MILSTEIN JACKSON FAIRCHILD & WADE, LLP
Gillian L. Wade, State Bar No. 229124
gwade@mjfwlaw.com
Sara D. Avila, State Bar No. 263213
savila@mjfwlaw.com
Marc A. Castaneda, State Bar No. 299001
mcastaneda@mjfwlaw.com
10990 Wilshire Blvd., 8th Floor
Los Angeles, California 90024
Tel: (310) 396-9600
Fax: (310) 396-9635

LYNCH CARPENTER, LLP
Edwin J. Kilpela, Jr.
Elizabeth Pollock-Avery
Kenneth A. Held
1133 Penn Ave, 5th Floor
Pittsburgh, Pennsylvania 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
ekilpela@lcllp.com
elizabeth@lcllp.com
ken@lcllp.com

wh LAW
David Slade
slade@wh.law
Brandon Haubert
brandon@wh.law
Jessica Hall
jessica@wh.law
1 Riverfront Place, Suite 745
North Little Rock, AR 72114
Telephone: 501.891.6000
Facsimile: 501.222.3027

Attorneys for Plaintiffs individually and on behalf of all others similarly situated

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

LAUREN HUGHES and JANE DOE, *individually and on behalf of all others similarly situated,*

Plaintiffs,

v.

APPLE, INC.

Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1. Negligence
2. Strict Liability- Design Defect (Consumer Expectation Test)
3. Strict Liability-Design Defect (Risk-Benefit Test)
4. Unjust Enrichment
5. Intrusion Upon Seclusion
6. Violations of California's Constitutional Right to Privacy
7. Violations of CIPA, Cal. Pen. C. §§630, *et seq*.
8. Negligence *Per Se*
9. Violations of UCL's Unlawful Prong,

Cal. Bus. & Prof. C. §§17200, *et seq*.
10. Violations of UCL's Unfair Prong, Cal. Bus. & Prof. C. §§17200, *et seq*.
11. Violations of UCL's Fraudulent Prong, Cal. Bus. & Prof. C. §§17200, *et seq*.
12. Violations of N.Y. Bus. Law §349

INTRODUCTION

1. Each year, an estimated 13.5 million people are victims of stalking in the United States, with nearly one in three women and one in six men experiencing stalking at some point in their lifetime.[1]

2. Stalking can manifest in a host of ways, most often through unwanted and repeated behaviors such as phone calls, texts, visits, gifts, internet posts, or any other series of acts that would cause fear in a reasonable person. Regardless of the acts the stalker employs, the common theme of stalking behavior is the fear elicited in the victim.

3. This fear undermines and erodes a victim's autonomy and drastically disrupts their day-to-day life. One in eight employed stalking victims miss time from work because of their victimization and more than half lose more than five days of work.[2] One in seven stalking victims move as a result of their victimization.[3] Unsurprisingly, stalking victims suffer much higher rates of depression, anxiety, insomnia, and social dysfunction than people in the general population.[4]

4. Technology has increased the tools available to a stalker, with burner phones or call blocking software providing anonymity, and free email services and social media platforms providing a limitless vector for harassing electronic messages and posts.

5. One of the most dangerous and frightening technologies employed by stalkers is the use of real-time location information to track victims. These technologies allow stalkers to follow their victims' movements in real time and to undo any attempt on the part of the victim to

---

[1] Stalking Prevention Awareness and Resource Center (SPARC), Stalking Fact Sheet (available at https://www.stalkingawareness.org/wp-content/uploads/2019/01/SPARC_StalkngFactSheet_2018_FINAL.pdf)

[2] Baum, K., Catalano, S., & Rand, M. (2009). Stalking Victimization in the United States. Washington, DC: Bureau of Justice Statistics

[3] *Id*.

[4] Blaauw, E., Arensman, E., Winkel, F.W., Freeve, A., & Sheridan, L. (2002). The Toll of Stalking. Journal of Interpersonal Violence 17(1): 50-63

evade or hide from the stalker. If one's location is constantly being transmitted to an abuser, there is no place to run.

6. One of the products that has revolutionized the scope, breadth, and ease of location-based stalking is the Apple AirTag. Introduced in April 2021, this device is roughly the size of a quarter, and its sole purpose is to transmit its location to its owner.

7. What separates the AirTag from any competitor product is its unparalleled accuracy, ease of use (it fits seamlessly into Apple's existing suite of products), and affordability. With a price point of just $29, it has become the weapon of choice of stalkers and abusers.

8. The AirTag works by emitting signals that are detected by Bluetooth sensors on the hundreds of millions of Apple products across the United States. These sensors comprise Apple's "FindMy" network. When a device on the network detects a signal from the missing device, it reports that missing device's location back to Apple, which in turn reports it to the owner.

9. The ubiquity of Apple products, and their constituency in the FindMy network, means that an AirTag can more reliably transmit location data than any competitor. Indeed, in all metropolitan areas, and even many rural areas, one is never more than 100 yards away from an Apple device. Thus, one is never more than 100 yards away from having location data transmitted back to Apple.

10. None of this came as a surprise to Apple. Prior to and upon the AirTag's release, advocates and technologists urged the company to rethink the product and to consider its inevitable use in stalking. In response, Apple heedlessly forged ahead, dismissing concerns and pointing to mitigation features that it claimed rendered the devices "stalker proof."

11. The concerns were well founded. Immediately after the AirTag's release, and consistently since, reports have proliferated of people finding AirTags placed in their purses, in or on their cars, and even sewn into the lining of their clothes, by stalkers in order to track their whereabouts. The consequences have been as severe as possible: at least two reported murders have occurred in which the murderer used an AirTag to track the victim.

12. Its "stalker proof" protections exposed as totally inadequate, Apple spent the rest of 2021 and 2022 scrambling to address its failures in protecting people from unwanted, dangerous tracking. To date, most if not all, of these failures persist.

13. Plaintiffs, each of whom are victims of stalking through the use of an AirTag, bring this action on behalf of themselves and a class and subclasses of individuals who have been and who are at risk of stalking via this dangerous product.

14. Apple's acts and practices, as detailed further herein, amount to acts of negligence, negligence *per se*, intrusion-upon-seclusion, and product liability, constitute unjust enrichment, and violate California's constitutional right to privacy, California's Invasion of Privacy Act, Cal. Pen. Code § 630, *et seq*. ("CIPA"), California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL"), and New York General Business Law § 349 ("GBL"). Plaintiffs, in a representative capacity, seek statutory damages, actual damages, and punitive damages, as well as injunctive and declaratory relief against Apple, correcting Apple's practice of releasing an unreasonably dangerous product into the stream of commerce, misrepresenting the harms associated therewith, and facilitating the unwanted and unconsented to location tracking of Plaintiffs and Class members.

PARTIES

15. Plaintiff Lauren Hughes is a citizen of Travis County, Texas.

16. Plaintiff Jane Doe is a citizen of Kings County, New York.

17. Defendant Apple, Inc. ("Apple") is an American multinational technology company headquartered in Cupertino, California. Among Apple's flagship items of consumer electronics is the AirTag, and Apple generally oversees all aspects of this device, including but not limited to its design, manufacture, marketing, and technical support and maintenance.

JURISDICTION AND VENUE

18. Pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005 ("CAFA"), this Court has subject matter jurisdiction over this putative nationwide class action because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs,

and is a class action in which some members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A).

19. This Court has personal jurisdiction over Defendant because its worldwide headquarters are in California, and because it conducts in California substantial business from which the claims in this case arise.

INTRADISTRICT ASSIGNMENT

20. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(b)(1) because Apple is headquartered in this district and a substantial part of the events or omissions which give rise to the claims alleged herein occurred in in this district.

