KPMG

Regulatory Alert

Regulatory Insights

December 2024

Data Brokers and Data Protection: Regulatory Actions

KPMG Insights:

— ***Expanding Privacy:*** *New state laws impose registration and data privacy requirements on data brokers; CFPB proposes to define data brokers as consumer reporting agencies; FTC and FCC enforcement actions subject data brokers to "credit reporting-like" requirements (e.g., consent, permissible purpose).*

— ***Expanding Sensitive Data:*** *Regulators deem geolocation to be personal data, taking action on the use, sale or disclosure of certain sensitive locations (e.g., military, medical, or religious facilities).*

— ***Continuing Regulatory Focus:*** *Heightened focus is likely to continue at both the federal and state levels given increasing technology/model uses and the potential for harm (e.g., fraud, ID theft, national security).*

Regulators continue to take actions related to data brokers in order to strengthen data privacy protections. In doing so, regulators have argued the potential for national security and surveillance risks, criminal exploitation, issues of personal safety, and fraud. Recent regulatory actions relating to data brokers and data protections, including sensitive consumer data such as geolocation data, include:

1. Federal and State Enforcement Actions
2. CFPB Guidance on Worker Surveillance and FCRA Obligations
3. CFPB Proposal on FCRA Data Broker Practices

1. Enforcement Actions

Across federal agencies and state authorities, recent notable enforcement actions focus on protecting sensitive consumer data, often citing privacy practices deemed unfair and/or deceptive. Examples include:

— **Federal Agencies:**

– **FTC:** In 2024, the Federal Trade Commission (FTC) initiated four enforcement actions against data brokers and aggregators regarding the collection, purchase, sale, and potential misuse of location data. Under the related orders, the companies involved are required to design, implement, maintain, and document safeguards to protect the personal information that they handle, including sensitive location data, as well as implement programs to assess suppliers' compliance. The agency emphasizes the importance of building consumer trust through transparency of business practices and expects that consumers will be given the opportunity to provide or withdraw consent, request deletion of their data, and request the identity of anyone to whom their data has been sold or shared. In addition, the agency deems location data to be sensitive personal information, and further that certain sensitive location data must be banned from use or sale (e.g., military installations, religious organizations, medical facilities, schools and childcare facilities).

– **FCC:** In 2024, the Federal Communications Commission (FCC) took actions citing issues associated with data retention beyond the time needed to fulfill the purpose for which the data was collected and disclosing customer location data without consent to unauthorized third parties.

— **State Authorities**: Many states, including Texas, California, Colorado, Connecticut, and Virginia, among others, have enacted privacy laws that govern the use of consumers' personal data.

– **Texas:** Multiple enforcement actions have been initiated by the **s**tate in connection with a 2024 data

privacy and security initiative alongside recently enacted state privacy laws (e.g., Texas Privacy and Data Security Act (TPDSA), Texas Data Broker Law). The actions were taken against a variety of companies including digital providers and data brokers for collecting, selling, and/or sharing sensitive consumer data without consent (e.g., driver data, personal information of minors, biometric data).

- **California:** The Enforcement Division of the California Privacy Protection Agency (CPPA) recently announced it is conducting a public investigative sweep of data broker compliance with the State's Delete Act. This law requires data brokers to register with the CCPA and also to report whether they collect the personal information of minors, reproductive healthcare data, or precise geolocation data as well as the number of consumer deletion requests they receive along with the average response time to fulfill those requests. Separately, data privacy-related enforcement actions recently initiated by the State Attorney General address collecting and sharing children's data without obtaining parental consent, implementing "reasonable" data security, and selling customer personal information without providing notice or opportunity to opt-out.

2. CFPB Guidance on Worker Surveillance and FCRA Obligations

In October 2024, the Consumer Financial Protection Bureau (CFPB) issued guidance emphasizing worker protections under the Fair Credit Reporting Act (FCRA) in response to the increasing use of digital tools and consumer reports used to assess workers and the potential impacts of such data on workers' careers and livelihoods. The guidance states that employers using third-party consumer reports (e.g., background dossiers, algorithmic scores) for employment purposes (e.g., hiring, promotion, reassignment, retention) must adhere to the FCRA protections, including:

- **Consent:** Obtaining a worker's consent before purchasing a consumer report on the worker.
- **Transparency:** Providing notice to workers and a copy of their consumer report before taking adverse action — including firing, denials of promotions, and demotions or other reassignments — based on the reports.
- **Disputes:** Correcting or deleting inaccurate, incomplete, or unverifiable information when a worker disputes what is in a report.
- **Limits:** Limiting the use of these reports to purposes that are allowed under the law.

3. CFPB Proposal on FCRA Data Broker Practices

The CFPB proposed (December 2024) amendments to Regulation V, which implements the Fair Credit Reporting Act. The proposed changes aim to, among other things, "ensure that FCRA protections are applied to sensitive consumer information that the statute was designed to protect, including information sold by data brokers." The CFPB adds that the proposal would "limit the sale of personal identifiers like Social Security Numbers and phone numbers collected by certain companies and make sure that people's financial data such as income is only shared for legitimate purposes."

The proposed rule amendments include provisions that would:

- **Treat Data Brokers as Consumer Reporting Agencies**. Data brokers that sell information about a consumer's credit history, credit score, debt payments (including on non-credit obligations), or income or financial tier generally would be considered consumer reporting agencies selling consumer reports, regardless of the purpose for which any specific communication of such information is used or expected to be used.
- **Define a Consumer Reporting Agency**. A company would meet the definition of a consumer reporting agency if it assembles or evaluates information about consumers, including by collecting, gathering, or retaining; assessing, verifying, or validating; or contributing to or altering the content of such information
- **Deem Communications to be Consumer Reports**. A communication by a consumer reporting agency of information about a consumer would be a consumer report if the information is used for an FCRA-covered purpose.
- **Define "Credit Header Data" to be a Consumer Report**. Communications from consumer reporting agencies of certain personal identifiers collected to prepare a consumer report—such as name, addresses, date of birth, Social Security numbers, and phone numbers—generally would be considered consumer reports. Sales of such information would be restricted to a permissible purpose under the FCRA.
- **Identify When De-Identified Data is a Consumer Report**. Three alternatives are proposed for determining when de-identified data derived from a consumer reporting database would constitute a consumer report (and so be limited to sale only for FCRA permissible purposes).
- **Clarify the Permissible Purpose Provisions.** The statutory requirement that a consumer reporting agency may furnish a consumer report only under specific enumerated circumstances (permissible purposes)

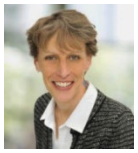
would be restated but also clarify that the "legitimate business needs" permissible purpose would not include marketing purposes.

— **Require Separate Consumer Authorization/Consent**. The consumer reporting agency or recipient of the consumer report would be required to provide the consumer with a separate clear and conspicuous disclosure and obtain the consumer's signature and express consent to the furnishing of the consumer report for the identified product, service, or use before the permissible purpose is applicable. The proposed disclosure would be required to meet certain format and content requirements. The consumer would also have the right to revoke consent.

Comment Period. The CFPB seeks comment on the proposed rule no later than March 3, 2025. The CFPB specifically requests comment on an effective compliance date that would be either six months or one year following publication of the final rule in the Federal Register.

For more information, contact Amy Matsuo, Todd Semanco, or Orson Lucas.

Contact the author:



Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialme