December 2013

IN-CAR LOCATION-BASED SERVICES

Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers

GAO Highlights

Highlights of GAO-14-81, a report to the Chairman, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate

Why GAO Did This Study

The prevalence of in-car communication systems provided by auto manufacturers (called telematics systems), PNDs, and smart phones has brought significant opportunities for consumers to access location-based services in their cars. As in-car location-based services have become commonplace, privacy groups and policy makers have questioned whether location data collected by companies can be used for purposes beyond the provision of services, such as by data brokers who collect information to resell the information.

GAO was asked to review this issue. This report addresses (1) what selected companies that provide in-car location-based services use location data for and if they share the data, and (2) how these companies' policies and reported practices align with industry-recommended privacy practices. GAO selected a non-generalizable sample of 10 companies. The companies were selected because they represent the largest U.S. market share or because their services are widely used. GAO examined documentation and interviewed representatives from each company regarding their privacy practices in effect in 2013 and compared those practices to industry recommended privacy practices.

What GAO Recommends

Since this report examines private companies' use of location data, GAO is not making recommendations to federal agencies. The Department of Commerce, Federal Trade Commission, and the selected companies provided technical comments, which GAO incorporated as appropriate.

View GAO-14-81. For more information, contact Lori Rectanus at (202) 512-2834 or rectanusl@gao.gov.

What GAO Found

Representatives from all 10 selected companies—auto manufacturers, portable navigation device (PND) companies, and developers of map and navigation applications for mobile devices—said they collect location data to provide consumers with location-based services. For example, companies collect location data to provide turn-by-turn directions. Nine companies share location data with third-party companies, such as traffic information providers, to provide services to consumers. Representatives from two companies said they share data where personally identifiable information has been removed (de-identified data) for purposes beyond providing services (e.g., for research), although such purposes are not always disclosed to consumers. All company representatives said that they do not share personally identifiable location data with or sell such data to marketing companies or data brokers.

All 10 selected companies have taken steps consistent with some, but not all, industry-recommended privacy practices. In addition, the companies' privacy practices were, in certain instances, unclear, which could make it difficult for consumers to understand the privacy risks that may exist.

- Disclosures: Consistent with recommended practices, all selected companies disclose that they collect and share location data. However, inconsistent with recommended practices, nine companies' disclosures provide reasons for collecting data that are broadly worded (e.g., the stated reasons for collecting location data were not exhaustive), and five companies' disclosures do not describe the purposes for sharing de-identified location data. Without clear disclosures, risks increase that data may be collected or shared for purposes that the consumer is not expecting or might not have agreed to.
- Consent and controls: Consistent with recommended practices, all selected companies obtain consumer consent to collect location data and obtain this consent in various ways. In addition, all companies offered consumers some controls over location data collection. However, if companies retained data, they did not allow consumers to request that their data be deleted, which is a recommended practice. Without the ability to delete data, consumers are unable to prevent the use or retention of their data, should they wish to do so.
- Safeguards and retention: All selected companies take steps to safeguard location data—a recommended practice—but use different de-identification methods that affect the extent to which consumers may be re-identified and exposed to privacy risks. Also, there is wide variation in how long companies retain vehicle-specific or personally identifiable location data. To the extent that a company's de-identification methods allow a consumer to be identified or that identifiable data are retained, risks increase that location data may be used in ways consumers did not intend or may be vulnerable to unauthorized access.
- Accountability: All selected companies disclose to consumers or take steps to protect location data that they share with third parties; such efforts are consistent with recommended practices. However, inconsistent with recommended practices, none of the selected companies disclose to consumers how they hold themselves and their employees accountable. The companies told GAO that internal company policies serve this function.