FACTUAL ALLEGATIONS

A. Apple AirTags, Generally

21. The AirTag was introduced in April 2021 as a standalone product. Roughly the size of a US quarter, it is a tracking beacon, meant to help consumers locate other objects, such as keys or purses.[5]

Fig. 1

[5] Apple, "*Apple introduces AirTag*" Press Release (Apr. 20, 2021) (available at https://www.apple.com/newsroom/2021/04/apple-introduces-airtag/).

Fig. 2

22. AirTags are not themselves connected to the Internet. Instead, they utilize Bluetooth technology, emitting Bluetooth signals to any Apple device that is nearby. In turn, those Apple devices report where an AirTag has last been seen.[6] Once an AirTag is identified as being near an Apple device or multiple Apple devices, the devices act as crowdsourced beacons, pinging with the AirTag to locate it for the AirTag's owner. The owner sees the AirTag on a map, and as they get closer to the AirTag, the owner switches interfaces and is directed with an arrow, sending them right to the AirTag. *E.g.*

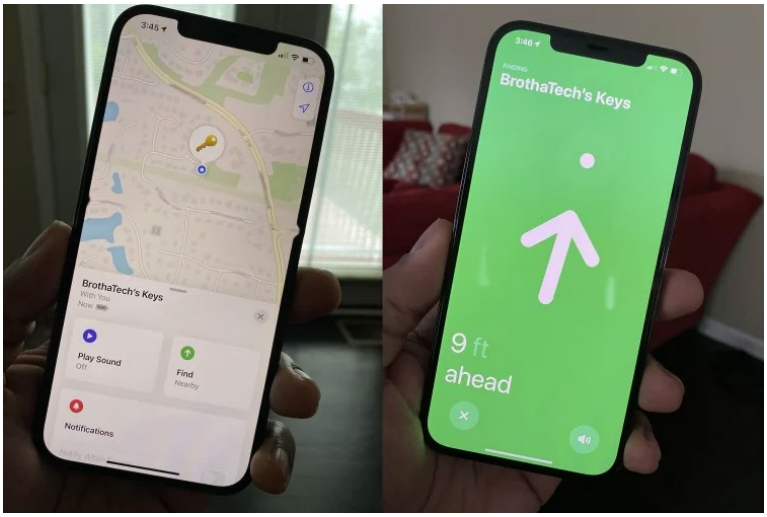


Fig. 3

[6] Ryan Mac and Kashmir Hill, "*Are Apple AirTags Being Used to Track People and Steal Cars?*" New York Times (Dec. 30, 2021) (available at https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html)

23. Bluetooth range is approximately 30 feet. Thus, for an AirTag to be identified by an Apple device, it must come within 30 feet of that device, at which time, the AirTag will have been located on Apple's network of iPhones, iPads, iPods, etc. that are owned and used by consumers in the United States.[7] This network is vast: as of 2017, 64% of Americans owned an Apple product.[8]

24. Because of this technology and because of the ubiquity of Apple products, it is virtually impossible to hide from an AirTag in most, if not all, populated areas. As one commentator challenged his readers: "try getting through the day without coming within 30 feet of an iPhone or iPad."[9]

25. Eva Galperin, the director of cybersecurity at the Electronic Frontier Foundation, points out that this ubiquity of Apple products makes AirTags "uniquely harmful," explaining "Apple automatically turned every iOS device into part of the network that AirTags use to report the location of an AirTag….The network that Apple has access to is larger and more powerful than that used by the other trackers. It's more powerful for tracking and more dangerous for stalking."[10]

B. Within Days of the Release of the AirTag, Technologists and Advocates Urged Apple to Consider the Risk Inherent in the Product

26. Immediately after Apple announced the release of the AirTag, prominent voices in the tech and domestic violence advocacy spaces began warning Apple of the risks inherent in its new product.

---

[7] Albert Fox Cahn, "*Apple's AirTags Are A Gift to Stalkers*," Wired (May 13, 2021) (available at https://www.wired.com/story/opinion-apples-air-tags-are-a-gift-to-stalkers/)

[8] Steve Leisman, "*America loves its Apple. Poll finds that the average household owns more than two Apple products*" CNBC (Oct. 10, 2017) (available at https://www.cnbc.com/2017/10/09/the-average-american-household-owns-more-than-two-apple-products.html)

[9] "*Apple's AirTags Are A Gift to Stalkers*," note 7, *supra.*

[10] "*Are Apple AirTags Being Used to Track People and Steal Cars?*" note 6, *supra*.

27. Within roughly a week of the product's announcement, representatives from the National Network to End Domestic Violence spoke out about the serious harms that AirTags pose. Erica Olsen, the Safety Net Project Director at NNEDV, explained: "When somebody tries to leave an abusive person, or they are planning to leave, that can be one of the most dangerous times that stalking and assault can escalate. So it's extremely important if people are planning to leave an abusive person, they're able to do so without the person tracking them down and finding them. It's definitely a concern that people will be using any type of [tracking] product they can."[11]

28. Corbin Streett, a Technology Safety Specialist at NNEDV, elaborated further that individuals being abused by domestic partners were particularly susceptible to being victimized by AirTags: "[Apple] is thinking about the threat model where it's a stalker who is walking by someone on the street they don't know—that stranger danger model—but what about when it is the person you come home to every day?...[H]ow do you build it in a way that those folks who are in relationships, so that this can't be used against them? I hope Apple keeps their learning hat on and works to figure out that piece of the puzzle."[12]

29. As another example, on May 5, 2021, Geoffrey Fowler, the prominent tech reporter for the Washington Post, published a story titled *Apple's AirTag trackers made it frighteningly easy to 'stalk' me in a test—Apple knows its tiny new lost-item gadgets could empower domestic abuse but doesn't do enough to stop it,*" in which he cautioned:

> Along with helping you find lost items, AirTags are a new means of inexpensive, effective stalking. I know because I tested AirTags by letting a Washington Post colleague pretend to stalk me. And Apple's efforts to stop the misuse of its trackers just aren't sufficient.
>
> …

---

[11] Mark Wilson, "*Apple AirTags could enable domestic abuse in terrifying ways*," Fast Company (Apr. 29, 2021) (available at https://www.fastcompany.com/90630404/apple-airtags-could-enable-domestic-abuse-in-terrifying-ways)

[12] *Id.*

> AirTags show how even Apple, a company known for emphasizing security and privacy, can struggle to understand all the risks involved in creating tech that puts everyday things online.
>
> …
>
> For most people, AirTags will be a useful convenience that offers precise tracking and a replaceable battery. So why focus on these problems? Because personal tech is no longer just about you. My job as a consumer advocate is to consider the people technology helps — and those it hurts…. Digital stalking is remarkably common, experts say, and it's strongly linked to physical abuse, including murder.[13]

30. Eva Galperin, the director of cybersecurity at the Electronic Frontier Foundation, expressed her concerns even before the product's launch last spring: "I was concerned ahead of their release as soon as I figured out how they worked. I was concerned very shortly after they were released when I started seeing reports of stalking and being contacted by people who were being stalked using these devices." While acknowledging that Apple subsequently engaged in mitigation efforts—*see*, Section E, *infra*—Galperin went on to state that "[t]he mitigations that Apple had in place at the time that the AirTag came out were woefully insufficient," and "the fact that they chose to bring the product to market in the state that it was in last year, is shameful."[14]

31. Wired released a story on the issue in a May 13, 2021 titled "Apple's AirTags Are a Gift to Stalkers," in which the author, Albert Fox Cahn, warned:

> Apple needs to take domestic abuse and stalking seriously. More than 10 million Americans have likely faced stalking in their lifetimes, with more than a million facing this threat every year. The rates for intimate partner violence is even starker, with more than a quarter of women and 10 percent of men reporting abuse. These are not outliers, this is an epidemic of

---

[13] Geoffrey Fowler, "*Apple's AirTag trackers made it frighteningly easy to 'stalk' me in a test—Apple knows its tiny new lost-item gadgets could empower domestic abuse but doesn't do enough to stop it*," Washington Post (May 5, 2021) (available at https://www.washingtonpost.com/technology/2021/05/05/apple-airtags-stalking/)

[14] Michael Levitt, "*AirTags are being used to track people and cars. Here's what is being done about it*" NPR (Feb. 18, 2022) (available at https://www.npr.org/2022/02/18/1080944193/apple-airtags-theft-stalking-privacy-tech).

