United States Government Accountability Office

Report to Congressional Requesters

April 2016

SMARTPHONE DATA

Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking

Accessible Version

GAO-16-317

GAO Highlights

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

April 2016

SMARTPHONE DATA

Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking

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.

Contents

Tables

Figures

Abbreviations

CDC	Centers for Disease Control and Prevention
CFAA	Computer Fraud and Abuse Act of 1986
COPPA	Children's Online Privacy and Protection Act
DOJ	U. S. Department of Justice
FCC	Federal Communications Commission
FIP	Fair Information Practice
FTC	Federal Trade Commission
GPS	Global Positioning System
HHS	Department of Health & Human Services
NCVS	National Crime Victimization Survey
NISVS	National Intimate Partner and Sexual Violence Survey
NNEDV	National Network to End Domestic Violence

NTIA	National Telecommunications and Information Administration
OVW	Office of Violence against Women
VAWA	Violence against Women Reauthorization Act of 2013

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

April 21, 2016

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate

The Honorable Al Franken
Ranking Member
Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate

The popularity of smartphones and the use of smartphone applications (apps) that access the phone's location data have grown significantly in recent years.[1] Consumers increasingly rely on location-based services, such as "find my phone" apps for lost phones or mapping apps that provide directions, or elect to share their location data with others through social media apps. But while many apps involve individuals using the location of their own phones, apps exist that allow individuals to access and track the location of someone else's phone or other mobile device, such as a tablet. These tracking apps can be useful in a variety of ways, such as, for example, allowing consenting spouses to know each other's locations. However, location data from mobile devices can be highly personal, including information about where a person lives, goes to school, or attends church, or whether a person has visited a bar, a psychiatrist, an attorney, or a former boyfriend's house. Moreover, certain tracking apps allow for the *surreptitious* collection and transmission of a person's smartphone location information and, in some cases, also allow for the surreptitious interception of the person's communications—such as texts, e-mails, and phone calls. Such monitoring can present a threat to a person's safety and privacy and can be used as a tool that facilitates stalking. According to the Centers for Disease Control and Prevention's (CDC) *National Intimate Partner and Sexual Violence Survey Summary Report of 2011*, roughly 7.5-million people reported that they had been stalked in the 12

[1]According to Pew Research, as of October 2015, 68 percent of U.S. adults own a smartphone, up from 35 percent in 2011 when Pew Research first began examining smartphone adoption.

months preceding the survey.[2] In a 2012 survey of over 750 victims' service agencies conducted by the National Network to End Domestic Violence, 72 percent of the agencies reported that abusers tracked victims via technologies using Global Positioning System (GPS) information, which would include smartphone apps.[3] Instances of such tracking resulting in domestic violence have been reported. For example, in August 2014 in San Angelo, Texas, a man was sentenced to 99 years in prison after using a tracking app to locate his wife at another man's home, where he killed her.

In support of the Judiciary Committee's ongoing work on privacy and technology, you asked that we examine the availability of smartphone tracking apps and any federal government actions taken to protect consumers from the surreptitious use of them. For this report, we addressed the following questions: (1) How are companies marketing their tracking apps on their websites? (2) What concerns do selected stakeholders have about the use of tracking apps to facilitate stalking? (3) What actions has the federal government taken to protect individuals from the use of surreptitious tracking apps, and what do the selected stakeholders believe are possible further actions that could be taken?

For each of these questions, we focused on tracking apps that are installed on smartphones and conducted a literature search to identify relevant articles and other information concerning tracking apps.[4] To determine how companies are marketing their tracking apps, we combined the results of our literature search with the results of our own Internet searches to develop a list of companies that are marketing tracking apps. We identified 40 companies that were marketing tracking apps at the time

[2]The survey was sponsored by CDC's Division of Violence Prevention. Located within CDC's National Center for Injury Prevention and Control, the Division of Violence Prevention's mission is to prevent injuries and death caused by violence.

[3]According to the National Network to End Domestic Violence, it is an organization dedicated to creating a social, political, and economic environment in which violence against women no longer exists. Founded in 1990, it represents 56 state and territory domestic violence coalitions who in turn represent nearly 2,000 local domestic violence service providers across the United States.

[4]However, we included within our general scope the consideration of "freestanding" or "slap-on" tracking devices. Freestanding GPS devices would include items such as handheld devices or wearable devices used to track hikers, small devices used to track equipment or merchandise, or devices that could be placed inside or under a car, on a dog's collar, or on any object that someone wanted to track using GPS technology. Such devices could also be used to track a person's location, with or without that person's knowledge.

of our review; these 40 companies may not represent the universe of tracking app companies as there may be some companies we did not identify. We then conducted a content analysis of the marketing language used on the companies' websites regarding their tracking app products. To identify stakeholder concerns about the use of tracking apps to facilitate stalking, we selected and interviewed 20 stakeholders, including representatives of 10 associations and non-profit organizations that advocate for victims of domestic violence, consumers, privacy, civil liberties, technology, and the mobile app industry; 3 academics in the field of privacy law; and representatives of 4 tracking app companies, 2 mobile phone carriers, and 1 smartphone operating system developer. We also met with officials from the CDC (which is located within the Department of Health & Human Services (HHS)), the California Department of Justice, the United States Department of Justice (DOJ), the Federal Communications Commission (FCC), the Federal Trade Commission (FTC), and the Department of Commerce's National Telecommunications and Information Administration (NTIA). The concerns expressed by the stakeholders in this report are not generalizable to all stakeholders in these areas. To identify actions that the federal government has taken to protect individuals from surreptitious tracking apps, we reviewed federal laws, court decisions, federal enforcement actions, congressional testimony, and law review articles. We discussed the issue with all of the stakeholders and government officials to obtain their views about past and current actions, and ideas about possible future actions. See appendix I for more information on our objectives, scope, and methodology, including a list of the stakeholders we interviewed and how we selected them.

We conducted this performance audit from April 2015 to April 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

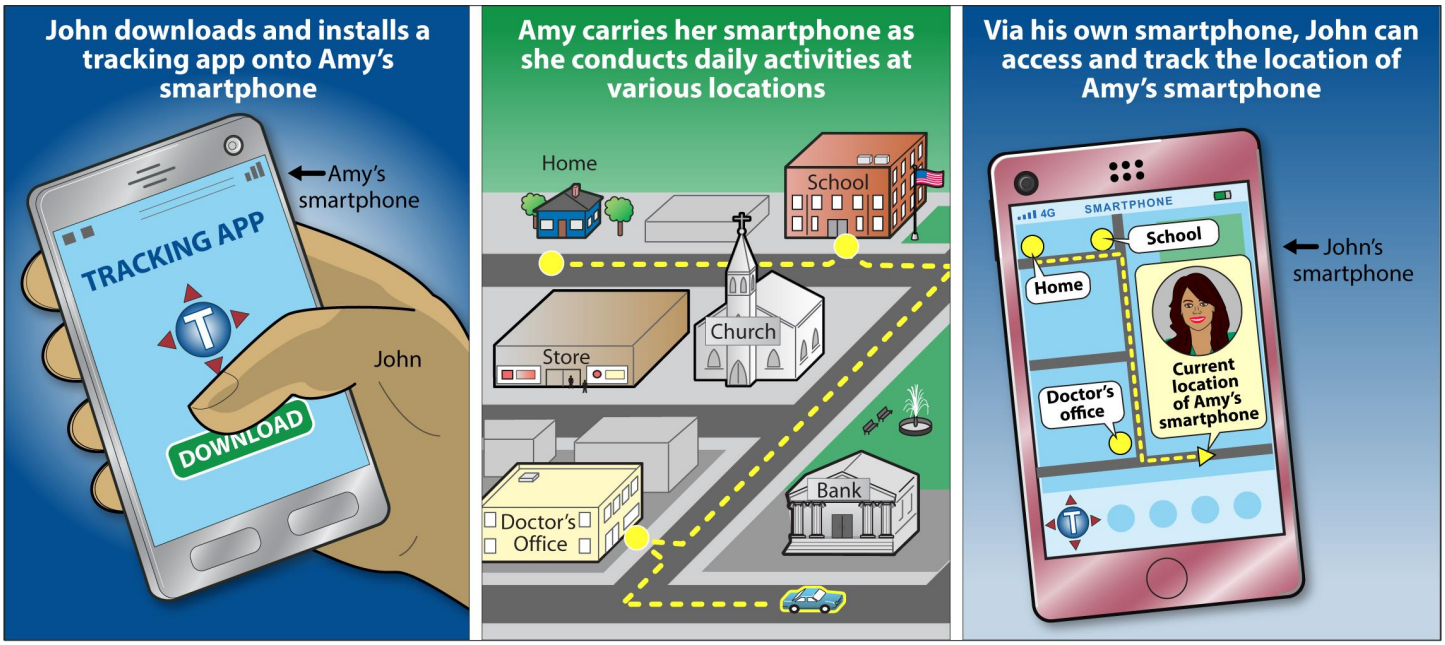
Smartphones[5] allow users to access location-based services based on increasingly precise information about the user's current location determined by GPS and other methods.[6] A tracking app is a computer program and location-based service that consists of two parts. One part is installed on the smartphone of the person being tracked; that part accesses and tracks the device's location and transmits that information. The second part is installed on a computer or another smartphone and is used by the person doing the tracking to receive the transmitted location data and see where the tracked person is or has been over a period of time. The installation of a tracking app on a smartphone can require physical access to the smartphone being tracked.[7] Figure 1 illustrates this technology.

