April 2016

# SMARTPHONE DATA

## Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking

GAO Highlights

Highlights of GAO-16-317, a report to congressional requesters

### Why GAO Did This Study

Smartphone tracking apps exist that allow a person to not only surreptitiously track another person's smartphone location information, but also surreptitiously intercept the smartphone's communications—such as texts, e-mails, and phone calls. This type of monitoring—without a person's knowledge or consent—can present serious safety and privacy risks.

GAO was asked to review issues around the use of surreptitious smartphone tracking apps. This report examines (1) how companies are marketing smartphone tracking apps on their websites, (2) concerns selected stakeholders have about the use of tracking apps to facilitate stalking, and (3) actions the federal government has taken or could take to protect individuals from the use of surreptitious tracking apps. GAO identified 40 smartphone tracking apps and analyzed their websites' marketing language. GAO interviewed stakeholders selected for their knowledge in this area, including academics; privacy, industry, and domestic violence associations; and tracking app and other companies. GAO also interviewed representatives of five federal agencies.

GAO is not making any recommendations in this report. The Federal Trade Commission, the Department of Health & Human Services, and DOJ reviewed a draft of this report and provided technical comments and clarifications that GAO incorporated as appropriate. The Federal Communications Commission and the Department of Commerce did not have any comments on the report.

View GAO-16-317. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

### What GAO Found

GAO found that the majority of the reviewed websites for smartphone tracking applications (apps) marketed their products to parents or employers to track the location of their children or employees, respectively, or to monitor them in other ways, such as intercepting their smartphone communications. Several tracking apps were marketed to individuals for the purpose of tracking or intercepting the communications of an intimate partner to determine if that partner was cheating. About one-third of the websites marketed their tracking apps as surreptitious, specifically to track the location and intercept the smartphone communications of children, employees, or intimate partners without their knowledge or consent.

The key concerns of the stakeholders with whom GAO spoke—including domestic violence groups, privacy groups, and academics—were questions about: (1) the applicability of current federal laws to the manufacture, sale, and use of surreptitious tracking apps; (2) the limited enforcement of current laws; and (3) the need for additional education about tracking apps. GAO found that some federal laws apply or potentially apply to smartphone tracking apps, particularly those that surreptitiously intercept communications such as e-mails or texts, but may not apply to some instances involving surreptitiously tracking location. Statutes that may be applicable to surreptitious tracking apps, depending on the circumstances of their sale or use, are statutes related to wiretapping, unfair or deceptive trade practices, computer fraud, and stalking. Stakeholders also expressed concerns over what they perceived to be limited enforcement of laws related to tracking apps and stalking. Some of these stakeholders believed it was important to prosecute companies that manufacture surreptitious tracking apps and market them for the purpose of spying. Domestic violence groups stated that additional education of law enforcement officials and consumers about how to protect against, detect, and remove tracking apps is needed.

The federal government has undertaken educational, enforcement, and legislative efforts to protect individuals from the use of surreptitious tracking apps, but stakeholders differed over whether current federal laws need to be strengthened to combat stalking. Educational efforts by the Department of Justice (DOJ) have included funding for the Stalking Resource Center, which trains law enforcement officers, victim service professionals, policymakers, and researchers on the use of technology in stalking. With regard to enforcement, DOJ has prosecuted a manufacturer and an individual under the federal wiretap statute for the manufacture or use of a surreptitious tracking app. Some stakeholders believed the federal wiretap statute should be amended to explicitly include the interception of location data and DOJ has proposed amending the statute to allow for the forfeiture of proceeds from the sale of smartphone tracking apps and to make the sale of such apps a predicate offense for money laundering. Stakeholders differed in their opinions on the applicability and strengths of the relevant federal laws and the need for legislative action. Some industry stakeholders were concerned that legislative actions could be overly broad and harm legitimate uses of tracking apps. However, stakeholders generally agreed that location data can be highly personal information and are deserving of privacy protections.