> violence touching nearly every corner of our globe. When Apple fails to protect survivors, the consequences can be fatal. Apple leadership needs to give abuse survivors and experts a central place in its development process, incorporating their feedback from the start. Otherwise, the company will continue to make products that endanger people more than they help.[15]

C. Apple Affirmatively Sought to Dismiss and Minimize Concerns About the Threats Surrounding AirTags, Going So Far As to Call the Product "Stalker-Proof"

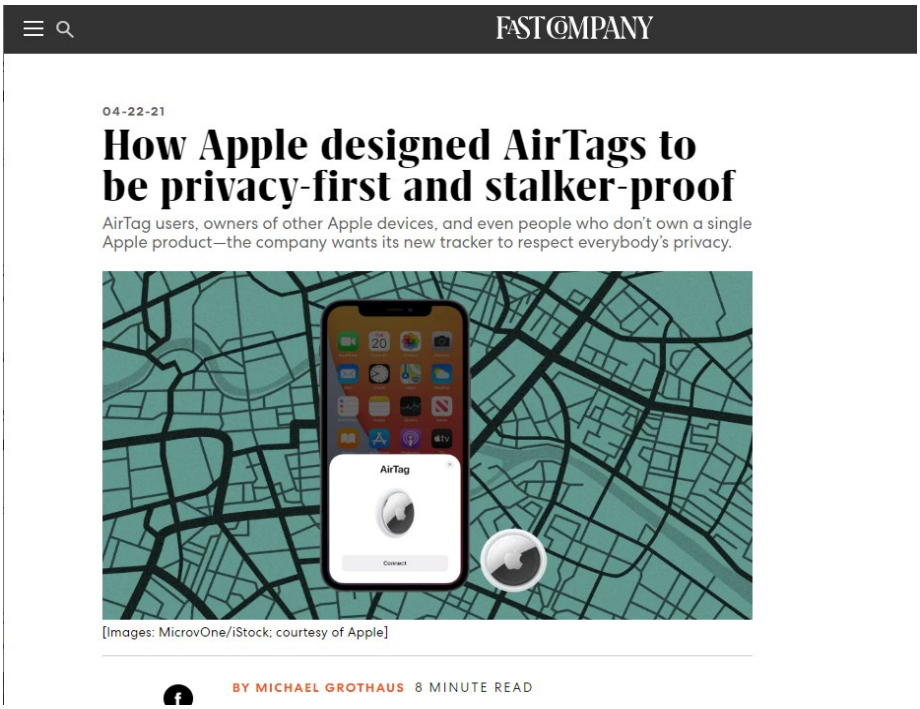
32. Upon the release of AirTags, rather than heed the concerns of outside groups and commentators, Apple proactively sought to minimize and dismiss those concerns, arranging for interviews with high-level executive[16] touting the safety of the product. Apple went so far as to represent, in multiple media outlets, that AirTags are "Stalker-Proof":

Fig. 4[17]

[15] "*Apple's AirTags Are A Gift to Stalkers*," note 7, *supra*.

[16] The principal interviewees appear to be Kaiann Drance, Apple's VP of worldwide iPhone product marketing, and Ron Huang, the Apple's senior director of sensing and connectivity.

[17] José Adorno, "*Apple execs explain how AirTag is 'stalker-proof' and whether you should use it to track pets*," 9to5 Mac (Apr. 22, 2021) (available at https://9to5mac.com/2021/04/22/apple-execs-explain-how-airtag-is-stalker-proof-and-whether-you-should-use-it-to-track-pets/)



FAST COMPANY

04-22-21

How Apple designed AirTags to be privacy-first and stalker-proof

AirTag users, owners of other Apple devices, and even people who don't own a single Apple product—the company wants its new tracker to respect everybody's privacy.

[Images: MicrovOne/iStock; courtesy of Apple]

BY MICHAEL GROTHAUS 8 MINUTE READ

Fig. 5[18]

AirTag is stalker-proof even with Android users

April 22, 2021

Apple unveiled on Tuesday its AirTag smart tracker. Designed to be "privacy-first" and "stalker-proof," two Apple executives shared more info about the AirTag with *Fast Company*.

In the interview, Apple's VP of worldwide iPhone product marketing Kaiann Drance and senior director of sensing and connectivity Ron Huang talked about the smart tracker creation and its benefits.

Fig. 6[19]

[18] Michael Grothaus, "*How Apple designed AirTags to be privacy-first and stalker-proof*," Fast Company (Apr. 22, 2021) (available at https://www.fastcompany.com/90628073/apple-airtag-privacy-security) (interviewing Drance and Huang)

[19] "*AirTag is stalker-proof even with Android users*," Telegraph (Apr. 22, 2021) (available at https://techtelegraph.co.uk/airtag-is-stalker-proof-even-with-android-users/)

Fig. 7[20]

33. These representations, and others, were part of an intentional, coordinated press campaign on the part of Apple, in which its executives and its publicists actively sought to portray the AirTag as a harmless—indeed "stalker-proof"—product. Thus, not only did Apple fail to adequately disclose the risks associated with the AirTag, it affirmatively *misled* the public and the press as to those risks.

D. Following Its Release, Reports Proliferated of People Being Stalked Via AirTags

34. Within months of the release of AirTags, reports began to abound of people being stalked by the product. A recent article in The Verge explained

> There's no question that AirTags can be — and have been — abused. Sports Illustrated model Brooks Nader recently reported finding a stranger's AirTag in her coat. One Connecticut man was arrested for placing an AirTag on his ex-girlfriend's car; a Texas man admitted to doing the same to his estranged wife last month.

[20] Dave LeClair, "*Apple Says AirTags Are Stalker-Proof, Not For Tracking Kids and Pets*," (Apr. 22, 2021) (available at https://www.makeuseof.com/airtags-stalker-proof-not-kids-pets/)

> A *New York Times* reporter successfully used them to track her husband's every move (for a story).[21]

35. A December 2021 New York Times article (different from the one mentioned in The Verge piece above) noted individuals reporting abuse on TikTok, Twitter, and Reddit, stating that "There is growing concern that the devices may be abetting a new form of stalking, which privacy groups predicted could happen when Apple introduced the devices in April."[22]

36. The anecdotal reports are often chilling, as illustrated by one commenter on Reddit who cautioned

> Check EVERYTHING. I have a friend who had this exact problem, traveling alone, AirTag notifications even though she didn't have one. She went to the police and they searched everything and found one hidden with extra sticky tape underneath a flap in her backpack. They told her they've seen these in trafficking circles. They kept the tag to investigate and gave her stuff back and told her to be extra vigilant[.][23]

37. Victims have been stalked across the country, in places like New York,[24] California,[25] Pennsylvania,[26] Mississippi,[27] and even at Disney World,[28] but the abuse is

---

[21] Monica Chin and Victoria Song "*AirTags Are Dangerous — Here's How Apple Could Fix Them*" The Verge (Mar. 1, 2022) (available at https://www.theverge.com/2022/3/1/22947917/airtags-privacy-security-stalking-solutions)

[22] "*Are Apple AirTags Being Used to Track People and Steal Cars?*" note 6, *supra*.