[5]Smartphones combine the telecommunications functions of a mobile phone with the processing power of a computer, creating an Internet-connected mobile device capable of running a variety of software apps for productivity or leisure. See GAO, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*, GAO-12-903 (Washington, D.C.: Sept. 11, 2012), for a description of how a smartphone works.

[6]Other methods to determine a smartphone's location include Assisted-GPS, the triangulation of cell towers, and Wi-Fi access point identification. See figure 2 in GAO-12-903 for a depiction of methods used to collect location information.

[7]However, one tracking app website we reviewed claimed that the app could be installed remotely by calling the target phone with a phone that has the tracking app installed on it. Another tracking app website we reviewed claimed that the tracking app could be installed remotely through the iCloud if the person installing the app had the other smartphone user's iCloud credentials.

Figure 1: Example of How a GPS-Based Smartphone Location Tracking App Operates



Source: GAO. | GAO-16-317

Three types of companies develop or offer smartphone tracking apps.

- Operating system developers: Underlying the various functions of a smartphone is an operating system that acts as a mobile computing platform to run the phone's hardware and software, including apps. The most prevalent smartphone operating systems are developed by Apple (for iPhones) and Google (for Android devices). Some operating systems include a phone location feature that can be used to find a lost or stolen phone.

- Mobile carriers: Carriers provide smartphone users with access to wireless networks for voice and data, generally with a subscription plan. In the United States, four carriers primarily serve customers nationwide: AT&T, Sprint, T-Mobile, and Verizon. These four carriers offer tracking apps aimed at locating all of the phones and devices operating under a single mobile phone account.

- App developers: As the popularity of smartphones has grown, so too has the number of companies developing smartphone apps. These developers range from small, start-up ventures to large, established corporations.

Some tracking apps can be obtained through an app store, such as Apple's App Store or the Google Play Store. Apple and Google have a review and approval process before an app can be offered in their stores. Apps can be rejected by operating system developers for a number of reasons including technical defects or not complying with their licensing agreements. For example, Apple's *App Store Review Guidelines* states that apps must notify users and obtain user consent before collecting, transmitting, or using location data. The Google Play Store policy states that apps that collect information (such as the user's location or behavioral data) without the user's knowledge are prohibited. Some tracking apps not offered in an app store require a user to download the app directly from the developer's website. Some app developers charge a fee for their app while other developers offer them free.

Although tracking apps are generally associated with location tracking, a number of tracking apps offer additional monitoring capabilities, most of which have significant privacy implications. Additional capabilities include, but are not limited to, intercepting phone calls, text messages, and e-mail messages. In addition, some tracking apps are designed to be surreptitious—that is, they operate in a hidden or stealth mode so that the person whose phone is being tracked is unaware that his or her location is being transmitted or that other functions on his or her phone, such as phone calls, e-mails, or texts, are being intercepted. Surreptitious operation generally means the app places no icon on the phone and does not present any permissions or notifications to the user of the phone to alert them to the existence or functioning of the app.

Several federal laws may be relevant to the issue of tracking apps. These laws include:

- The federal wiretap statute: This law makes it illegal, among other things, for an individual to intercept wire, oral, or electronic communications unless an exception applies, such as one of the

parties to the communication has consented to the interception.[8] It also makes it illegal to manufacture, sell, or advertise a device knowing that it is primarily intended for surreptitious interception of communications. This is both a civil and a criminal statute, providing individuals with a private right of action and DOJ with authority to enforce criminal violations of the statute.

- FTC Act Section 5: The core consumer-protection authority in section 5 of the FTC Act enables FTC to bring cases against individuals and companies that it determines have engaged in unfair or deceptive acts or practices in or affecting commerce.[9] FTC can seek injunctive relief in an administrative proceeding or in federal court. FTC may seek monetary relief in the form of restitution and disgorgement of a defendant's proceeds from the alleged unfair or deceptive act or practice, but may not seek civil penalties under Section 5.[10]

- Computer Fraud and Abuse Act of 1986: This law makes it illegal for an individual to access a protected computer without or exceeding authorization, among other things.[11] Federal courts have found that smartphones are considered computers under the act.[12] This is both a

[8]Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act, is commonly referred to as the federal wiretap statute. *See*18 U.S.C. §§ 2510-2522. Electronic communication interception is permitted by "an investigative or law enforcement officer in the ordinary course of his duties." 18 U.S.C. § 2510(5)(a) (2012). The act recognizes that the "interception of [wire and oral] communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice." Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351 § 801(c), 82 Stat. 211 (1968). In addition, "to safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communications has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court." *Id.,* at § 801(d).

[9]15 U.S.C. § 45.

[10]Disgorgement is a monetary remedy designed to deprive a wrong doer of the financial benefits of his or her illegal conduct.

[11]18 U.S.C. § 1030.

[12]*See, e.g., United States v. Kramer*, 631 F.3d 900, 901 (8th Cir. 2011) (the "language of 18 U.S.C. § 1030(e)(1) is exceedingly broad. If a device is an electronic or other high speed data processing device performing logical, arithmetic, or storage functions, it is a computer"); *Desoto v. Bd. of Parks & Rec.*, 64 F. Supp. 3d 1070, 1102 (M.D. Tenn. 2014) (a "protected computer" under the Computer Fraud and Abuse Act has "an exceptionally broad definition that would seem to encompass a BlackBerry" smartphone).

civil and a criminal statute, providing individuals with a private right of action and DOJ with authority to enforce criminal violations of the statute.

- The federal stalking statute: This is a criminal statute, enforced by DOJ, that prohibits individuals from using electronic communications systems or services for stalking purposes, among other things.[13] The statute was most recently amended by the Violence against Women Reauthorization Act of 2013 (VAWA).[14] VAWA includes provisions pertaining to sexual assault, domestic violence, dating violence, and stalking.

There are efforts within two federal agencies to gather more information about technology and stalking. These data collection efforts include:

- National Crime Victimization Survey, Supplemental Victimization Survey: A survey sponsored by DOJ that is designed to enhance knowledge about the extent and nature of stalking in the United States.[15]

- National Intimate Partner and Sexual Violence Survey: An ongoing, national telephone survey conducted by CDC that collects information about instances of sexual violence, stalking, and intimate partner violence among women and men aged 18 or older in the United States.

[13]18 U.S.C. § 2261A(2)(A-B).

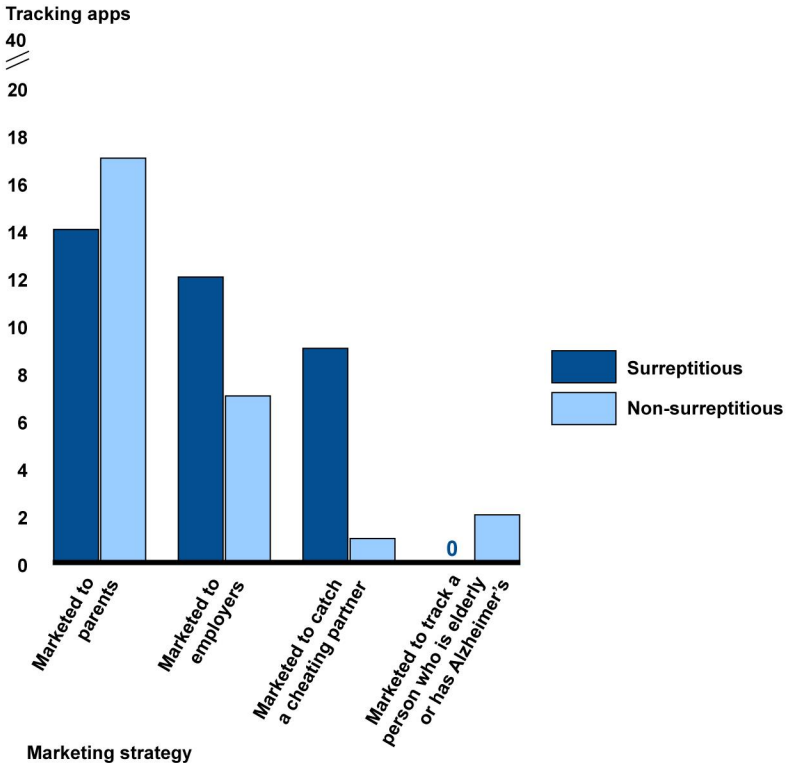
[14]Violence Against Women Reauthorization Act of 2013, Pub. L. No. 113-4, 127 Stat. 54 (2013).

[15]Data from the National Crime Victimization Survey, which focuses more broadly on nonfatal personal crimes and household property crimes and does not focus on stalking, was last published in 2015 using 2014 data. The Supplemental Victimization Survey, a non-routine supplement to the NCVS, focuses on stalking and was last administered in 2006.

Most of the Companies' Websites Marketed Tracking Apps to Parents or Employers; about One-Third Marketed Apps for Surreptitious Tracking

We found that the majority of tracking app websites we reviewed marketed their products to parents or employers to track the location of their children or employees, respectively, or to monitor their children or employees in other ways, such as intercepting their smartphone communications. Several tracking apps were also marketed to individuals for the purpose of tracking or intercepting the communications of an intimate partner to determine if that partner was cheating. Two tracking apps were marketed for monitoring the location of an elderly person or someone with Alzheimer's disease. About one-third of the websites we reviewed (14 of 40) explicitly marketed their product as a surreptitious tracking app, specifically to track the location information and intercept the communications of children, employees, or intimate partners. (See fig. 2.) Some of the websites included language requiring consent of the tracked individual in the terms of use statements and, in the case of some surreptitious apps, we found that the terms of use language sometimes contradicted the marketing language.

