Stalking Concerns Raised by Bluetooth Tracking Technologies: In Brief

February 15, 2022

Congressional Research Service
https://crsreports.congress.gov
R47035

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47035

February 15, 2022

Emily J. Hanson
Analyst in Social Policy

Kristin Finklea
Specialist in Domestic Security

Stalking Concerns Raised by Bluetooth Tracking Technologies: In Brief

Recent media reports have raised concerns about the use of Bluetooth tracking technologies (e.g., Apple AirTags, Tile trackers; hereinafter, *e-trackers*) to facilitate crimes such as motor vehicle theft and gender-based violence, including stalking. E-trackers are small, wireless devices intended for tracking the location of belongings such as wallets or keys. However, they can also be attached to a person's car or belongings to surveil their movements and reveal their real-time location.

A Bureau of Justice Statistics (BJS) report summarizing data collected from the Supplemental Victimization Survey to the National Crime Victimization Survey estimates that among the estimated 3.4 million U.S. persons ages 16 and older who reported experiencing stalking in 2019, 80% indicated that the use of technology was involved. Among this group, 14% reported they had their whereabouts tracked with an electronic device. There is a well-established connection between stalking and domestic violence, and some abusers use technology to track their victims. Studies have found high rates of tracking by abusers, and victims frequently seek assistance in preventing technologies, like their cell phones, from being used for location tracking.

Some technology companies have made efforts to develop features to address stalking via e-trackers (e.g., audible alerts, cell phone notifications). While some companies have developed and deployed certain protections to help mitigate nefarious use of e-trackers, these protections are only available to a subset of potential victims (e.g., individuals who download a certain app or possess a smartphone) and their use also places the onus largely on individuals to prevent their own victimization by ensuring they have the full scope of apps to prevent unwanted surveillance. Concerns about the availability and use of e-trackers for stalking are also related to the ongoing debate about whether the speed of technology change outpaces law enforcement's investigative capabilities.

Generally, stalking offenses are the purview of state and local criminal justice systems. However, federal law prohibits use of "the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce" with the intent to "kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person," and in a way that causes a person to have reasonable fear of death or serious bodily injury to themselves, a family member, a spouse/intimate partner, or a pet.

Several bills before Congress include provisions that may pertain to stalking facilitated with e-trackers. For instance, H.R. 1620, a Violence Against Women Act (VAWA) reauthorization bill that passed the House in March 2021, and S. 3623, a VAWA reauthorization bill introduced in the Senate in February 2022, would both authorize a new grant for a National Resource Center on Cybercrimes Against Individuals and define technological abuse for the purpose of VAWA grants that address domestic and dating violence, sexual assault, and stalking.

To learn more about the relationship between e-tracker technologies and crimes such as stalking and motor vehicle theft, Congress may consider holding hearings with law enforcement and technology companies to discuss means to protect privacy, prevent victimization, and enhance investigations of criminal acts. Policymakers may also consider funding research to learn more about criminal victimizations with e-trackers. To help target offenders who abuse such technologies and to assist potential victims, Congress may also consider creating or enhancing penalties for certain stalking offenses or amending VAWA or the Family Violence and Prevention Services Act to add a new grant program or purpose area addressing the use of e-trackers in domestic violence and related crimes such as stalking.

Contents

Contacts

Recent media reports have raised concerns about the use of Bluetooth tracking technologies (e.g., Apple AirTags, Tile trackers; hereinafter, *e-trackers*) to facilitate crimes such as stalking and motor vehicle theft.[1] E-trackers are small, wireless devices intended for tracking the location of belongings such as wallets or keys. However, they can also be attached to a person's car or belongings to surveil their movements and reveal their real-time location. Although e-trackers have existed for some time, advances in their precision (e.g., AirTag's ability to locate a tag down to the centimeter and floor level),[2] their widespread marketing, and accounts of e-trackers being found secreted into purses or attached to vehicles have heightened concerns about implications for gender-based violence, and stalking in particular.[3]

This report provides an overview of the most recent statistics on technology used to facilitate stalking, features that some technology companies have implemented to prevent their e-trackers from being used to enable stalking, barriers to investigating these offenses, and selected policy options under consideration.