[23] https://www.reddit.com/r/applehelp/comments/rkfxnr/unsettling_notification_re_detected_airtag_cause/

[24] Sara Boboltz "*AirTags Are A Growing Headache For Apple Amid Disturbing Reports Of Tracking*," Huffington Post (Dec. 2, 2022) (available at https://www.huffingtonpost.co.uk/entry/apple-airtags-tracking_n_61f425ade4b067cbfa1cb2b8)

[25] "*Are Apple AirTags Being Used to Track People and Steal Cars?*" note 6, *supra*.

[26] Zahriah Balentine, "*2 women believe Apple Airtag was used to stalk them after leaving Central Pa. restaurant*," Williamsport Sun-Gazette (Jan. 21, 2022) (available at https://www.sungazette.com/news/2022/01/2-women-believe-apple-airtag-was-used-to-stalk-them-after-leaving-central-pa-restaurant/)

[27] Sara Boboltz *AirTags Are A Growing Headache For Apple Amid Disturbing Reports Of Tracking*, Huffington Post (Dec. 2, 2022) (available at https://www.huffingtonpost.co.uk/entry/apple-airtags-tracking_n_61f425ade4b067cbfa1cb2b8)

international in scope, with one woman reporting a harrowing experience in Paris following a flight from the US.[29]

38. Tragically, in multiple instances, AirTag tracking led directly to a murder.

39. In January 2022, an Akron, Ohio woman was stalked by her ex-boyfriend, who buried an AirTag in the back pocket of the passenger seat in her car. The stalker used the AirTag to follow the woman and shoot her.[30]

40. In June of 2022, an Indianapolis woman hid an AirTag in her boyfriend's car, followed him to a bar, and ran him over with her car, killing him at the scene.[31]

E. Individuals Have Few, If Any, Meaningful Remedies When They Are Tracked

41. While Apple has built safeguards into the AirTag product, they are woefully inadequate, and do little, if anything, to promptly warn individuals if they are being tracked. Moreover, there is a gross imbalance between the protections available to iOS/Apple users, versus those available to individuals with Android devices—rendering Android users nearly defenseless to tracking/stalking using an AirTag.

Remedies for iOS Users (and Their Limitations)

42. Apple has attempted to mitigate the potential danger of being unwantedly tracked with an AirTag by introducing several features into its operating (iOS) architecture.

43. **Device-based text notifications:** if an individual has an iPhone, iPad, or iPod Touch with iOS 14.5 or later, their phone is programmed to display an alert if the phone detects

---

[28] Caitlyn Shelton, *AirTag tracks family through Disney World,* ABC News 10 (May 3, 2022) (available at https://www.news10.com/news/crime/airtag-tracks-family-through-disney-world/)

[29] Maggie Kim, *I Was Stalked with an Apple AirTag—Here's What I Wish I'd Known*, Reader's Digest (Feb. 11. 2022) (available at https://www.rd.com/article/apple-airtag-stalking/)

[30] *Family Believes Akron Mother Was Chased Before Murder*, Ohio News (March 2, 2022) (available at https://darik.news/ohio/family-believes-akron-mother-was-chased-before-murder/532936.html)

[31] Alexis McAdams, *Apple AirTags, meant to help you track your stuff, have become tools of stalkers and criminals*, Fox News (June 14, 2022) (available at https://www.foxnews.com/tech/apple-airtag-stalking-dangerous-crime)

an unknown AirTag moving with the device. The warning in question states: "AirTag Found Moving With You. The location of this AirTag can be seen by the owner."

Fig. 8[32]

44. This alert, however, is not immediate. Originally, Apple's algorithm would wait 72 hours before notifying an individual that they had been in the proximity of an unknown AirTag. Put another way, a victim could have been stalked for three days before Apple alerted them of the potential danger.[33] Recently, Apple reduced the time period for the notification, but individuals still report not receiving an alert after as much as a day of being tracked—"[a]ccording to Apple, the timing of the alerts can vary depending on the iPhone's operating system and location settings,"[34] but users have no control over this. As a report by an industry

[32] https://support.apple.com/en-us/HT212227

[33] "*AirTags Are Dangerous — Here's How Apple Could Fix Them,*" note 21, *supra*.

[34] "*Are Apple AirTags Being Used to Track People and Steal Cars?*" note 6, *supra*.

expert noted, "Apple estimates it takes between four and eight hours to send an alert, which could be a potentially fatal span of time."[35]

45. Further, the notification only gets sent to individuals who have (1) iPhones, iPads, or iPod Touches that (2) run iOS version 14.5 or later. This means that the notifications do *not* appear for owners of older iPhones running older software.[36]

Remedies for Android Users (and Their Limitations)

46. While an iPhone owner might get a timely alert that then makes them aware of the potential danger of being tracked by an AirTag, users of Android phones and devices do not have that protection, as their devices run on the Android operating system, which is outside of the control of Apple. To date, Apple has not worked in conjunction with Google to provide automated alerts when Android users are being stalked.

47. Thus, individuals who do not own iPhones, iPads, or iPod Touches are thus more vulnerable to being tracked using an AirTag. Android mobile devices have a 41.9% market share in the United States,[37] meaning that almost half of America's population would not receive any notification if they were being stalked by an AirTag.

48. Apple recently developed an app ("Tracker Detect") for Android devices, but it is inadequate for multiple reasons.

---

[35] Michael Simon, "*Apple has an AirTag Problem—here's how to solve it."* Macworld (Jan. 21, 2022) (available at https://www.macworld.com/article/606934/apple-airtag-problem-notifications-android-sound.html)

[36] The notification also purportedly enables the iPhone, iPad, or iPod Touch user to have the AirTag emit a beep so that it can be located. As discussed in paragraphs 53-58, *infra*, the sound the AirTag emits is hard to hear and easily confused with other gadgets. More importantly, however, this feature appears not to work reliably. One reporter who tested it stated: "The AirTag was literally inches away from [the test] phone, but it wouldn't connect. We tried multiple times. Nada. The same thing happened to me when I was trying to find which pocket of my bag my husband had stashed his AirTag in. My phone was in my hand. My bag was in my other hand. Nothing. This is obviously an issue, as it's hard to get rid of an unknown AirTag if you can't find it. Another problem is that sound alerts may not be helpful if a victim is trying to find the tracker discreetly without tipping off their abuser." *See,* "*AirTags Are Dangerous — Here's How Apple Could Fix Them,*" note 21, *supra*.

[37] https://gs.statcounter.com/os-market-share/mobile/united-states-of-america

49. *First*, the Android device owner would have to be alerted to, or suspect, the potential of AirTag stalking in the first instance, and would then have to search the Google App Store to find Apple's app. Apple has not taken meaningful steps to alert Android users of the threat posed by AirTags, and to date, Tracker Detect has only (roughly) one million downloads, worldwide.[38] Thus, virtually every Android phone user would be oblivious to being tracked by an AirTag.

50. *Second*, the app itself has been described as an example of Apple "fulfilling its obligations *to the least extent possible*."[39]

> The Android app is little more than a button to scan the surrounding area for any nearby trackers. It doesn't perform background scanning or issue push notifications, and it certainly doesn't let Android users track items on the Find My network or set up Find My compatible devices.[40]

51. This limitation is critical and, potentially, deadly: unlike the "always-on" scan that Apple provides for iPhone, iPad, or iPod Touch owners (meaning that these devices constantly conduct background scans for unwanted AirTags), an Android owner must selectively, and intentionally, engage Tracker Detect to conduct a scan. Once that scan concludes, the app will not scan for AirTags again until the Android device owner once more engages the app. Put another way, any Android owner who downloads Tracker Detect must decide when and where to scan for AirTags—something a person being unknowingly tracked would be unlikely to do.

