September 2012

MOBILE DEVICE LOCATION DATA

Additional Federal Actions Could Help Protect Consumer Privacy

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-903, a report to the Chairman, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate

Why GAO Did This Study

Smartphones can provide services based on consumers' location, raising potential privacy risks if companies use or share location data without consumers' knowledge. FTC enforces prohibitions against unfair and deceptive practices, and NTIA sets national telecommunications policy. GAO was asked to examine this issue. GAO reviewed (1) how mobile industry companies collect location data, why they share these data, and how this affects consumers; (2) actions private sector entities have taken to protect consumers' privacy and ensure security of location data; and (3) actions federal agencies have taken to protect consumer privacy and what additional federal efforts, if any, are needed. GAO analyzed policies and interviewed representatives of mobile industry companies, reviewed documents and interviewed officials from federal agencies, and interviewed representatives from industry associations and privacy advocates.

What GAO Recommends

GAO recommends that NTIA work with stakeholders to outline specific goals, milestones, and performance measures for its process to develop industry codes of conduct and that FTC consider issuing guidance on mobile companies' appropriate actions to protect location data privacy. Because the agencies had concerns about certain aspects of GAO's draft recommendations, GAO revised them by including that NTIA should work with stakeholders in the process to develop industry codes and removing from the draft FTC recommendation that the guidance should include how FTC will enforce the prohibition against unfair practices.

View GAO-12-903. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Using several methods of varying precision, mobile industry companies collect location data and use or share that data to provide users with location-based services, offer improved services, and increase revenue through targeted advertising. Location-based services provide consumers access to applications such as real-time navigation aids, access to free or reduced-cost mobile applications, and faster response from emergency services, among other potential benefits. However, the collection and sharing of location data also pose privacy risks. Specifically, privacy advocates said that consumers: (1) are generally unaware of how their location data are shared with and used by third parties; (2) could be subject to increased surveillance when location data are shared with law enforcement; and (3) could be at higher risk of identity theft or threats to personal safety when companies retain location data for long periods or share data with third parties that do not adequately protect them.

Industry associations and privacy advocates have developed recommended practices for companies to protect consumers' privacy while using mobile location data, but companies have not consistently implemented such practices. Recommended practices include clearly disclosing to consumers that a company is collecting location data and how it will use them, as well as identifying third parties that companies share location data with and the reasons for doing so. Companies GAO examined disclosed in their privacy policies that the companies were collecting consumers' location data, but did not clearly state how the companies were using these data or what third parties they may share them with. For example, some companies' policies stated they collected location data and listed uses for personal information, but did not state clearly whether companies considered location to be personal information. Furthermore, although policies stated that companies shared location data with third parties, they were sometimes vague about which types of companies these were and why they were sharing the data. Lacking clear information, consumers faced with making a decision about whether to allow companies to collect, use, and share data on their location would be unable to effectively judge whether the uses of their location data might violate their privacy.

Federal agencies have held educational outreach events, developed reports with recommendations aimed at protecting consumer privacy, and developed some guidance on certain aspects of mobile privacy. The Department of Commerce's National Telecommunications and Information Administration (NTIA) is implementing an administration-proposed effort to bring industry, advocacy, and government stakeholders together to develop codes of conduct for industry to address Internet consumer privacy issues generally. However, NTIA has not set specific goals, milestones, and performance measures for this effort. Consequently, it is unclear if or when the process would address mobile location privacy. Furthermore, the Federal Trade Commission (FTC) could enforce adherence to the codes if companies adopted them, but since adoption is voluntary, there is no guarantee companies would adopt the resulting codes. While FTC has issued some guidance to address mobile location privacy issues, it has not issued comprehensive guidance that could inform companies of the Commission's views on the appropriate actions companies should take to protect consumers' mobile location data privacy.