Figure 2: Marketing Strategies of 40 Identified Smartphone Tracking App Websites, as of July 2015



Source: GAO analysis. | GAO-16-317

Note: We reviewed 40 websites, but some apps were marketed to more than one type of user and therefore are represented in more than one category of marketing strategy.

Additional Monitoring Capabilities

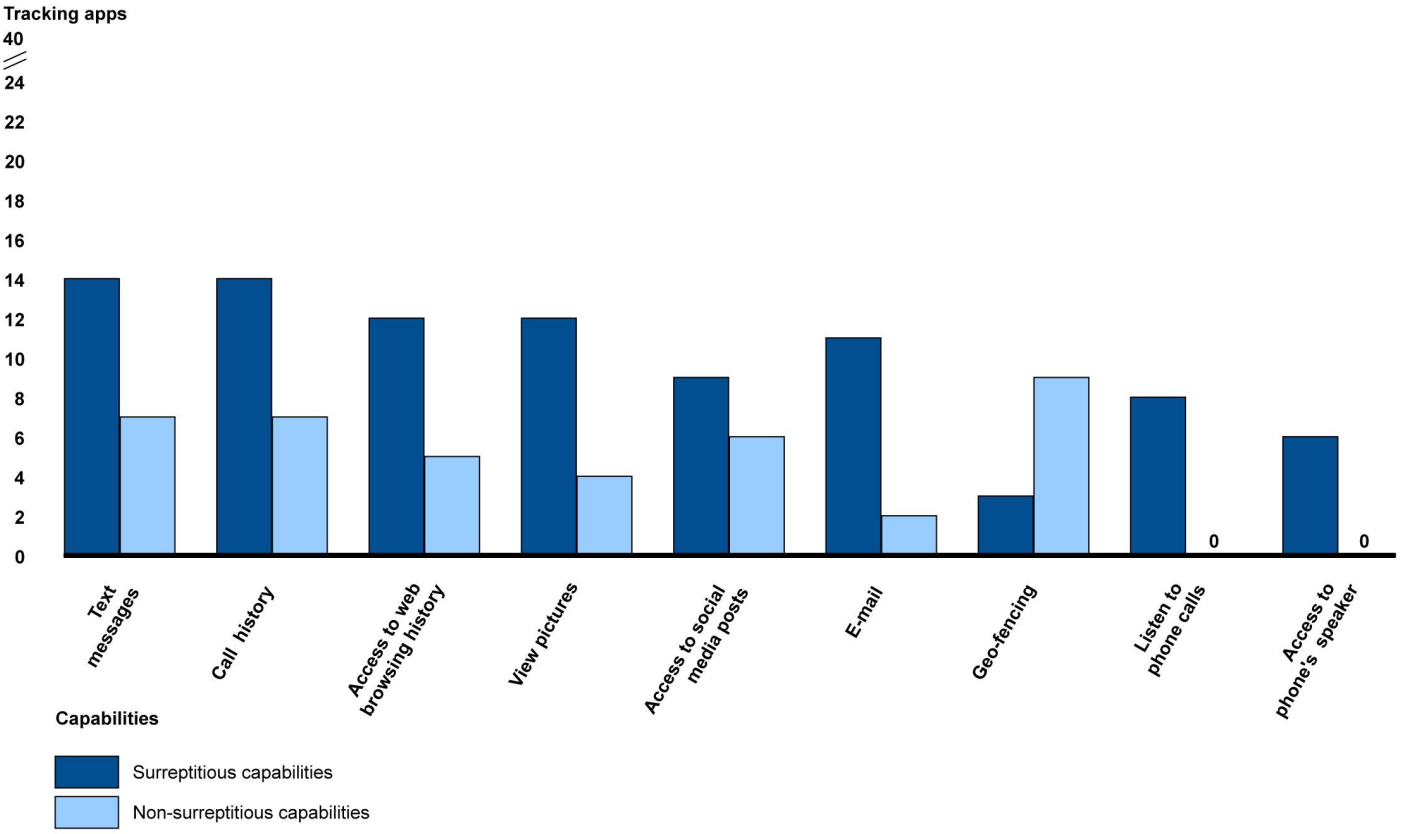
Additional monitoring capabilities that we identified that were being offered by some of the companies along with location tracking included:

- geo-fencing (defining a virtual boundary around the person being tracked);[16]
- intercepting and reading e-mail messages;
- intercepting and reading text messages;
- accessing and reading call history;
- the ability to view pictures on the tracked smartphone;
- the ability to listen in on and record phone calls;
- accessing and reading the phone's web-browsing history;
- accessing and reading social media posts (e.g., Facebook, Twitter); and
- the ability to use the smartphone's speaker to listen in on conversations or other audible sounds taking place in the phone's vicinity.

Based on our review, we found that a number of websites marketed these additional capabilities as surreptitious (see fig. 3). For example, a little over one quarter of the websites we reviewed (11 of 40) marketed the surreptitious interception and reading of e-mail messages. Thirty percent of the websites we reviewed (12 of 40) marketed the surreptitious viewing of pictures and the ability to read the target phone's web-browsing history.

[16]With geo-fencing, the software allows the person doing the tracking to define a geographic boundary around the person being tracked. When the tracked smartphone exits the established boundary, a text message or other alert is sent to the tracker.

Figure 3: Number of 40 Identified Smartphone Tracking App Websites That Marketed Additional Surreptitious and Non-surreptitious Monitoring Capabilities, as of July 2015



Source: GAO analysis. | GAO-16-317

Note: We reviewed 40 websites, but some apps offered multiple capabilities and therefore are represented in multiple categories of capabilities.

Not all smartphone apps we reviewed offered these additional capabilities. We found that 12 of the 40 websites offered apps that only provided location tracking, and of these, none marketed these apps as surreptitious.[17] All current apps marketed as capable of surreptitious interception of communications and location tracking, however, can be used to secretly track an individual's location alone.

[17]Later, during the course our review, we identified additional apps that solely and surreptitiously track location.

Tracking Apps Marketed to Parents

The majority of the tracking apps we reviewed (31 of 40) were marketed to parents to monitor the location of their child's smartphone or to intercept the phone's communications. The websites discussed the safety aspects of tracking children. Of these websites, 17 apps were not marketed as surreptitious. For example, one app's website stated:

- "Child safety is constantly on every parent's mind. Knowing your child's location is key to knowing that your kids are safe. Are they at school? On a fieldtrip? Did they make it to their friend's house? Are they on their way home? [Our] app can answer these typical kid safety questions by telling you where your child is at all times."

Fourteen of the 31 tracking app websites marketing to parents were marketing their app as surreptitious. These websites described their app's ability to track a child's smartphone's location or the app's ability to intercept a child's smartphone's communications without his or her knowledge. For example, one website's marketing material stated:

- "Just install the software on your child's mobile phone, and you can secretly learn the truth about their calls, text messages, and GPS locations."

Tracking Apps Marketed to Employers

Almost half of the tracking apps we reviewed (19 of 40) were marketed to track an employee's location or to intercept an employee's smartphone's communications. These websites touted their products' ability to track the location of an employee's smartphone; about half of the websites specifically mentioned using the app to ensure that employees were conducting company business. Of these websites, 7 were not marketed as surreptitious. For example, one app's website stated:

- "[Our product] can utilize the GPS receiver in your employee's smartphone or tablet to act as a GPS tracker. It monitors GPS locations every 30 minutes and you can get instant tracks by sending an SMS message to your employee's phone. You will get a reply message stating the coordinates at that specific time."

Of the 19 tracking apps we reviewed that were marketed toward employers, 12 were marketed as surreptitious. These apps marketed their ability to track the location of an employee's smartphone without his or her knowledge or the ability to intercept the communications of an employee's smartphone without his or her knowledge. According to one website:

- "As an employer you want to monitor all company owned phones and make sure they are not being misused. Works in complete invisible mode, it will never appear on the monitored phone." [sic – several errors inside quote]

Tracking Apps Marketed to Catch Suspected Cheating Partners

One quarter of the tracking apps we reviewed (10 of 40) were marketed to track a suspected cheating partner. Of these, 9 marketed their app's ability to surreptitiously track an intimate partner's location or intercept communications. According to one of these websites:

- "If your partner is cheating on you and you want to catch your partner red handed. [sic] Then [our product] has the power to do that [sic] for you without letting your partner know about this spying activity."

Tracking Apps Marketed to Track a Person Who Is Elderly or Has Alzheimer's

Two of the 40 tracking apps we reviewed were marketed to track a person who is elderly or has Alzheimer's disease. These apps promoted monitoring the well-being of the elderly person or person with Alzheimer's. Neither app was promoted as surreptitious. For example one website's marketing language stated:

- "Through [our product], caregivers and family members can provide individual's [sic] with Alzheimer's a greater level of independence, while still maintaining their safety and security."