52. Nor is this technology particularly helpful in densely populated areas, where myriad AirTags are likely to be present. As demonstrated by the experience of Plaintiff Doe—see Paragraph 82, *infra*—downloading Tracker Detect was fruitless for determining whether a specific AirTag was in her vicinity. All it could tell her was that AirTags, in general, were nearby.

---

[38] https://play.google.com/store/apps/details?id=com.apple.trackerdetect&hl=en_US&gl=US

[39] "*Apple has an AirTag Problem—here's how to solve it,"* note 35, *supra.*

[40] *Id.*

Remedies That Do Not Rely on a Specific Operating System (and Their Limitations)

53. **Sound notifications:** if an unknown AirTag is away from its owner for a long time—Apple does not specify precisely how long but says between eight and 24 hours—Apple states that the AirTag will play a chime-like sound so that it can be found.

54. However, the alert sound is roughly 60 decibels, which is approximately as loud as a normal conversation between two people, or background music. Moreover, the sound is not particularly distinctive, meaning that it can be mistaken for other, benign and ambient noises coming from other devices. As one reporter who tested the security feature noted: "the sound was easy to confuse with all the other beeps and boops gadgets make these days. It also stopped playing long before [the tester] was able to find it."[41] Ultimately, "[w]hether you hear the AirTag chime feels like a crapshoot."[42]

55. This is particularly problematic if the victim is hearing impaired or in a loud environment, or if the stalker places the AirTag in a place where it will be muffled or out of range of hearing (like the outside of a car). As one commentator noted, "If [an AirTag is] behind your license plate and you're driving, you're never going to hear that."[43]

56. As one other reporter wrote, "Many stalking victims in AirTag cases have complained that when they received the warning that an AirTag was traveling with them, they were unable to find it after searching. This left them feeling exposed and vulnerable, as they weren't sure if the AirTag was still nearby."[44]

---

[41] "*AirTags Are Dangerous — Here's How Apple Could Fix Them,*" note 21, *supra*.

[42] *Id*.

[43] *Id*.

[44] Sarah Perez, "*Apple to Address AirTag Stalking Problems With Upcoming Features*," TechCrunch (Feb. 10, 2022)" (available at https://techcrunch.com/2022/02/10/apple-to-address-airtag-stalking-problem-with-upcoming-features/#:~:text=Many%20stalking%20victims%20in%20AirTag,the%20AirTag%20was%20still%20nearby.)

57. Worse, still, people have figured out how to disable the speaker on AirTags, and are selling modified "silent AirTags" on mainstream e-commerce sites like eBay and Etsy.[45] Per similar reporting, "tutorials that illustrate how to deactivate or completely remove the AirTag's speaker are readily available online. There are no software updates that Apple can release that will make a physically modified AirTag start to make noise again, and the other included safety features are still dependent on victims not only having an up-to-date smartphone but also being technically savvy enough to download and use the necessary apps to find rogue AirTags nearby. *The risks involved with a product like this being abused still seem like they far outweigh the convenience of finding a misplaced set of keys*."[46]

58. Further, in the event an individual finds the AirTag, they must still figure out what to do with it. AirTags can be deactivated by removing the battery. Doing so not only stops it from updating its current location but also alerts the device's owner. However, law enforcement agencies have pointed out that removing the AirTag's battery could potentially contaminate it as evidence.[47]

59. Other options to deal with a found AirTag can be equally fraught: "If the offender is monitoring the victim's actions and sees that the AirTag has now gone to [somewhere like a] police station, that can escalate the situation and put a victim more in danger," cautions Jennifer Landhuis, the director of the Stalking Prevention Awareness and Resource Center.[48]

---

[45] Hartley Charlton, "*Sale of 'Silent AirTags' on eBay and Etsy Raises Privacy Concerns*," MacRumors (Feb. 3, 2022) (available at https://www.macrumors.com/2022/02/03/silent-airtags-privacy-concerns/#:~:text=The%20modified%20AirTags%2C%20dubbed%20%22Silent,battery%20to%20disconnect%20the%20speaker)

[46] Andrew Liszewski, "*Silenced AirTags With Disabled Speakers Are Popping Up for Sale Online*," Gizmodo (Feb. 3, 2022) (available at https://gizmodo.com/silenced-airtags-with-disabled-speakers-for-sale-online-1848473673)

[47] "*AirTags are being used to track people and cars. Here's what is being done about it*," note 14, *supra*.

[48] "*AirTags are being used to track people and cars. Here's what is being done about it*," note 14, *supra*.

F. Victims of Stalking Via AirTags Have Little Meaningful Recourse

60. Even in the event that a victim of AirTag stalking is able to discover the AirTag and bring it to law enforcement, there are very few, meaningful protections that such a victim would then be able to receive. At present, only 23 states have electronic tracking laws,[49] and stalking, in and of itself, is a crime that often goes unprosecuted:

> Stalking goes unrecognized, uncharged, and unprosecuted for a number of reasons. Victims, police, and prosecutors often fail to recognize patterns of behavior as "stalking," or associate the term exclusively with following, monitoring, or surveillance--acts that represent only one variety of the many types of behavior that may fit the statutory definition of stalking. Police and prosecutors may focus on a specific incident that resulted in a law enforcement response (e.g., an assault, an isolated threat, an act of vandalism) and fail to explore the context within which the act was committed—context that may include a course of conduct chargeable as stalking. Prosecutors, failing to understand the strategic value of a stalking charge, may wonder why they should bother "complicating" their case when they have strong evidence of a crime that is perceived to be more serious and easier to prosecute.[50]

61. Indeed, the number of individuals who are stalked in the United States is jaw-dropping. More than 6 million people over the age of 18 are stalked each year in the United States, according to data from the Department of Justice's Bureau of Justice Statistics (BJS).[51] That number is believed to be much higher, however, as BJS statistics indicate just 40% of stalking cases are reported to police.[52] According to the Stalking Prevention, Awareness, and Resource Center (SPARC), one in six women and one in 17 men are stalking survivors. Roughly

---

[49] Alexis McAdams, "*Apple AirTags, meant to help you track your stuff, have become tools of stalkers and criminals,*" Fox News (June 14, 2022) (available at https://www.foxnews.com/tech/apple-airtag-stalking-dangerous-crime).

[50] Stalking Prevention Awareness and Resource Center ("SPARC"). *Prosecutor's Guide to Stalking* (2020) (available at https://www.stalkingawareness.org/wp-content/uploads/2020/01/SPA-19.005-Prosecutors-Guide-to-Stalking-00000002.pdf)

[51] Megan Stone, "*After 9-year fight to prosecute her stalker, woman shares story to help other survivors*," ABC News (Jan. 5, 2021) (available at https://abcnews.go.com/GMA/Living/year-fight-prosecute-stalker-woman-shares-story-survivors/story?id=74878256)

[52] *Id*.

15% of those individuals said the stalking forced them to move.[53] Yet, once reported to the police, only 8% of stalking perpetrators are arrested.[54]

G. The Federal Trade Commission Makes Clear That Stalking Technologies and Unwanted Location Tracking Violates Section 5 of the FTC Act.

62. Recent enforcement actions by the FTC directly speak to the plainly-illegal, dangerous, and fundamentally unfair nature of Apple's conduct.