Statistics on Technology and Stalking

The Bureau of Justice Statistics (BJS) estimates that 3.4 million U.S. persons ages 16 and older experienced stalking in 2019.[4] Of those who reported experiencing stalking, 80% indicated that technology was involved. Among this group, 14% reported they had their whereabouts tracked with an electronic device. While there was an 11% decrease in the overall number of individuals reporting technology involvement in their stalking victimization from 2016 to 2019, there was a 39% increase in reports of location tracking with electronics over the same time.[5] Of note, these findings are based on data collected in the 2019 National Crime Victimization Survey (NCVS).[6] While this survey was administered after the 2014 release of Tile trackers, it predates the 2021 release of AirTags. As such, BJS findings may not reflect current trends in the involvement of e-trackers in stalking incidents.

There is a well-established connection between stalking and domestic violence, and some abusers have been found to have used technology to track their victims.[7] Studies have found high rates of tracking by abusers, and victims frequently seek assistance in preventing technologies, like their cell phones, from being used for location tracking.[8] However, there are no comprehensive data on

[1] See, for example, Dalvin Brown, "New Apple Update Targets AirTag Tracking Concerns," *Wall Street Journal*, February 10, 2022; and David Ingram, "A Tracking Device Made by Apple is Showing Up in Suspected Crimes," *NBC News*, February 10, 2022. For more information on AirTags, see https://www.apple.com/airtag/. For more information on Tile trackers, see https://www.thetileapp.com/en-us/.

[2] Shelby Brown, "What's an AirTag? Apple's New Trackers, Explained," *CNET*, May 6, 2021.

[3] Megan Hickey, "Another Chicagoan Comes Forward, Says Apple AirTag Was Used to Track and Stalk Her," *CBS Chicago*, January 20, 2022.

[4] Rachel E. Morgan and Jennifer L. Truman, *Stalking Victimization, 2019*, Bureau of Justice Statistics (BJS), NCJ 301735, February 2022. BJS findings are based on the 2019 Supplemental Victimization Survey to the National Crime Victimization Survey. For more information on BJS's role in criminal justice data collection and analysis, see CRS In Focus IF11857, *Bureau of Justice Statistics (BJS) Role in Criminal Justice Data Collection and Dissemination*, by Emily J. Hanson and Kristin Finklea.

[5] Ibid. See also, Jennifer L. Truman and Rachel E. Morgan, *Stalking Victimization, 2016*, Bureau of Justice Statistics, NCJ 253526, April 2021.

[6] For more information on the National Crime Victimization Survey and the Supplemental Victimization Survey, see https://bjs.ojp.gov/data-collection/supplemental-victimization-survey-svs.

[7] Heather C. Melton, "Stalking: A Review of the Literature and Direction for the Future," *Criminal Justice Review*, vol. 25, no. 2 (Autumn 2000), pp. 246-262.

[8] Brenda Baddam, "Technology and Its Danger to Domestic Violence Victims: How Did He Find Me?", *Albany Law*

the use of e-trackers in the commission of crimes such as stalking. For instance, while the NCVS polls a sample of individuals about their victimization—including the involvement of location-tracking technology in stalking victimization—these survey data are not necessarily nuanced to understand the true scope of the use of e-trackers in stalking or other crimes. However, like criminal use of technologies such as the internet, social media, and smartphones,[9] it may be that as e-trackers improve and proliferate, their use in crime may become more common. This has similarly been suggested by the increase in *stalkerware* apps.[10]

Preventing E-tracking Enabled Stalking

Technology companies have made efforts to develop features to prevent stalking via e-trackers. For instance, when AirTags were released in April 2021, they included a feature to alert iPhone users (who had the Find My feature enabled) if an AirTag (that was away from the owner who registered it) was moving with them.[11] The alert also provides instructions on how to disconnect or disable the AirTag. In December 2021, Apple released an app called Tracker Detect to alert Android users in a similar fashion.[12] Similarly, Tile is developing a Scan and Secure feature that will allow anyone with a Tile app to scan and see if an unknown Tile device is near them.[13]

An AirTag that has been separated from its registered device for a period of time—the duration of which has decreased with subsequent security updates[14]—will make a sound to alert those nearby to its presence. However, there have been anecdotal reports of aftermarket AirTags with physically disabled speakers being sold online.[15] Tile trackers do not have this audible alert feature.

Barriers to Addressing Criminal Use of AirTags

While some companies have developed certain protections to help mitigate nefarious use of e-trackers, these protections are only available to a subset of potential victims. For Tile, some protections may be available to those individuals who download the forthcoming Scan and Secure app. For Apple, some protections may be available to individuals with an iPhone enabling Find My notifications and Android users who have downloaded an app with tracker alerts. Android users not using an app such as Tracker Detect and individuals without smartphones are among those who may not have these protections available to them. Further, it appears that the onus may be largely on individuals to prevent their own victimization by ensuring they have the full scope of apps and proper settings to scan and prevent unwanted surveillance by an e-tracker. In addition to the potential gaps in individuals using available apps to detect unwanted tracking, aftermarket manipulation of tracking devices may prevent them from alerting potential victims.