User Consent Requirements in Disclaimers or Terms of Use

Some websites provided a disclaimer or terms of use related to tracking an individual without his or her consent. These disclaimers (disclaiming that the company is marketing the app for surreptitious use) or terms of use included language requiring the consent of the person being tracked before accessing his or her smartphone's location or other functions. The majority of the websites (25 of 40) suggested obtaining the consent of a smartphone's user in the disclaimer or terms of use or explicitly stated that the app should not be used to spy, track, or harass. For example, one website stated:

- "You are required to notify users of the device that they are being monitored. [Our product] is designed for ethical monitoring for parents who wish to monitor their underage children or for employers who wish to monitor their employees with their written consent. The buyer of [our product] must own the smartphone or must have written consent from their children or employees granting them permission to monitor before they install and activate the [product] onto the smartphone." [sic – several errors inside quote]

Disclaimers or Terms of Use That Contradicted a Product's Marketing

Our review found that a number of apps' disclaimers or terms of use contradicted the marketing of the product. Specifically, 13 of the 27 websites that had a disclaimer contradicted the websites' marketing of the services their apps offer. We found that these websites promoted their product's ability to be hidden or stealth, or that the target smartphone's user would be unaware of the tracking activity, yet at the same time, the website's disclaimer stated that the target smartphone's user's consent is required. For example, one website's marketing language stated:

- "One of the best ways to find out if your partner is indeed having an affair is to simply gain access to his or her phone. You would be surprised as to how much information you can find about someone just by accessing their [sic] phone. So how can you monitor cell phone activity without having to physically peak [sic] at the phone at regular intervals? Install [our product]. The software will provide you all the information you need to find out the truth about a suspected affair. And of course, if it turns out your partner is not cheating; [sic] it will bring the two of you closer because you will know that you can trust your partner."

However, the same website's disclaimer stated:

- "[Our product] is designed for monitoring your children or employees on a smartphone you own or have proper consent to monitor (in compliance with applicable laws), and you must inform anyone who uses a device upon which the software is installed that their activity may be monitored. You should NEVER attempt to spy on a cell phone you don't own, monitor your spouse, significant other or adult children with any cell phone monitoring product without the consent and knowledge of such persons. Doing so may be illegal, and violate local, state, and federal laws in your country and you could be subject to civil or criminal penalties. We will cooperate with authorities in investigation of any allegations of misuse."

Stakeholders' Key Concerns Related to Applicability of Federal Laws, Limited Enforcement of Existing Laws, and Need for Additional Education of Law Enforcement Officials and Consumers

Applicability of Current Federal Laws

The applicability of federal laws to the manufacture, sale, and use of surreptitious tracking apps to facilitate stalking was a key concern to stakeholders. Opinions differed on how federal laws apply. Four federal laws were most often discussed by stakeholders as relevant to surreptitious electronic stalking: the federal wiretap statute, the FTC Act, the Computer Fraud and Abuse Act, and the federal stalking statute. (See tables 1 and 2.) The federal wiretap statute has been used to successfully prosecute an individual for actions pertaining to the surreptitious interception of communications and to successfully prosecute a manufacturer for the sale, manufacture, and advertisement of a device primarily useful for the surreptitious interception of communications; in the context of smartphone tracking apps, the other three laws have not been tested in court.

Table 1: Federal Statutes That Have Been Applied to Address the Surreptitious Interception of Communications (E-mail, Text Messages, and Phone Calls) through Smartphone Tracking Apps

Statute	Brief description	How the statute has been applied to address smartphone tracking apps
The Federal Wiretap Statute (18 U.S.C. § 2512)	Section 2512 prohibits any person from intentionally manufacturing, assembling, possessing, or selling any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications. It also prohibits the advertisement of any such device rendered primarily useful for the purpose of surreptitious interception of wire, oral, or electronic communications. Interception is defined by law as pertaining to the content of the communications, and some federal courts have found location information is not content covered by the wiretap statute.	In 2014, under sections 2512(c)(i) and 2512(b) respectively, DOJ prosecuted a manufacturer for illegally advertising and selling a smartphone app that was primarily useful for the purpose of the interception of wire, oral, or electronic communications. The app allowed a user to surreptitiously and remotely monitor the calls, texts, videos, location, and other information of another individual.[a] DOJ also successfully prosecuted an individual in 2014 under section 2512(b)—possession of an interception device transported in interstate commerce. The interception device used was a smartphone equipped with various smartphone tracking apps.[b]
The Federal Wiretap Statute (18 U.S.C. § 2511)	Section 2511 prohibits individuals from intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept, any wire, oral, or electronic communication unless consent is provided. Interception is defined by law as pertaining to the content of the communications, and some federal courts have found that content does not include location information.	DOJ also prosecuted the same individual as above under section 2511 for the surreptitious interception of communications. The defendant confessed to using a smartphone tracking app to activate another user's smartphone's microphone for the purposes of eavesdropping and recording the ongoing conversations of the user's smartphone without the user's knowledge or consent.[c]

Source: GAO analysis. | GAO-16-317

[a]*United States v. Akbar*, No. 1:14-cv-0276 (E.D. Va. Nov. 25, 2014) (Plea Agreement); *see also* Press Release, Department of Justice, Man Pleads Guilty for Selling "StealthGenie" Spyware App and Ordered to Pay $500,000 Fine (Nov. 25, 2014), accessed October 2015, http://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine.

[b]*United States v. Nyunt*, No. 5:14-cr-00530-1 (N.D. Cal. Oct. 17, 2014); Press Release, Department of Justice, California Resident Pleaded Guilty To Wiretapping Law Enforcement Communications And Others (Nov. 10, 2014), accessed December 2015, http://www.justice.gov/usao-ndca/pr/california-resident-pleaded-guilty-wiretapping-law-enforcement-communications-and

[c]Press Release, Department of Justice, California Resident Pleaded Guilty To Wiretapping Law Enforcement Communications And Others (Nov. 10, 2014), accessed December 2015, http://www.justice.gov/usao-ndca/pr/california-resident-pleaded-guilty-wiretapping-law-enforcement-communications-and.

Table 2: Other Federal Statutes That Potentially Apply to the Surreptitious Use of Smartphone Tracking Apps

Potentially applicable statute	Brief description	How the statute may potentially apply to address smartphone tracking apps
Federal Trade Commission (FTC) Act Section 5 (15 U.S.C. § 45)	Section 5 of the FTC Act gives the FTC authority to initiate a civil proceeding when the FTC has reason to believe that a person, partnership, or corporation has been or is using an unfair method of competition or an unfair or deceptive act or practice. Additionally, Section 5 of the FTC Act applies to unfair or deceptive acts involving foreign commerce that cause or are likely to cause reasonably foreseeable injury within the United States, or involve material conduct occurring within the United States.	FTC staff told us that they interpret Section 5 of the FTC Act to extend to the manufacture and sale of smartphone tracking apps that surreptitiously intercept e-mails, text messages, telephone calls, or location information. In 2010, the FTC settled a case with a company that allegedly engaged in surreptitious tracking of a third party's use of his or her computer through computer-based software.[a]
Computer Fraud and Abuse Act of 1986 (18 U.S.C. § 1030)	The statute prohibits any individual who intentionally accesses a computer without authorization or exceeds authorized access from obtaining information from a protected computer, and, if certain aggravating factors are present, may result in imprisonment not to exceed 20 years or a fine or both. A 2008 amendment broadened the definition of a protected computer to include any computers used in or affecting interstate or foreign commerce or communication.	According to stakeholders we interviewed, this statute may potentially apply to individuals who install software on a cellphone that is intended to access e-mail, text messages, phone calls, or location information without or in excess of what is authorized.
Federal Stalking Statute (18 U.S.C. § 2261A)	The statute makes it a felony for someone to use any interactive computer service or electronic communication service or system with the intent to kill, injure, harass, intimidate, or place under surveillance with the intent to kill, injure, harass, or intimidate another person and engage in a course of conduct that places a person in reasonable fear of death or serious bodily injury, or causes, attempts to cause, or would reasonably be expected to cause substantial emotional distress.	According to stakeholders we interviewed, this statute may potentially apply to individuals using smartphone tracking apps to intercept a person's emails, text messages, telephone calls, or location information, who also meet the specified intent and other criteria established in law.

Source: GAO analysis of statutes and stakeholder comments. | GAO-16-317

[a]*FTC v. Cyberspy Software*, *LLC,* No. 6:08-cv-1872-GAP-GJK (M.D. Fla. Apr. 22, 2010).

The Federal Wiretap Statute

DOJ and 10 of the 13 stakeholders we met with who have knowledge of the law mentioned the federal wiretap statute as applicable to address tracking apps that surreptitiously intercept communications such as e-mails, texts, or phone conversations.[18] The federal wiretap statute is codified at sections 2510 to 2522 of title 18 of the U.S. Code. Section 2511 prohibits

[18]These 10 stakeholders included three academics, a carrier, an app developer, two domestic violence prevention organizations, a consumer organization, a civil liberties organization, and a technology policy organization.

individuals from intentionally intercepting wire, oral, or electronic communications. Section 2512 prohibits, among other things, individuals or entities from manufacturing, assembling, possessing, selling, distributing, or advertising any device knowing that is primarily intended for surreptitious interception of wire, oral, or electronic communications in interstate or foreign commerce. Three stakeholders told us that a number of current tracking apps—those that surreptitiously intercept emails, texts, and other communications—currently may be violating both of these sections of the federal wiretap statute. However, 7 of the stakeholders we spoke with stated that they believed the federal wiretap statute was not applicable to the surreptitious tracking of a smartphone's location information.[19] In fact, some federal courts have held that location information does not comprise the substance or content of a communication and thus is not covered by the wiretap statute.[20] According to DOJ officials, applying the wiretap statute to geolocation tracking requires a fact specific determination and depends on what is done to collect such data; however, DOJ officials also stated that charges would most likely be brought under other statutes in such cases.[21]

[19]These five stakeholders included two academics, two domestic violence prevention organizations, and a civil liberties organization.