63. For example, in August 2022, the Commission filed suit against the data broker Kochava, Inc.

> [F]or selling geolocation data from hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations. Kochava's data can reveal people's visits to reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities. The FTC alleges that by selling data tracking people, Kochava is enabling others to identify individuals and exposing them to threats of stigma, stalking, discrimination, job loss, and even physical violence.[55]

64. Per the Commission, the lawsuit involves Kochava's "vast troves of location information derived from hundreds of millions of mobile devices….People are often unaware that their location data is being purchased and shared by Kochava and have no control over its sale or use."[56]

65. Risks associated with the unwanted collection of location data include identification of individuals' home addresses, and, more broadly, "puts consumers at significant risk. The company's data allows purchasers to track people at sensitive locations that could reveal information about their personal health decisions, religious beliefs, and steps they are

---

[53] *Id.*

[54] *Id.*

[55] Federal Trade Commission, "*FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*" (August 29, 2022) (available at https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other)

[56] *Id.*

taking to protect themselves from abusers. The release of this data could expose them to stigma, discrimination, physical violence, emotional distress, and other harms."[57]

66. Such acts and practices "reveal consumers' visits to sensitive locations, including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at-risk populations, and addiction recovery" and, in turn "cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition." Accordingly, they "constitute unfair acts or practices in violation of Section 5 of the FTC Act."[58]

67. The enforcement action against Kochava is not an outlier. In 2019, the FTC brought an enforcement action against Retina-X, a company accused of creating "stalking apps," that could be placed on users phones in order to surreptitiously surveil them. Like the Kochava action, and like the instant action against Apple, "these apps were designed to run surreptitiously in the background and are uniquely suited to illegal and dangerous uses. Under these circumstances, we will seek to hold app developers accountable for designing and marketing a dangerous product."[59]

68. There, as here, the defendant "sold monitoring products and services that required circumventing certain security protections implemented by the Mobile Device operating system or manufacturer, and did so without taking reasonable steps to ensure that the monitoring products and services will be used only for legitimate and lawful purposes by the purchaser. Respondents' actions cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to

---

[57] *Id.*

[58] Complaint, *Federal Trade Commission v. Kochava, Inc.*, Case No. 2:22-cv-377 (D. Idaho), Dkt. No. 1 at ¶¶ 36-38.

[59] Federal Trade Commission, "*FTC Brings First Case Against Developers of 'Stalking' Apps*," (October 22, 2019) (available at https://www.ftc.gov/news-events/news/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps)

consumers or competition. This practice is an unfair act or practice [in violation of the FTC Act]"[60]

H. Plaintiffs' Experience With AirTags.

i. Lauren Hughes

69. Plaintiff Hughes began being stalked online in late August 2021, following the breakup of a three-month relationship. Her stalker began by making abusive posts on various social media accounts, as well as using fake accounts to try to follow Plaintiff Hughes's own, private social media accounts (as Ms. Hughes had previously blocked her stalker).

70. The stalker continued his campaign, calling Ms. Hughes from blocked numbers and leaving threatening voicemails. When she ignored him, he posted screenshots of their text conversations to his Twitter account, seeking to embarrass Ms. Hughes by revealing the contents of private conversations.

71. Throughout September, the stalker's behavior escalated, with him creating fake social media accounts under Ms. Hughes' name, and continuing to leave threatening messages from blocked numbers and even leaving objects at Ms. Hughes' residence. *E.g.,*

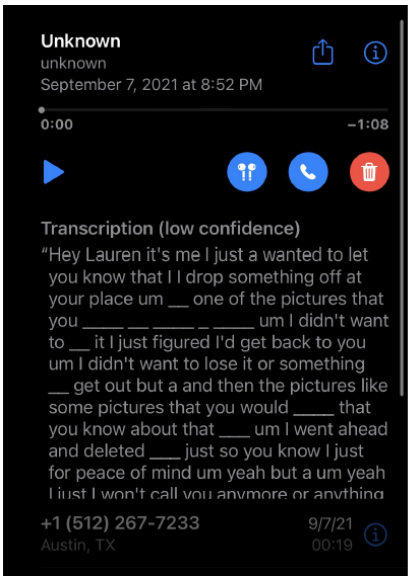


Fig. 9

[60] *In the Matter of Retina-X Studios, LLC, a limited liability company; and James N. Johns, Jr., individually and as sole member of Retina-X Studios, LLC.*, FTC Matter/File Number 172-3118, Complaint, at ¶ 32.

Fig. 10

72. By October 2021, Ms. Hughes elected to move, fearing for her safety and staying in a hotel until she could fully move from her current residence.

73. On October 7, Ms. Hughes was returning to her hotel room from her apartment, after having spent the day packing for her move. Once she got to the hotel, she received a notification on her iPhone that an unknown AirTag was traveling in her vicinity. Ms. Hughes attempted to engage the feature causing the AirTag to beep, but could only get it to work one time.

74. Ms. Hughes searched her car and found an AirTag, placed by her stalker, in the wheel well of the rear passenger tire of her car. The AirTag had been colored with a sharpie marker and tied up in a plastic baggie.

Fig. 11

75. Terrified that her stalker now knew the location of both her hotel and her new residence, Ms. Hughes took the AirTag to a nearby Apple Store and asked how long the AirTag had been on her car. The employees stated that they could not tell.

76. Ms. Hughes brought the AirTag back to her apartment and then returned to her hotel. The following day, Plaintiff returned to her apartment to continue the process of moving. On her way to her apartment, she encountered a strange man who was lurking near her apartment and looking at his phone. Ms. Hughes entered her apartment to find that the door jamb had been damaged and the AirTag was making noise. Ms. Hughes believes that the stranger had been sent by her stalker to retrieve the AirTag.

77. Thereafter, Ms. Hughes went to her local police department and was told by a detective that they could read the stalker a cease and desist, "but that's about it."

78. Ms. Hughes subsequently moved. However, by March 15, 2022, her stalker once again posted on social media, showing a picture of a taco truck in Plaintiff's new neighborhood, including hashtags referencing streets in Plaintiff's new neighborhood, and including a winking emoji with the separate hashtag "#airt2.0"

Fig. 12

79. Ms. Hughes continues to fear for her safety—at minimum, her stalker has evidenced a commitment to continuing to use AirTags to track, harass, and threaten her, and continues to use AirTags to find her location.

ii. Plaintiff Jane Doe[61]

80. Plaintiff Doe first encountered an unwanted AirTag in the Summer of 2022. In the wake of a contentious divorce, she found her former spouse harassing her, challenging her about where she went and when, particularly when she was with the couple's child.

81. Ms. Doe was unable to figure out how her former spouse could follow her movements so closely, until one day she found an AirTag in her child's backpack. She attempted to disable or otherwise render ineffective that AirTag, but another one soon showed up in its place.

82. Ms. Doe asked a friend to download the Tracker Detect app to see if she could confirm the presence of additional, hidden AirTags moving forward. However, she lives in a densely populated area, meaning that the app would constantly tell her (unsurprisingly) that AirTags abounded nearby, but the app was unable to help her confirm or deny whether a specific AirTag was being placed in her child's effects by her estranged spouse.

83. Ms. Doe continues to fear for her safety—at minimum, her stalker has evidenced a commitment to continuing to use AirTags to track, harass, and threaten her, and continues to use AirTags to find Plaintiff's location.

84. Plaintiff Doe seeks to bring this action anonymously due to the real risk that being identified would expose her to increased risk of harassment and/or physical harm.

[61] When a plaintiff asks to proceed anonymously, the court must balance "the general presumption that parties' identities are public information" against "(1) the severity of the threatened harm; (2) the reasonableness of the anonymous party's fears; and (3) the anonymous party's vulnerability to . . . retaliation." *Doe v. Ayers*, 789 F.3d 944, 945 (9th Cir. 2015). The Ninth Circuit has stated that, "[i]n this circuit, we allow parties to use pseudonyms in the 'unusual case' when nondisclosure of the party's identity 'is necessary . . . to protect a person from harassment, injury, ridicule or personal embarrassment'" and then noted that in *Doe v. Madison Sch. Dist. No. 321*, 147 F.3d 832, 834 n.1 (9th Cir. 1998), *vacated on other grounds*, 177 F.3d 789 (9th Cir. 1999) (en banc), the "plaintiff filed [the] case as 'Jane Doe' because she feared retaliation by the community." *Does I thru XXIII v. Advanced Textile Corp.*, 214 F.3d 1058, 1067-68 (9th Cir. 2000) (cleaned up). Here, Plaintiff Doe is involved in a contentious divorce, in which an estranged former spouse is engaging in paradigmatically abusive behavior. The threat of harm is severe; Plaintiff's fears are reasonable, and the threat of retaliation is substantial.

