

Highlights of [GAO-19-621T](#), a testimony before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate

Why GAO Did This Study

Information resellers—companies that collect and resell information on individuals—have dramatically increased the collection and sharing of personal data in recent years, raising privacy concerns. Increasing use of social media, mobile applications, and other technologies have intensified these concerns.

This statement is primarily based on findings from GAO's 2013 report on information resellers ([GAO-13-663](#)). It also discusses a 2015 report on facial recognition technology ([GAO-15-621](#)), a 2018 report on financial technology ([GAO-18-254](#)), and two 2019 reports on internet privacy and consumer data protection ([GAO-19-52](#) and [GAO-19-196](#), respectively). GAO discusses (1) existing federal laws related to the privacy of consumer information held by information resellers and (2) any gaps in this legal framework. For the prior work, GAO analyzed relevant laws, regulations, and enforcement actions and interviewed representatives of federal agencies, trade associations, consumer and privacy groups, and resellers.

What GAO Recommends

In 2013, GAO recommended that Congress consider strengthening the consumer privacy framework to reflect the effects of changing technologies and markets. In 2019, GAO recommended that Congress consider comprehensive internet privacy legislation. Legislation on these issues has not been enacted to date.

View [GAO-19-621T](#). For more information, contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov.

CONSUMER PRIVACY

Changes to Legal Framework Needed to Address Gaps

What GAO Found

In recent years, GAO issued reports that relate to information resellers and consumer privacy issues. Two central findings from a 2013 GAO report remain current:

- **No overarching federal privacy law governs the collection and sale of personal information among private-sector companies**, including information resellers (data brokers). Instead, a variety of laws are tailored to specific purposes, situations, or entities. For example, the Fair Credit Reporting Act limits use and distribution of personal information collected or used to help determine eligibility for such things as credit or employment. Other laws apply to health care providers, financial institutions, or to online collection of information about children.
- **Gaps exist in the federal privacy framework**. With regard to data that private-sector entities use for marketing, no federal statute provides consumers the right to learn what information is held about them and who holds it. In many cases, consumers also do not have the legal right to control the collection or sharing with third parties of sensitive personal information (such as their shopping habits and health interests) for marketing purposes. In 2013 and in 2015, GAO also reported that the statutory framework for consumer privacy did not fully address new technologies—such as online tracking and facial recognition—and the vastly increased marketplace for personal information, including the proliferation of information sharing among third parties.

In two 2019 reports, GAO found additional gaps in the federal privacy framework and potential limitations in regulatory authority under current privacy law. Internet content providers and internet service providers collect, use, and share information from customers to enable their services, support advertising, and for other purposes. Although the Federal Trade Commission (FTC) generally has addressed internet privacy through its unfair and deceptive practices authority, and other agencies have used industry-specific statutes, there is no comprehensive federal privacy statute with specific internet privacy standards for the private sector. GAO also reported that the Gramm-Leach-Bliley Act, a key law governing the security of consumer information, does not provide FTC with civil penalty authority for violations of the privacy and data security provisions of the act. New and more advanced technologies and changes in the marketplace for consumer information have vastly increased the amount and nature of personal information collected and the number of parties using or sharing it. Such changes warrant reconsideration of how well the current privacy framework protects personal information.