

# GAO Highlights

Highlights of [GAO-14-649T](#), a testimony before the Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, United States Senate

## Why GAO Did This Study

Smartphones and in-car navigation systems give consumers access to useful location-based services, such as mapping services. However, questions about privacy can arise if companies use or share consumers' location data without their knowledge.

Several agencies have responsibility to address consumers' privacy issues, including FTC, which has authority to take enforcement actions against unfair or deceptive acts or practices, and NTIA, which advises the President on telecommunications and information policy issues.

This testimony addresses (1) companies' use and sharing of consumers' location data, (2) consumers' location privacy risks, and (3) actions taken by selected companies and federal agencies to protect consumers' location privacy.

This testimony is based on GAO's September 2012 and December 2013 reports on mobile device location data and in-car location-based services and December 2012 and May 2013 updates from FTC and NTIA on their actions to respond to the 2012 report's recommendations.

## What GAO Recommends

GAO made recommendations to enhance consumer protections in its 2012 report. GAO recommended, for example, that NTIA develop goals, milestones, and measures for its stakeholder initiative. NTIA stated that taking such actions is the role of the stakeholders and that its stakeholders had made progress in setting goals, milestones, and performance measures. GAO will continue to monitor this effort.

View [GAO-14-649T](#). For more information, contact Mark L. Goldstein at (202) 512-2834 or [goldsteinm@gao.gov](mailto:goldsteinm@gao.gov).

June 2014

## CONSUMERS' LOCATION DATA

### Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not Be Clear to Consumers

#### What GAO Found

Fourteen mobile industry companies and 10 in-car navigation providers that GAO examined in its 2012 and 2013 reports—including mobile carriers and auto manufacturers with the largest market share and popular application developers—collect location data and use or share them to provide consumers with location-based services and improve consumer services. For example, mobile carriers and application developers use location data to provide social networking services that are linked to consumers' locations. In-car navigation services use location data to provide services such as turn-by-turn directions or roadside assistance. Location data can also be used and shared to enhance the functionality of other services, such as search engines, to make search results more relevant by, for example, returning results of nearby businesses.

While consumers can benefit from location-based services, their privacy may be at risk when companies collect and share location data. For example, in both reports, GAO found that when consumers are unaware their location data are shared and for what purpose data might be shared, they may be unable to judge whether location data are shared with trustworthy third parties. Furthermore, when location data are amassed over time, they can create a detailed profile of individual behavior, including habits, preferences, and routes traveled—private information that could be exploited. Additionally, consumers could be at higher risk of identity theft or threats to personal safety when companies retain location data for long periods or in a way that links the data to individual consumers. Companies can anonymize location data that they use or share, in part, by removing personally identifying information; however, in its 2013 report, GAO found that in-car navigation providers that GAO examined use different de-identification methods that may lead to varying levels of protection for consumers.

Companies GAO examined in both reports have not consistently implemented practices to protect consumers' location privacy. The companies have taken some steps that align with recommended practices for better protecting consumers' privacy. For example, all of the companies examined in both reports used privacy policies or other disclosures to inform consumers about the collection of location data and other information. However, companies did not consistently or clearly disclose to consumers what the companies do with these data or the third parties with which they might share the data, leaving consumers unable to effectively judge whether such uses of their location data might violate their privacy. In its 2012 report, GAO found that federal agencies have taken steps to address location data privacy through educational outreach events, reports with recommendations to protect consumer privacy, and guidance for industry. For example, the Department of Commerce's National Telecommunications and Information Administration (NTIA) brought stakeholders together to develop codes of conduct for industry, but GAO found this effort lacked specific goals, milestones, and performance measures, making it unclear whether the effort would address location privacy. Additionally, in response to a recommendation in GAO's 2012 report, the Federal Trade Commission (FTC) issued guidance in 2013 to inform companies of the Commission's views on the appropriate actions mobile industry companies should take to disclose their privacy practices and obtain consumers' consent.