Journal of Science and Technology, vol. 28, no. 1 (2017), pp. 73-93.

[9] See, for example, Jack Karsten, *As Criminals Adapt to New Technology, So Must International Law*, Brookings Institute, April 21, 2017.

[10] Brian X. Chen, "'Stalkerware' Apps Are Proliferating. Protect Yourself," *New York Times*, September 30, 2021.

[11] Apple Support, https://support.apple.com/en-us/HT212227.

[12] Ian Sherr, "Apple Launches AirTags and Find My Detector App for Android, in Effort to Boost Privacy," *CNET*, December 13, 2021.

[13] Tile, "Introducing Our Newest Bluetooth Tile Trackers," October 11, 2021.

[14] Caitlin McGarry, "Apple Says It Will Make AirTags a Little Less Scary," *Gizmodo*, June 3, 2021.

[15] Andrew Liszewski, "Silenced AirTags With Disabled Speakers Are Popping Up for Sale Online," *Gizmodo*, February 3, 2022.

In addition, there has been an ongoing debate about whether the speed of technology change outpaces law enforcement's investigative capabilities.[16] The proliferation of e-trackers may be one example.[17] For instance, while each AirTag registered has a serial number that may assist law enforcement in identifying the owner, AirTags are protected by end-to-end encryption such that even Apple does not know the location of an AirTag nor the identity of the device that is linked to the AirTag to help find it.[18] Law enforcement has argued that end-to-end encryption can stymie investigations, as it may not have the capabilities to bypass the encryption to access information, even in instances where access is lawfully authorized.[19]

Current Federal Law on Stalking

In many cases, stalking offenses are the purview of state and local criminal justice systems. However, stalking cases occurring in locations under federal authority, those involving interstate travel, and those facilitated by the mail or computer or electronic communication services do fall under federal jurisdiction.[20] Specifically, federal law prohibits use of "the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce" with the intent to "kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person," and in a way that causes a person to have reasonable fear of death or serious bodily injury to themselves, a family member, a spouse/intimate partner, or a pet.[21] Although the federal stalking law does not specifically call out the use of e-trackers, their use to facilitate stalking appears to be covered under existing law.

Although federal law does not speak specifically to location tracking, several states have taken action in this realm. Some states have passed laws directly addressing the use of electronic devices by individuals to track others without consent. For instance, some state legislatures have banned the use of e-trackers to follow another's location without their consent.[22] Some have more specifically barred placing e-trackers on motor vehicles without the owner's consent.[23] Other states have expanded their stalking statutes to prohibit the use of GPS and e-trackers in the commission of a stalking offense.[24]

[16] For more information on this debate, see CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, by Kristin Finklea.

[17] See, for example, Courtney Robinson, "Tampa Bay Law Enforcement Agencies Report Apple's AirTags Being Used to Track People," *Tampa Bay 10 News*, December 30, 2021.

[18] Apple, "AirTag," https://www.apple.com/airtag/.

[19] For more information, see CRS In Focus IF11769, *Law Enforcement and Technology: the "Lawful Access" Debate*, by Kristin Finklea.

[20] Department of Justice, U.S. Attorney's Office, Northern District of Georgia, *Interstate Stalking*, December 23, 2021.

[21] 18 U.S.C. §2261A.

[22] Pam Greenberg, "Private Use of Mobile Tracking Devices," *National Conference of State Legislatures*, vol. 24. no. 43 (November 2016), https://www.ncsl.org/research/telecommunications-and-information-technology/private-use-of-mobile-tracking-devices.aspx (hereinafter, "NCSL Private Use of Mobile Tracking Devices"). These states include California, Hawaii, Louisiana, Minnesota, New Hampshire, North Carolina, and Virginia.

[23] NCSL Private Use of Mobile Tracking Devices. These states include Delaware, Illinois, Michigan, Rhode Island, Tennessee, Texas, and Wisconsin.

[24] NCSL Private Use of Mobile Tracking Devices. These states include Arizona, Connecticut, Illinois, New York, and North Dakota.

The Violence Against Women Act and Stalking

The Violence Against Women Act (VAWA; Title IV of P.L. 103-322), originally enacted in 1994, is a primary legislative package governing federal efforts to address violence against women, including domestic violence, dating violence, sexual assault, and stalking.[25] Among other things, VAWA authorizes grants to state, local, and tribal law enforcement entities to investigate and prosecute violent crimes against women, and several of these grant programs directly address stalking.