CLASS ALLEGATIONS

85. Plaintiffs bring this class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes and sub-classes, which are jointly referred to throughout this Complaint as the "Class:"

> **The iOS Stalked Class:** all persons residing in the United States who own iOS devices and who were tracked, without consent, by Apple's AirTag.
>
> **The Android Stalked Class:** all persons residing in the United States who own Android devices (and who do not own iOS devices) and who were tracked, without consent, by Apple's AirTag.
>
> **The iOS At-Risk-Of-Stalking Class:** all persons residing in the United States who own iOS devices.
>
> **The Android At-Risk-Of-Stalking Class:** all persons residing in the United States who own Android devices.
>
> **The Multistate Sub-Class:** all persons residing in the States of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia who were tracked, without consent, by Apple's AirTag.
>
> **The New York Sub-Class:** all persons residing in the State of New York who were tracked, without consent, by Apple's AirTag.

86. Plaintiff Lauren Hughes is the proposed Class Representative for the iOS Stalked Class, the iOS At-Risk-of-Stalking Class, and the Multistate Sub-Class. Plaintiff Jane Doe is the proposed Class Representative for the Android Stalked Class, the Android At-Risk-Of-Stalking Class, and the New York Sub-Class.

87. Excluded from each Class are the following individuals: officers and directors of Apple and its parents, subsidiaries, affiliates, and any entity in which Apple has a controlling

interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

88. Plaintiffs reserve the right to modify or amend the definition of each of the proposed Classes before the Court determines whether certification is appropriate.

89. This action readily satisfies the requirements set forth under Federal Rule of Civil Procedure 23:

a. Each Class is so numerous that joinder of all members is impracticable. As of April 2022, at least 150 police reports were filed describing AirTags being used to stalk victims,[62] however this number only captures incidents that were (1) reported to police and (2) obtained through FOIA results. Upon Plaintiff's counsel's investigation, information, and belief, this number is significantly higher.

b. There are questions of law or fact common to the Classes. These questions include, but are not limited to, the following:

i. Whether Apple's acts and practices complained of herein amount to the use of an electronic tracking device to determine the location or movement of a person, in violation of Cal. Pen. Code § 637.7;

ii. Whether AirTags are "electronic tracking devices" under Cal. Pen. Code § 637.7(d);

iii. Whether Apple's acts and practices complained of herein amount to egregious breaches of social norms;

iv. Whether Apple acted intentionally in violating Plaintiffs' and Class members' privacy rights;

v. Whether Apple's acts and practices complained of herein violate N.Y. GBL § 349;

vi. Whether an injunction should issue; and

---

[62] Samantha Cole, "*Police Records Show Women Are Being Stalked With Apple AirTags Across the Country*," Vice (Apr. 6, 2022) (available at https://www.vice.com/en/article/y3vj3y/apple-airtags-police-reports-stalking-harassment)

vii. Whether declaratory relief should be granted.

c. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class members, were subject to unwanted stalking via the Apple AirTag.

d. Moreover, like all Class members, Plaintiffs suffer a substantial risk of repeated injury in the future. Each Plaintiff continues to be at risk of unwanted and unlawful tracking via an AirTag device. Because the conduct complained of herein is systemic, Plaintiffs and all Class Members face substantial risk of the same injury in the future. Apple's conduct is common to all Class members and represents a common pattern of conduct resulting in injury to all members of the Class. Plaintiffs have suffered the harm alleged and have no interests antagonistic to any other Class member.

e. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs' interests do not conflict with the interests of the Class members. Furthermore, Plaintiffs have retained competent counsel experienced in class action litigation, consumer protection litigation, and electronic privacy litigation. Plaintiffs' counsel will fairly and adequately protect and represent the interests of the Class. FRCP 23(a)(4) and 23(g) are satisfied.

f. In acting as above-alleged, and in failing and refusing to cease and desist despite public outcry, Apple has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and corresponding declaratory relief each appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class members would create the risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Apple.

g. Injunctive relief is necessary to prevent further unlawful and unfair conduct by Apple. Money damages, alone, could not afford adequate and complete relief, and injunctive relief is necessary to restrain Apple from continuing to commit its illegal and unfair violations of privacy.

CAUSES OF ACTION

COUNT I
(Negligence)
(On Behalf of the Class)

90. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

91. Apple owed Plaintiffs and Class members a duty of care in its design, marketing, and introduction into the market of its AirTags. This duty is evidenced by, *inter alia*, Apple's unique position to monitor Plaintiffs' and Class members' behavior through AirTags' access to Apple's vast network of mobile devices, which in turn are used to locate Plaintiffs and Class members with unparalleled reach and precision. It is further supported by the surreptitious and non-intuitive nature of Defendant's tracking.

92. Apple breached that duty by rushing AirTags to market with insufficient safeguards to prohibit their use for stalking purposes.

93. This breach of duty on the part of Apple was the proximate or legal cause of injury suffered by Plaintiffs and Class members.

94. As a result of Apple's actions, Plaintiffs and Class members seek injunctive relief, damages and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Apple's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights. Punitive damages are warranted to deter Apple from engaging in future misconduct.

COUNT II
(Strict Liability – Design Defect – Consumer Expectation Test)
(On Behalf of the Class)

95. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

96. Apple manufactures, distributes, and sells its AirTag product.

97. Apple's design of the AirTag was defective because the product did not—and does not—perform as safely as an ordinary consumer would have expected it to perform when used or misused in an intended or reasonably foreseeable way. The foreseeability of the

use/misuse of AirTags for stalking is evidenced by, *inter alia*, the fact that Apple preemptively sought to assuage consumer fears by (falsely) claiming that AirTags were "stalker-proof" in multiple media outlets.

98. Plaintiffs and Class members were harmed as a result of the AirTag's design defect.

99. The AirTag's design defect was a substantial factor in causing Plaintiffs' and Class members' harm.

100. As a result of Apple's actions, Plaintiffs and Class members seek injunctive relief, damages and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Apple's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights. Punitive damages are warranted to deter Apple from engaging in future misconduct.

COUNT III
(Strict Liability – Design Defect – Risk-Benefit Test)
(On Behalf of the Class)

101. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

102. Apple manufactures, distributes, and sells its AirTag product.

103. The AirTag was defectively designed.

104. Plaintiffs and Class members were harmed as a result of the AirTag's design defect.

105. The AirTag's design defect was a substantial factor in causing Plaintiffs' and Class members' harm.

106. The benefits of Apple's AirTag design do not outweigh the risks of the design. A consideration of the following factors—the gravity of the potential harm caused by the design defect (*i.e.*, its propensity for use in stalking and other crimes); the likelihood that this harm would occur; the feasibility of an alternative safer design at the time of manufacture; the cost of an alternative design; and any disadvantages of an alternative design all weigh in favor of

Plaintiffs and the Class, and make clear that the risks associated with the AirTag outweigh the benefits.

107. As a result of Apple's actions, Plaintiffs and Class members seek injunctive relief, damages and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Apple's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights. Punitive damages are warranted to deter Apple from engaging in future misconduct.

COUNT IV
(Unjust Enrichment)
(On Behalf of the Class)

108. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

109. Apple should have not released the AirTags into the stream of commerce, because of the dangers detailed herein.

110. As a result of Apple's selling the AirTags, Apple received a benefit, which it is unjust for Apple to retain.

111. Under the circumstances, it is against equity and good conscience to permit Apple to retain the ill-gotten benefits that it received from the conduct complained of herein.