[20]*See, e.g.*, *United States v. Reed*, 575 F.3d 900, 916 (9th Cir. Cal. 2009) (data that is incidental to the use of a communication device, such as origin or destination, contains no "content"); *In re: iPhone Application Litig.* 844 F. Supp. 2d 1040, 1050-51, 1055 (N.D. Cal. 2012) (personally identifiable information that is automatically generated by the communication, such as geographic location information, does not comprise the substance of meaning of the communication and thus is not interception covered by the federal wiretap statute). *See also*, *In re Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 758 (S.D. Tex. 2005).

[21]Some states also have statutes that prohibit some form of geolocation tracking. For example, Texas, Delaware, and California have statutes that prohibit some form of surreptitious geolocation tracking using a tracking device. Specifically, the Texas and Delaware statutes prohibit the installation of a tracking device on a motor vehicle owned by another. *See* Tex Penal Code Ann. § 1606 (2015); 11 Del. Code Ann. tit. 11 § 1335 (2015). In comparison, the California statute prohibits a person or entity from using a tracking device to determine the location or movement of a person. Cal. Penal Code § 637.7 (2015). Some states have statutes that prohibit the sale of surreptitious interception devices. For example, Pennsylvania prohibits the intentional sale, transfer, or distribution of a device primarily useful for surreptitious interception of communications, while Maine prohibits a person from selling a device commonly used for the interception of communications. *See* 18 PA Cons. Stat. Ann. § 5705 (2015); ME. Rev. Stat. tit. 15 § 710 (2015).

Section 5 of the FTC Act

Another statute mentioned by FTC staff and 6 of the 13 stakeholders with whom we discussed the potential applicability of laws to surreptitious tracking apps was Section 5 of the FTC Act, which gives FTC the authority to challenge companies or individuals that engage in unfair or deceptive acts or practices. [22] FTC may use its authority under Section 5 to challenge practices that occur in the United States or practices involving foreign commerce that cause, or are likely to cause, reasonably foreseeable injury within the United States. Stakeholders we spoke with, as well as staff of the FTC, believed that such authority could apply to manufacturers of a tracking app that either surreptitiously tracks location data or intercepts communications and that was advertised for the specific use of tracking an adult without his or her knowledge and consent. The harm in these cases would not be suffered by the person purchasing the product, but by third parties to the transaction. Although a third party would experience the harm in these transactions, FTC staff interpreted Section 5 of the FTC Act as applying to such a scenario, and FTC has applied Section 5 of the FTC Act in an analogous case in the past.[23] Other stakeholders we spoke with also believed Section 5 would potentially apply in these circumstances.

Computer Fraud and Abuse Act

The third statute mentioned by DOJ and 6 of the 13 stakeholders with whom we spoke was the Computer Fraud and Abuse Act (CFAA).[24] These stakeholders believed the CFAA could potentially be used to prosecute an individual who has accessed the smartphone of another person without or in excess of authorization, and installed an app that either accessed location information to track the person or intercepted the smartphone's communications. All 6 stakeholders believed that the action of accessing another person's smartphone to install a tracking app without their knowledge would constitute a violation of the CFAA. DOJ staff noted that both physical and remote access would be a violation of the CFAA. Two of these stakeholders pointed out, however, that a violation would be more difficult to prove in cases where the two parties involved were in a relationship where they had a shared phone plan or the same wireless

[22]These seven stakeholders included two academics, FTC staff, a consumer organization, a civil liberties organization, a technology policy organization, and a domestic violence organization.

[23]For example, FTC settled a case with a software company that allegedly advertised and sold "keylogger" software used to surreptitiously record a third party's use of his or her computer. *FTC v. Cyberspy Software, LLC*, No. 6:08-cv-1872-GAP-GJK (M.D. Fla. Apr. 22, 2010).

[24]The six stakeholders included two academics, a civil liberties group, a technology policy group, a domestic violence prevention organization, and a technology association.

account and the person installing the app was the account holder. In such cases, the person might be able to argue that, as the holder of the account, he or she was an authorized user and had a right to access and install an app on the phone. One stakeholder noted that with the CFAA, it would be necessary—but difficult—to prove that the app is on the phone and that the defendant installed it. One stakeholder also pointed out that the impetus behind the act was to prevent computer hacking so it would not be the most straightforward way to prosecute an individual for electronic stalking activities.

The Federal Stalking Statute

The final statute discussed by DOJ and 5 of 13 stakeholders was the federal stalking statute, which they believed potentially may be used to bring criminal charges against a stalker who used a tracking app to track the victim's location or intercept the victim's communications.[25] However, some stakeholders stated that the federal stalking statute is rarely used in such cases, as most stalking cases are brought under state law. According to the stakeholders, all 50 states have stalking statutes, but they differ, and some might address the use of tracking apps and other forms of electronic or cyberstalking better than others. One stakeholder told us that prior to 2013, the federal stalking statute was difficult to apply because it required that the stalking activities cross state lines or that the stalker and victim reside in different jurisdictions, which is often not the case in domestic situations. However, the Violence Against Women Reauthorization Act of 2013 amended the federal stalking statute to permit prosecutors to pursue cyberstalking cases regardless of where the victim and offender reside. The revised statute allows prosecutors to also focus on whether the offender used an electronic communication system capable of interstate commerce, such as a smartphone, to stalk the victim. According to a DOJ official, this revision has modernized the federal stalking statute by not requiring that the stalking activities be committed across state lines.[26]

Limited Enforcement of Existing Laws

Domestic violence prevention groups, a privacy group, a consumer group, and academics told us that they believe that there is not enough

[25]The five stakeholders included two academics, two carriers, and a domestic violence group.

[26]Bea Hanson, Principal Deputy Director, Office on Violence Against Women, Department of Justice, *The Location Privacy Protection Act of 2014* testimony before the Subcommittee on Privacy, Technology, and the Law, Committee on the Judiciary, 113th Cong. 6, 2014.

enforcement of either federal or state existing laws related to smartphone tracking apps and stalking. Three of these stakeholders believed it was important to prosecute the companies that are manufacturing surreptitious tracking apps and marketing them to individuals for the purpose of spying on others. To date, at the federal level, DOJ has brought one case against the seller of a tracking app under the federal wiretap statute.[27] FTC has not brought any cases against a surreptitious smartphone tracking app developer under Section 5 of the FTC Act.

While most stalking cases are brought at the state level, according to an official from the National Association of Attorneys General, they are brought against individuals for stalking behaviors rather than against companies that manufacturer tracking apps. Some states have state law versions of the federal wiretap statute and may be able to prosecute companies making or selling surreptitious apps under those state laws. One high-ranking state official in the state office of attorney general cited the following challenges to prosecuting cases against companies producing such apps under state law: (1) many companies are based overseas, thus operating outside of a state's jurisdiction; (2) the time it takes to build a case against a company gives the company time to change its name, its marketing strategy, or the design of the app, making states reluctant to focus on building a case for fear that resources would be wasted; and (3) lack of resources to fully understand or hire technical experts to explain how an app functions. A few stakeholders also expressed concerns about a lack of understanding by law enforcement

[27]In that case, a developer created, advertised, and sold a mobile app that surreptitiously tracked the location data of phones on which it was installed, and also surreptitiously intercepted communications to and from the phone, such as text messages and e-mails. *United States v. Akbar*, No. 1:14-cv-0276 (E.D. Va. Nov. 25, 2014) (Plea Agreement); see also Press Release, Department of Justice, Man Pleads Guilty for Selling "StealthGenie" Spyware App and Ordered to Pay $500,000 Fine (Nov. 25, 2014), accessed December 2015, http://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine. DOJ successfully demonstrated that the defendant, a Danish citizen, had advertised and sold a smartphone tracking app primarily used for the surreptitious interception of wire, oral, or electronic communications. *Id*. In addition, as mentioned in table 1, DOJ has successfully prosecuted an individual under the wiretap statute for the illegal interception of communications, as well as for the possession of a device primarily useful for the surreptitious interception of communications. *See United States v. Nyunt*, No. 5:14-cr-00530-1 (N.D. Cal. Oct. 17, 2014); Press Release, Department of Justice, California Resident Pleaded Guilty To Wiretapping Law Enforcement Communications And Others (Nov. 10, 2014), accessed October 2015, http://www.justice.gov/usao-ndca/pr/california-resident-pleaded-guilty-wiretapping-law-enforcement-communications-and.

officials about current state laws and their applicability to smartphone tracking apps.

Need for Additional Education about How Tracking Apps Work

Domestic violence prevention groups told us, and a Minnesota detective has testified before Congress, that additional training of local law enforcement officials about how to protect against, detect, and remove tracking apps is needed. The National Network to End Domestic Violence (NNEDV) works with local law enforcement officials to educate them about how to identify whether a tracking app is hidden on a phone and about how state and federal laws apply. However, according to representatives of the organization, its funding only allows it to reach a small portion of law enforcement needing the training. According to NNEDV, training to detect and remove tracking apps is needed and has been requested by officers and advocates in all states, U.S. territories, and tribal communities. A 2012 NNEDV survey found that 72 percent of victim services providers want more training and resources concerning electronic-stalking technologies and safety strategies. NNEDV has testified that it must turn down two to three requests for training on electronic-stalking prevention, awareness, and detection for every one training request it is able to fulfill. Similarly, a detective from Anoka County, Minnesota, with expertise in computer forensics testified in June 2014 before the Subcommittee on Privacy, Technology, and the Law of the Senate Judiciary Committee that most local law enforcement entities do not have the resources, staffing time, training, or forensic equipment to examine mobile devices for tracking apps operating in stealth mode.[28] He explained that demand and outside requests for his expertise is growing, noting that he conducted 377 exams in 2013, up 220 percent from 2011.

