Increased Costs.** Managing different types of personal information could require substantial costs and resources, especially ensuring personal information is properly classified and handled throughout its lifecycle. Voluntary compliance with the privacy protections implemented on the state level may also require businesses to update systems and processes to accommodate and operationalize rights requests, such as the right to opt out of certain uses of personal information.

**RELATED INDUSTRIES + PRACTICES**

- Consumer Financial Protection Bureau (CFPB)
- Consumer Financial Services
- Privacy + Cyber