The authorization of appropriations for VAWA grants expired in FY2018, and currently there are congressional efforts to amend VAWA and reauthorize its grant programs.[26] Some of these efforts directly address stalking and the use of technology to facilitate it and other crimes covered by VAWA. For instance, H.R. 1620, a VAWA reauthorization bill that passed the House in March 2021, and S. 3623, a VAWA reauthorization bill introduced in the Senate in February 2022, would both authorize a new grant for a National Resource Center on Cybercrimes Against Individuals to aid state and local criminal justice systems in identifying, prosecuting, and protecting individuals from certain forms of cybercrime, including stalking.[27] Both bills would also define *technological abuse* as

> an act or pattern of behavior that occurs within domestic violence, sexual assault, dating violence or stalking and is intended to harm, threaten, intimidate, control, stalk, harass, impersonate, exploit, extort, or monitor, except as otherwise permitted by law, another person, that occurs using any form of information technology, including: internet enabled devices, online spaces and platforms, computers, mobile devices, cameras and imaging platforms, apps, location tracking devices, communication technologies, or any other emerging technologies.[28]

This definition would apply to VAWA grants, thus expanding access to VAWA resources, but would not amend federal criminal law provisions.[29] The cybercrimes provisions included in S. 3623 would also require the Federal Bureau of Investigation (FBI) to collect and publish data on cybercrimes against individuals as part of their National Incident-Based Reporting System (NIBRS) and Uniform Crime Reporting (UCR) programs.[30]

Policy Considerations

To learn more about the relationship between e-tracker technologies and crimes such as stalking and motor vehicle theft, Congress could consider a number of options, including holding hearings with law enforcement and technology companies to discuss means to protect privacy, prevent victimization, and enhance investigations of criminal acts. Policymakers may also consider funding research to learn more about criminal victimizations with e-trackers. Although some

[25] For more information on VAWA, see CRS Report R45410, *The Violence Against Women Act (VAWA): Historical Overview, Funding, and Reauthorization*, by Lisa N. Sacco and Emily J. Hanson.

[26] For more information on selected VAWA reauthorization issues before Congress, see CRS Report R46742, *The Violence Against Women Act (VAWA) Reauthorization: Issues for Congress*, by Emily J. Hanson and Lisa N. Sacco.

[27] For more information, see CRS Report R46742, *The Violence Against Women Act (VAWA) Reauthorization: Issues for Congress*, by Emily J. Hanson and Lisa N. Sacco.

[28] See S. 3623.

[29] For more information, see CRS Report R46742, *The Violence Against Women Act (VAWA) Reauthorization: Issues for Congress*, by Emily J. Hanson and Lisa N. Sacco.

[30] For more information on UCR see CRS Report R46668, *The National Incident-Based Reporting System (NIBRS): Benefits and Issues*, by Emily J. Hanson.

information about the use of technology for stalking is captured in the NCVS and included in periodic reports on stalking published by BJS, Congress may consider a study specifically focused on the use of e-trackers in crimes such as stalking, domestic and dating violence, motor vehicle theft, and others. Congress may also consider authorizing funding for further data collection by the National Intimate Partner and Sexual Violence Survey (NISVS). The NISVS was conducted annually by the Center for Disease Control (CDC) from 2010 to 2012 and again in 2015.[31] This survey captured data on participant experiences of domestic violence both over their lifespan and in the last 12 months. A future iteration of the NISVS could include questions about the involvement of e-trackers in victimization.

To help target offenders who abuse such technologies and to assist potential victims, Congress may also consider creating or enhancing penalties for federal stalking and related offenses or amending VAWA to add a new grant program or purpose area targeting the use of e-trackers in violence against women. Congress may also consider amending the purpose areas of VAWA or Family Violence Prevention and Services Act (FVPSA)[32] grants to provide training and technical assistance to victims and victim service providers on understanding, preventing, and addressing e-tracker-facilitated abuse.

Author Information

Emily J. Hanson
Analyst in Social Policy

Kristin Finklea
Specialist in Domestic Security

Disclaimer

[31] For more information on the NISVS, see https://www.cdc.gov/violenceprevention/datasources/nisvs/index.html and CRS Report R42838, *Family Violence Prevention and Services Act (FVPSA): Background and Funding*, by Adrienne L. Fernandes-Alcantara and Kara Clifford Billings.

[32] For more information, see CRS In Focus IF11170, *Family Violence Prevention and Services Act (FVPSA)*, by Kara Clifford Billings.