In addition, the Stalking Resource Center and NNEDV have pointed out the importance of educating potential victims about how smartphone technologies can be harmful to users and how users can protect themselves from these risks. Specifically, the Stalking Resource Center and NNEDV have noted the importance of educating consumers about:

[28]Brian Hill, Detective, Criminal Investigations Division, Anoka County Sheriff's Office, testimony before the Subcommittee on Privacy, Technology and the Law, Senate Judiciary Committee, 113th Cong. 3, 2014, accessed May 2015, http://www.judiciary.senate.gov/imo/media/doc/06-04-14HillTestimony.

- how their devices work;
- how someone might use the technology in a nefarious manner;
- what types of information are collected by the device;
- what steps a victim can take if he or she believes someone is using the technology against them, including how to remove spyware apps from the device; and
- how victims can report abuse.

The Federal Government Has Undertaken Some Legislative, Enforcement, Education, and Data Collection Efforts; Stakeholders Differed Over Whether Current Federal Laws Need to be Strengthened to Combat Stalking

Legislative and Enforcement Actions

As indicated in table 1, an individual and a manufacturer have been prosecuted under the federal wiretap statute. In October of 2014, DOJ indicted an individual under section 2511 of title 18 for the surreptitious interception of communications and under section 2512 (1) (b) for the possession of an interception device, transported in interstate commerce. The defendant pled guilty to each count, having admitted to installing various smartphone tracking apps on the smartphone of another user. Specifically, the defendant had activated the microphone of the user's smartphone, eavesdropping and recording conversations occurring within

the proximity of the smartphone. Additionally, the defendant had intercepted private e-mail communications and texts from individuals who had not given consent and were unaware of the interceptions. In February 2015, the defendant was sentenced to 3 years of probation for each count, to be served concurrently.

As discussed earlier, in September 2014, federal prosecutors at DOJ brought charges against the chief executive officer of the company that sold StealthGenie under section 2512 of title 18. The StealthGenie mobile app surreptitiously tracked the location data of phones on which it was installed and also surreptitiously intercepted communications to and from the phone, such as text messages and e-mails. DOJ successfully demonstrated that the defendant had advertised and sold a smartphone tracking app primarily used for the surreptitious interception of wire, oral, or electronic communications. After pleading guilty, the defendant was sentenced to time served and ordered to pay a fine of $500,000. Additionally, the defendant was ordered to surrender the tracking app's source code to the U.S. government.

Stakeholders with whom we spoke identified two actions that they believed could be taken involving the federal wiretap statute that would further protect against stalking via tracking apps. First, three stakeholders felt that DOJ should bring more cases against existing stalking app developers to help curb the availability of such devices. Our analysis identified a number of companies that continue to manufacture and market tracking apps that surreptitiously intercept smartphone communications. While DOJ staff declined to indicate whether they had current tracking app cases or investigations, they stated that they are "active in this area." Additionally DOJ officials stated to us that DOJ has prosecuted stalking behavior under the federal stalking statute that involved GPS tracking, but not GPS tracking on a smartphone. However, DOJ staff pointed out that the department has numerous competing priorities for resources and investigates and brings cases involving many types of serious offenses, including terrorism and other violent crimes. DOJ's Principal Deputy Director of the Office of Violence against Women testified in June 2014 that most stalking offenses are better handled by state and local police departments and prosecutors under state stalking laws. When speaking with us, a senior DOJ official explained that cybercrimes require technical expertise, involve the collection of electronic evidence, and can present novel legal questions. All of these factors can make cybercrime investigations time-consuming and difficult given the high legal burden for criminal prosecutions.

The second suggested action involving the federal wiretap statute that two domestic violence groups, three academics, and one civil liberty group identified was for Congress to amend the statute to explicitly include the tracking of location data. Most of the stakeholders who discussed this option believed that it would generally entail bringing location information into the definition of the communications covered by the statute. These stakeholders pointed out that beyond the risk of serious physical violence that can be involved in some cases, surreptitious tracking of someone's location represents an invasion of privacy akin to the interception of private communications. As previously mentioned, location data from mobile devices can be highly personal, including information about where a person lives, goes to school, or attends church, or other personal information. Congress recognized this potential sensitivity when it enacted the Children's Online Privacy and Protection Act (COPPA).[29] One academic with whom we met believed that the COPPA definition of location data would be a good model for Congress to follow in any amendment of the federal wiretap statute, and would help promote uniformity among privacy laws. Stakeholders said that a benefit of amending the act would be to make it applicable to apps or devices that surreptitiously track only location data. According to stakeholders, amending section 2512 of the statute could explicitly bring the manufacturing and marketing of apps or devices primarily intended to surreptitiously track someone's location data under the purview of the act, while amending section 2511 could get at the use by stalkers of surreptitious tracking apps that track location only. Although our content analysis of the marketing of tracking apps did not identify any that offered only location tracking services and were also marketed as surreptitious, we identified two such apps later in the course of our review. The risk exists that such apps can be manufactured, sold, and used to track someone's location without that person's knowledge and consent. As stated earlier, some federal courts have held that location information is not covered by the federal wiretap statute, and a number of stakeholders agreed.

[29]COPPA includes "a home or other physical address including street name and name of a city or town" in the definition of "personal information" that websites and online services that are directed toward children, as well as those with actual knowledge that they are dealing with a child, may collect only with parental consent. 15 U.S.C. § 6501(8)(B). In the implementing regulations, the FTC has specified that "personal information" also includes "[g]eolocation information sufficient to identify street name and name of a city or town." 16 C.F.R. § 312.2.

In addition, DOJ has identified other concerns with using the wiretap statute as currently written to prosecute manufacturers and thus has proposed legislative changes to Congress that DOJ believes would allow it to further address the deployment and manufacturing of surreptitious tracking apps. According to DOJ staff, its proposed changes would allow DOJ to reach the proceeds that companies obtain from the sale of surreptitious tracking apps. Most importantly, DOJ believes such changes in the law could help reduce the financial motivation to manufacture and sell these types of apps. Specifically, DOJ has proposed amending section 2513 of title 18, which currently allows for the forfeiture of the surreptitious interception device for smartphone tracking apps, to also allow for the forfeiture of proceeds from the sale of smartphone tracking apps.[30] In addition, DOJ has proposed amending section 1956 of title 18, which involves predicates for money-laundering offenses. [31] DOJ would like to have the ability to charge the manufacturers and sellers of surreptitious smartphone tracking apps with money-laundering offenses when applicable. Under current law, the selling of surreptitious tracking apps is not a predicate offense for a charge of money laundering, so DOJ cannot bring such charges. DOJ staff pointed out that another complication with prosecuting many of these companies is that the individuals running the companies often live abroad. This makes prosecuting the individuals themselves difficult unless they come to the United States.[32] The legislative changes proposed by DOJ, according to DOJ staff, would allow them to reach the financial gains from the sale of surreptitious tracking apps regardless of where company officials reside.

Although DOJ has undertaken two prosecutions involving the federal wiretap statute with regard to surreptitious smartphone tracking apps, FTC has not brought any cases under its Section 5 authority against companies that market such surreptitious tracking apps. Four stakeholders with whom we spoke believed that FTC could do more to

[30]Letter from Peter J. Kadzik, Assistant Attorney General, Department of Justice, to Al Franken, United States Senator (Dec.7, 2015).

[31]A "predicate offense" can be described as a crime that is a component of a more serious offense. For example, in the case of money laundering, the crime that produces the funds that are to be laundered is the predicate offense. *See* Eric A. Fisher, Cong. Research Serv., R42114, *Federal Laws Relating To Cybersecurity: Overview and Discussion of Proposed Revisions* 50 (2013).

[32]The defendant in the StealthGenie case was arrested when he came into the United States.

take action against developers of surreptitious tracking apps. Stakeholders stated that such apps are inherently unfair and deceptive, as there is no legitimate need for a tracking app to operate in stealth or be designed to be hidden or undetectable. FTC officials pointed out that FTC is a civil law enforcement agency and has no criminal jurisdiction. FTC staff further explained that since many of these companies are located overseas, there are practical problems in enforcing injunctive relief abroad. In addition, when we spoke with FTC staff, they emphasized that although the agency has had no cases involving manufacturers of surreptitious tracking apps, the agency has in several instances used its core consumer-protection authority under Section 5 to bring enforcement actions against companies responsible for surreptitious computer software and mobile apps that collected consumers' personal information and location data without their consent.[33]

Four industry stakeholders we met with, however, did not believe that legislative changes or government actions were needed to protect individuals against the use of surreptitious tracking apps and instead believed that the solution to the availability and use of surreptitious tracking apps was better handled through voluntary industry action. Two of these stakeholders pointed to several industry standards that call for notification and consent whenever location information is being accessed and transmitted. For example, the Fair Information Practices (FIP) are

[33]For example, FTC settled a case with a software company that allegedly advertised and sold "keylogger" software used to surreptitiously record a third party's use of his or her computer. The software enabled a consumer to surreptitiously record a third party's websites visited, passwords used, and keystrokes typed on his or her computer. *FTC v. Cyberspy Software, LLC,* No. 6:08-cv-1872-GAP-GJK (M.D. Fla. Apr. 22, 2010). FTC also settled a case with a messaging app company that allegedly made misrepresentations about transmitting location information from users of its app, even though its privacy policy claimed that it did not track users or access such information. *Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 31, 2014) (Decision and Order), accessed December 2015, https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf. FTC also settled a case with a national rent-to-own company that allegedly installed monitoring software on its computers to track the physical location of the rented computers without acquiring the consent or knowledge of the renter. *Aaron's, Inc.*, No. C-4442 (F.T.C. Mar. 11, 2014) (Decision and Order), accessed December 2015, https://www.ftc.gov/system/files/documents/cases/140311aaronsdo.pdf. FTC also settled with a case with the developer of a flashlight app—one of the most popular apps for the Android platform—for allegedly failing to disclose that the app transmitted the device's location data to third parties without the knowledge or consent of the consumer. *Goldenshores Technologies, LLC*, No. C-4446 (F.T.C. Apr. 9, 2014) (Decision and Order), accessed December 2015, https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf.

widely accepted principles for protecting the privacy and security of personal information.[34] One FIP states that the collection of personal information (such as location data) should only occur with the knowledge or consent of the individual. One privacy rights organization we spoke with told us that FIPs should be a framework used by any company designing a smartphone app. In 2010, CTIA—the Wireless Association published industry *Best Practices and Guidelines for Location Based Services*. These guidelines again rely on the fundamental principles of user notice and consent. [35] Some industry stakeholders suggested that the industry can self-regulate by complying with these types of best practices and that no further government action is needed. However, other stakeholders, while agreeing with the intent and substance of the industry guidelines, pointed out that such guidelines are neither mandated nor binding and involve no penalties for noncompliance.

