

Highlights of [GAO-14-251T](#), a statement for the record to the Committee on Commerce, Science, and Transportation, U.S. Senate

Why GAO Did This Study

Members of Congress and others have raised privacy concerns about information resellers (data brokers) and consumer information. In part, their concerns stem from consumers not always knowing the nature and extent of the information collected and how it is used. Growing use of the Internet, social media, and mobile applications has intensified privacy concerns because these media greatly facilitate gathering of personal information, tracking of online behavior, and monitoring of individuals' locations and activities. This statement for the record discusses (1) existing federal laws and regulations on the privacy of consumer information held by information resellers, (2) any gaps that may exist in this legal framework, and (3) views on approaches for improving consumer data privacy.

This statement draws from a September 2013 report ([GAO-13-663](#)), which focuses on information used for marketing. GAO analyzed relevant laws and regulations; interviewed representatives of federal agencies, trade associations, consumer and privacy groups, and resellers; and identified and reviewed approaches for improving consumer data privacy.

What GAO Recommends

In September 2013, GAO suggested that Congress should consider strengthening the consumer privacy framework and review issues such as the adequacy of consumers' ability to access, correct, and control their personal information; and privacy controls related to new technologies such as web tracking and mobile devices.

View [GAO-14-251T](#). For more information, contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov.

December 18, 2013

INFORMATION RESELLERS

Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace

What GAO Found

No overarching federal privacy law governs the collection and sale of personal information among private-sector companies, including information resellers. Instead, laws tailored to specific purposes, situations, or entities govern the use, sharing, and protection of personal information. For example, the Fair Credit Reporting Act limits the use and distribution of personal information collected or used to help determine eligibility for such things as credit or employment, but does not apply to information used for marketing. Other laws apply specifically to health care providers, financial institutions, or to the online collection of information about children.

The current statutory framework for consumer privacy does not fully address new technologies—such as tracking of online behavior or mobile devices—and the vastly increased marketplace for personal information, including the proliferation of information sharing among third parties. No federal statute provides consumers the right to learn what information is held about them for marketing and who holds it. In many circumstances, consumers also do not have the legal right to control the collection or sharing with third parties of sensitive personal information (such as health information) for marketing purposes. As a result, although some industry participants have stated that current privacy laws are adequate, GAO found that gaps exist in the current statutory framework for information privacy. The framework also does not fully reflect the Fair Information Practice Principles, widely accepted principles for protecting the privacy and security of personal information that have served as a basis for many privacy recommendations federal agencies have made.

Views differ on the approach that any new privacy legislation or regulation should take. Some privacy advocates have argued that a comprehensive privacy law would provide greater consistency and address gaps in law left by the current sector-specific approach. Others have stated that a comprehensive, one-size-fits-all approach would be burdensome and inflexible. Some privacy advocates also cited the need to provide consumers with greater ability to access, control the use of, and correct information about themselves, particularly for data being used for purposes different than those for which they originally were provided. Industry representatives have asserted that restrictions on the collection and use of personal data would impose compliance costs, inhibit innovation, and reduce consumer benefits. Nonetheless, the rapid increase in the amount and type of personal information that is collected and resold warrants reconsideration of how well the current privacy framework protects personal information. The challenge will be providing appropriate privacy protections without unduly inhibiting the benefits to consumers, commerce, and innovation that data sharing can accord.