In line with industry guidelines, some app developers that we spoke with described specific methods that they were employing to alert smartphone users that they were being tracked. For example, several app developers that we spoke with or websites that we reviewed have tracking apps that require initial notification and consent by the person being tracked to install the app on the phone and then include periodic reminders that one's location data were being accessed. Some apps also displayed an icon as a reminder of the presence of the app on the phone.

Ten stakeholders, including three from industry, stated that there was never a reason for a tracking app to be surreptitious. NNEDV, the Stalking Resource Center, and two academics stated that persons engaged in legitimate monitoring—such as a parent worried about a child's location or an employer concerned about an employee's misuse of a company phone—need not use an app that disguises its presence, so there is no reason why an app would need to operate in stealth mode. On the other hand, three industry stakeholders told us that technology itself is

[34]The Organisation for Economic Co-operation and Development, an international organization, developed a revised version of the FIPs that has been widely adopted. Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980).

[35]Other industry codes of conduct, such as the Mobile Location Analytics Code of Conduct (Future of Privacy Forum) and the Short Form Notice Code of Conduct to Promote Transparency in Mobile Application Practices (NTIA), also cite notice and consent as fundamental principles of privacy protection.

neutral, so no specific technology should be banned, including surreptitious tracking technologies. They argued that it is the nefarious intent and use by individuals abusing those technologies that should be prevented and criminalized. In addition, four industry stakeholders told us that they had concerns that any legislative attempts to prohibit surreptitious tracking apps might be worded too broadly and could unintentionally cover too many technologies, harming legitimate uses of tracking apps. Two industry stakeholders told us that they believe that federal and state stalking laws are already sufficient to address most stalking occurrences involving tracking apps, although other stakeholders told us federal and state stalking laws are often not used due to both the high burden in the statutory language and the limited resources at both the federal and state level. Additionally, stalking laws would apply to the individuals committing stalking activities through the use of a surreptitious tracking app rather than to the manufacturer of the app and would apply after the harm has already occurred.

Education Initiatives

The federal government has undertaken educational initiatives to help protect individuals from unwanted tracking. DOJ's Office on Violence against Women (OVW) implements the provisions of the Violence against Women Act (VAWA) in part by funding a number of educational initiatives. In 2015, OVW awarded 686 grants totaling $399 million to states, tribes, units of local government, victim service providers, and other entities to fund initiatives aimed at combating violence against women.[36] A small portion of this funding goes to programs focused on the problem of stalking using technology. For example, since 2000, OVW has funded the Stalking Resource Center, a program of the National Center for Victims of Crime, to provide training and technical assistance to law enforcement, victim service professionals, policymakers, and researchers on developing effective responses to the crime of stalking.[37] DOJ testified in June 2014 that since 2000, the Stalking Resource Center has trained and provided technical assistance to over 100,000 multi-disciplinary professionals nationwide, with an emphasis on the use of technology to stalk. Among other projects, the Stalking Resource Center has co-hosted 11 national conferences that specifically focused on the use of technology in intimate partner stalking cases. In addition, with funding from DOJ's Office for Victims of Crime,

[36]Office on Violence Against Women, Department of Justice, "Grant Programs," (Jan. 11, 2016).

[37]In 2014, the National Center for Victims of Crime received roughly $622,000 from DOJ.

the Stalking Resource Center developed two training tools focused specifically on the use of technology to stalk. The first is a 15-minute training DVD and discussion guide designed to help law enforcement officers, victim advocates, and allied professionals understand the most common forms of technology used by stalkers. The second is a self-paced, interactive online-training course that explores many of the technologies used by stalkers and discusses how to document and obtain evidence related to these technologies as well as considerations for victims' safety.

Another effort funded by OVW is NNEDV's Safety Net Project. Since 2004, this project has provided technical assistance and training to a wide range of grantees to address how technology issues affect the safety, privacy, and rights of victims of domestic violence, dating violence, sexual assault, and stalking. In FY 2013, NNEDV received a 3-year award in the amount of $945,000 to fund the Safety Net Project. NNEDV educates victim advocates and the general public on ways to use technology strategically to increase and maintain safety and privacy. NNEDV also trains law enforcement and justice system personnel, social service workers, and coordinated community response teams on tactics to detect and combat technology misuse and how the law applies. For example, law enforcement personnel are educated on how to detect if tracking apps have been installed on a person's phone, something that would otherwise require a computer forensics expert. In 2014, NNEDV testified that it has trained over 65,000 police, prosecutors, victim advocates, and other professionals since 2002 on the safe use and the potential misuse of technology. To serve survivors of violence and abuse, NNEDV and OVW partnered to develop the Technology and Confidentiality Online Toolkit, a website that provides updated information and resources for agencies and collocated partnerships (serving victims of domestic violence and sexual assault).

FTC has also taken action to help educate and protect individuals from unwanted tracking. FTC testified that it continually assesses new developments and emerging trends and threats in the privacy area. In 2014, the FTC hosted a "Spring Privacy Series" to examine the privacy implications of a number of new technologies in the marketplace. The first seminar included a panel of industry, technical experts, and privacy advocates and examined the privacy and security implications of mobile device tracking. Among other things, the seminar examined how mobile device tracking technologies work and how they are used. FTC has also worked to educate consumers about location tracking technologies specifically. In February 2015, FTC staff published an article on

technology tips for domestic violence and stalking victims.[38] Tips included using a safer computer (or mobile device)—one that the abuser does not have access to—and changing the passwords to that computer so potential abusers would have difficulty accessing them.

Data Collection Efforts

Data concerning the scope of stalking via tracking apps and devices are important to understanding the extent of the problem and helping inform federal decision-making on prevention and enforcement efforts and the allocation of federal resources. On behalf of DOJ, the U.S. Census Bureau annually conducts the National Crime Victimization Survey (NCVS), which collects information on nonfatal personal crimes (rape or sexual assault, robbery, aggravated and simple assault, and personal larceny) and household property crimes (burglary and motor-vehicle and other theft), both reported and not reported to police.[39] The Supplemental Victimization Survey, which collects stalking data and has been part of the NCVS, was last administered in 2006. The Supplemental Victimization Survey identified seven types of harassing or unwanted behaviors consistent with a course of conduct experienced by stalking victims. Based on the findings of that survey, DOJ's Bureau of Justice Statistics reported in 2012 that an estimated 3.3 million persons age 18 or older were victims of stalking during a 12-month period in 2006. Stakeholders, such as domestic violence prevention groups, have told us, and DOJ has acknowledged, that data from 2006 do not reflect current conditions given the pace of developments in technology and that the data need to be updated. DOJ officials told us that they plan for an updated survey, which they expect to publish in the summer of 2017, to include questions that focus on the use of technology to facilitate stalking. For example, according to DOJ, the survey will include questions on unwanted contact or behavior using technology and whether an individual has been stalked by a person using location tracking technology. DOJ is collaborating with

[38]See "Technology Tips for Domestic Violence and Stalking Victims," FTC Consumer Article (Feb. 2015), accessed November 2015, http://www consumer.ftc.gov/blog/technology-tips-domestic-violence-and-stalking-victims.

[39]According to DOJ, NCVS is the nation's primary source of information on criminal victimization. The survey provides a detailed picture of crime incidents, victims, and trends. The NCVS collects detailed information on the frequency and nature of the crimes of rape and other sexual assault, robbery, aggravated and simple assault, personal larceny, household burglary, motor vehicle theft, and other theft. The survey produces national estimates of criminal victimization, as well as information on the characteristics of crimes and victims, and the consequences of victimization.

a number of stakeholders in developing the most recent version of the Supplemental Victimization Survey, including obtaining input from CDC, the Census Bureau, the Stalking Resource Center, NNEDV, and academic researchers from the University of Kentucky and the University of Cincinnati.

Like DOJ, CDC also obtains data on stalking through a survey. CDC's National Intimate Partner and Sexual Violence Survey (NISVS) has provided annual data that are used to understand the national and state-level prevalence of intimate partner violence, sexual violence, and stalking; the subgroups most likely to experience these forms of violence; and the health conditions associated with victimization.[40] CDC's NISVS *Summary Report of 2011* reported that roughly 7.5 million people were stalked in the 12 months preceding the survey and that 15 percent of women and almost 6 percent of men were stalked at some point in their lifetime. CDC's survey includes a section on "Stalking Tactics" that asks respondents questions about whether they have experienced a number of different stalking behaviors, including whether someone has "watched or followed you from a distance, or spied on you with a listening device, camera, or GPS [global positioning system]?" CDC has recently updated and revised its stalking questions and plans to include additional questions on the use of technology in stalking, which CDC staff said was a growing concern. According to CDC staff, the latest version of the survey instrument has completed testing, and the agency expects to administer the updated survey instrument in 2016.[41] The efforts of both DOJ and CDC to update their survey instruments with regard to the use of smartphone tracking apps and other forms of technology that can facilitate stalking should help provide valuable and timely information for understanding the scope of the problem and how to best prioritize federal resources to combat it.

[40]While DOJ's NCVS has a criminal justice focus and seeks to determine if a crime has occurred, the CDC's NISVS has a public health focus and seeks to determine who in the population has had unwanted or unhealthy sexual experiences. CDC's NISVS will be moving toward a biennial survey going forward that collects 12 months of data every other year and doubles the current sample size. CDC had conducted its NISVS survey annually (except 2014) but does not report out on a regular schedule.

[41]We are currently conducting a review comparing the similarities and differences across federal efforts to collect data on rape and sexual assault, as well as examining how the differences affect people's understanding of the extent to which these crimes are occurring. We expect to issue our report in summer 2016.

Agency Comments

We provided a draft of this report to FCC, FTC, and the Departments of Commerce, Health & Human Services, and Justice for their review and comment. FTC, HHS, and DOJ provided technical comments and clarifications that we incorporated as appropriate. FCC and the Department of Commerce did not have any comments on the report.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 17 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees; the Secretary of Health & Human Services and the Director of the CDC; the Attorney General; the Chairwoman of the FTC; the Chairman of the FCC; and the Secretary of Commerce and the Administrator of the NTIA. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or members of your staff have questions about this report, please contact me at (202) 512-2834 or goldsteinm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Mark L. Goldstein
Director, Physical Infrastructure

Appendix I: Objectives, Scope, and Methodology

For this report, we addressed the following questions: (1) How are companies marketing their tracking apps on their websites? (2) What concerns do selected stakeholders have about the use of tracking apps to facilitate stalking? (3) What actions has the federal government taken to protect individuals from the use of surreptitious tracking apps, and what do the selected stakeholders believe are possible further actions that could be taken? We focused our examination on tracking apps that are installed on smartphones; however, we included within our general scope the consideration of "freestanding" or "slap-on" tracking devices.

For all of our objectives, we conducted a literature search to identify relevant articles and other information concerning tracking apps. The literature search was performed using keyword and controlled vocabulary searches in commercial databases (LexisNexis and ProQuest) that index recent and historical content relevant to mobile phone app development and trends. The terms used for the search strategies were developed and chosen based on internal GAO discussions and sample searches in relevant databases. The terms included, but were not limited to, keywords such as "application" or "app" or "phone" combined with "geo" or "location" or "geography" often within proximity to truncated variations on "track" or "stalk" or "monitor," as well as the phrase "domestic violence." We also conducted an Internet search to identify background material using the search terms "smartphone tracking apps," "stalking," "location data," and "GPS."

To determine how companies are marketing their tracking apps, we examined the results of our literature search along with the results of our own Internet searches for names of tracking app companies. We identified 40 companies that were marketing smartphone tracking apps as of July 2015. These 40 companies may not represent the universe of tracking app companies as there may be some companies that did not arise through our literature search or Internet searches. We reviewed the websites of these 40 companies. We accessed the webpages on the websites that were relevant to the companies' tracking app products. We took screen captures of all these webpages on July 22-23, 2015, so that analyses of website content would be as comparable as possible. Using the screen captures, two GAO analysts independently conducted a content analysis of the marketing language used on the websites, looking for specific information such as to whom the product was marketed (e.g., parents, employers, intimate partners or spouses, etc.) and whether the product was explicitly marketed as surreptitious (e.g., using language such as "hidden," "stealth mode," "spy," etc.). The analysts then

compared their analyses; all discrepancies were discussed, and the analysts reached consensus on all decisions.

To identify the stakeholders' concerns about the use of tracking apps to facilitate stalking, we interviewed staff from government agencies; representatives of associations that advocate for victims of domestic violence, consumers, privacy, civil liberties, and the technology and mobile app industry; academics in the field of privacy law; and representatives of mobile phone carriers, mobile phone operating system companies, and companies producing smartphone tracking apps. We selected associations, non-profits, and academics to interview through our literature search, including those testifying at recent privacy hearings before the Subcommittee on Privacy, Technology and the Law of the Senate Judiciary Committee, and from recommendations made by stakeholders during interviews about groups or individuals most involved in the subject of tracking apps and their possible use to facilitate stalking. We selected mobile app developers to interview by first dividing them into four groups; one group consisted of mobile carriers, and three groups were app companies that we categorized based on the degree to which they marketed their app as surreptitious. The first group of app companies developed apps that tracked location only and were not surreptitious; the second group of app developers marketed capabilities beyond location tracking, such as e-mail and text interception, but explicitly said consent should be obtained before using these apps; the third group also marketed features beyond location tracking, such as e-mail and text interception, but marketed the apps' ability to spy, be surreptitious, undetectable, or completely hidden. We randomly selected specific carriers and app developers to interview within each category. Our goal was to obtain two interviews with companies in each group. We continued making contacts down the randomly selected list within each category until we had spoken to two companies in each category. However, none of the companies marketing surreptitious apps that intercept e-mail, texts, and phone conversations were willing to speak with us, so we were unable to interview any companies in this category. We also contacted two operating system developers—Google and Apple, which account for 95 percent of the market share—to obtain their perspectives. Only Google responded and was interviewed. To identify "key" concerns, we conducted a content analysis of the concerns raised by stakeholders. The three concerns most frequently identified by stakeholders are referred to as "key." Throughout our report, we refer collectively to the individuals and organizations we interviewed as "stakeholders." A complete list of the government agencies, organizations, and individuals we interviewed is provided in table 2.

Table 3: List of Government Agencies and Stakeholder Organizations and Individuals Interviewed by GAO

Government agencies	California Department of Justice
	Centers for Disease Control and Prevention
	Federal Communications Commission
	Federal Trade Commission
	National Telecommunications and Information Administration
	United States Department of Justice
Civil liberties groups	American Civil Liberties Union
	Electronic Frontier Foundation
Privacy	Future of Privacy Forum
Associations and non-profits	Application Developers Alliance
	Center for Democracy and Technology
	Consumer Technology Association
	National Association of Attorneys Generals
	National Center for Victims of Crime, Stalking Resource Center
	National Consumers League
	National Network to End Domestic Violence
Tracking app developers	Family Tracker
	Mobile Spy
	TiSpy
	Where's My Droid?
Mobile carriers	AT&T (offers the tracking app FamilyMap)
	Sprint (offers the tracking app Family Locator)
Operating system company	Google
Academics	Alvaro Bedoya (Georgetown Law)
	Danielle Citron (University of Maryland Francis King Carey School of Law)
	Jonathan Mayer (Stanford University)

Source: GAO. | GAO-16-317.

To identify actions that the federal government has taken, or might take, to protect individuals from surreptitious tracking apps, we reviewed relevant federal laws, court decisions, federal enforcement actions, congressional testimony, and law review articles. We discussed the issue with all of the government agencies and stakeholders to obtain their views about past and current actions, and ideas about possible future actions.

We conducted this performance audit from April 2015 to April 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Mark L. Goldstein, (202) 512-2834 or goldsteinm@gao.gov

Staff Acknowledgments

In addition to the contact named above, Faye Morrison (Assistant Director), Joanna Berry, Melissa Bodeau, Jason Bromberg, Richard Bulman, Alicia Cackley, Jeremy Conley, Lacey Coppage, John deFerrari, Camilo Flores, Sarah Gilliland, Gretta Goodwin, Andrew Huddleston, Michael Kaeser, Hannah Laufe, Gerald Leverich, Kristy Love, Kieran McCarthy, Joshua Ormond, Jose Pena, Michael Silver, and Maria Stattel made key contributions to this report.

Appendix III: Accessible Data

Data Tables

Accessible Text for Figure 1: Example of How a GPS-Based Smartphone Location Tracking App Operates

1. John downloads and installs a tracking app onto Amy's smartphone
2. Amy carries her smartphone as she conducts daily activities at various locations
3. Via his own smartphone, John can access and track the location of Amy's smartphone

Data Table for Figure 2: Marketing Strategies of 40 Identified Smartphone Tracking App Websites, as of July 2015

Marketing strategy	Surreptitious	Non-Surreptitious
Marketed to Parents	14	17
Marketed to Employers	12	7
Marketed to Catch a Cheating Partner	9	1
Marketed to track a person who is elderly or has Alzheimer's	0	2

Data Table for Figure 3: Number of 40 Identified Smartphone Tracking App Websites That Marketed Additional Surreptitious and Non-surreptitious Monitoring Capabilities, as of July 2015

	Surreptitious Capabilities	Non-surreptitious Capabilities
Text Messages	14	7
Call History	14	7
Access to web browsing history	12	5
View Pictures	12	4
Access to social media posts	9	6
E-mail	11	2
Geo-fencing	3	9
Listen to Phones Calls	8	0
Access to Phone's Speaker	6	0