112. As a direct and proximate result of Apple's actions, Apple has been unjustly enriched. Plaintiffs and Class members have a right to restitution in an amount to be proven at trial.

COUNT V
(Intrusion Upon Seclusion)
(On Behalf of the iOS Stalked Class,
the iOS At-Risk-Of-Stalking Class
and the Multistate Sub-Class)

113. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

114. Plaintiffs and Class members have reasonable expectations of privacy in their persons and their whereabouts, generally. Plaintiffs' and Class members' private affairs include their locations.

115. The reasonableness of such expectations of privacy is supported by Apple's unique position to monitor Plaintiffs' and Class members' behavior through AirTags' access to Apple's vast network of mobile devices, which in turn are used to locate Plaintiffs and Class members with unparalleled reach and precision. It is further supported by the surreptitious and non-intuitive nature of Defendant's tracking.

116. Defendant intentionally intruded on and into Plaintiffs' and Class members' solitude, seclusion, or private affairs by intentionally geolocating them.

117. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, Supreme Court precedent (most recently and forcefully articulated in the *Carpenter* opinion), legislation enacted by Congress, rules promulgated and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying location tracking, particularly in the context of stalking and abuse.

118. Plaintiffs and Class members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

119. Apple's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Class members.

120. As a result of Apple's actions, Plaintiffs and Class members seek injunctive relief, damages and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Apple's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights. Punitive damages are warranted to deter Apple from engaging in future misconduct.

COUNT VI
(California Constitutional Right to Privacy)
(On Behalf of the iOS Stalked Class and the iOS At-Risk-Of-Stalking Class)

121. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

122. Plaintiffs and Class members have reasonable expectations of privacy in their persons and their whereabouts, generally. Plaintiffs' and Class members' private affairs include their locations.

123. Apple intentionally intruded on and into Plaintiffs' and Class members' solitude, seclusion, right of privacy, or private affairs by intentionally tracking their location with AirTags.

124. These intrusions are highly offensive to a reasonable person, because they disclosed sensitive and confidential location information, constituting an egregious breach of social norms. This is evidenced by, *inter alia*, Supreme Court precedent (most recently and forcefully articulated in the *Carpenter* opinion), legislation enacted by Congress, rules promulgated and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying location tracking, particularly in the context of stalking and abuse.

125. Plaintiffs and Class members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

126. Apple's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Class members.

127. As a result of Apple's actions, Plaintiffs and Class members seek injunctive relief, damages and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Apple's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights. Punitive damages are warranted to deter Apple from engaging in future misconduct.

COUNT VII
(Violations of CIPA, Cal. Pen. Code §§ 630, *et seq.*)
(On Behalf of the iOS Stalked Class and the iOS At-Risk-Of-Stalking Class)

128. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

129. Cal. Pen. Code § 630 provides that "[t]he Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques

for the purpose of eavesdropping upon private communication and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society."

130. Apple's acts and practices complained of herein violated and continue to violate Cal. Pen. Code § 637.7.

131. Cal. Pen. Code § 637.7(a) prohibits the use of an electronic tracking device to determine the location or movement of a person. As used in Cal. Pen. Code § 637.7, "electronic tracking device" means "any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals." Cal. Pen. Code § 637.7(d).

132. In direct violation of this prohibition and without the consent of Plaintiffs or Class members, Apple has knowingly introduced into the stream of commerce a standalone device whose sole purpose is to locate whatever it is affixed to. Apple has done this despite being warned prior to and immediately after the release of the AirTag that the product is a dangerous tool that enables stalkers and abusers.

133. As described herein, AirTags are "electronic tracking devices" as defined by Cal. Pen. Code § 637.7(d), used "to determine the location or movement of a person." Cal. Pen. Code § 637.7(a).

134. As a result of Apple's violations of Cal. Pen. Code § 637.7, and pursuant to Cal. Pen. Code § 637.2, Plaintiffs and Class members are entitled to the following relief: (1) A declaration that Apple's conduct violates CIPA; (2) Statutory damages and/or trebled actual damages; (3) Injunctive relief in the form of, *inter alia*, an order enjoining Apple from using AirTags to geolocate Class members in violation of CIPA; (4) Injunctive relief in the form of, *inter alia*, an order requiring Apple to destroy all data created or otherwise obtained from its illegal tracking of Class members; and (5) An award of attorney's fees and costs of litigation as provided by CIPA, the private attorney general doctrine existing at common law and also codified at California Civil Code Section 1021.5, and all other applicable laws.

COUNT VIII
(Negligence *Per Se*)
(On Behalf of the iOS Stalked Class,
the iOS At-Risk-Of-Stalking Class,
and the New York Class)

135. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

136. As set forth above, Apple's conduct complained of herein violated both CIPA and California's Constitutional Right to Privacy. Additionally, as set forth in Paragraphs 161-169, *infra*, Apple's conduct violates New York General Business Law § 349.

137. These violations of CIPA and California's Constitutional Right to Privacy proximately caused injury to Plaintiff Hughes and the iOS Stalked Class and the iOS At-Risk-Of-Stalking Class. The violations of NY GBL § 349 proximately caused injury to Plaintiff Doe and the New York Class.

138. These injuries resulted from an occurrence, the nature of which CIPA, California's Constitutional Right to Privacy, and NY GBL § 349 were designed to prevent.

139. Plaintiff Hughes, the iOS Stalked Class, and the iOS At-Risk-Of-Stalking Class are a part of the class of persons for whose protection CIPA and California's Constitutional Right to Privacy were made into law, respectively. Plaintiff Doe and the New York Class are a part of the class of persons for whose protection NY GBL § 349 was made into law.

140. As a result of Apple's actions, Plaintiffs and Class members seek injunctive relief, damages and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Apple's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights. Punitive damages are warranted to deter Apple from engaging in future misconduct.

COUNT IX
(California Bus. and Prof. Code § 17200, *et seq.* – Unlawful Prong)
(On Behalf of the iOS Stalked Class and
the iOS At-Risk-Of-Stalking Class)

141. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

142. As set forth above, Apple's conduct violates multiple laws of the State of California, including CIPA and California's Constitutional Right to Privacy, and amount to acts of negligence, negligence *per se*, intrusion-upon-seclusion, and product liability. Each of these independent violations of law also serve as predicate violations of the UCL's unlawful prong.

143. Plaintiff Hughes has standing to pursue this claim as she suffered injury in fact and has lost money or property as a result of Apple's actions as set forth herein. Specifically, Plaintiff Hughes has been forced to move at least once—and perhaps more times in the future—as a result of having her whereabouts monitored, by her stalker, via Apple's AirTags.

144. Pursuant to section 17203 of the UCL, Plaintiff Hughes, individually and on behalf of the iOS Stalked Class and the iOS At-Risk-Of-Stalking Class, seeks restitution and an order of this Court enjoining Apple from engaging in the unlawful business practices alleged herein in connection with the sale of AirTags.

COUNT X
(California Bus. and Prof. Code § 17200, *et seq*. – Unfair Prong)
(On Behalf of the iOS Stalked Class and the iOS At-Risk-Of-Stalking Class)

145. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

146. Apple's business practices, as alleged herein, are unfair because its conduct in releasing AirTags into the marketplace is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers. The gravity of the harm to consumers is not outweighed by the utility of Apple's conduct.

147. Apple's business practices are also unfair because they undermine public policy, which is tethered to specific statutory provisions, including CIPA and the California Constitutional Right to Privacy.

148. Lastly, Apple's business practices are unfair because: (1) the injury to the consumer is substantial; (2) the injury is not outweighed by any countervailing benefits to consumers or competition; and (3) consumers could not reasonably have avoided the injury.

149. There were reasonably available alternatives to further Apple's legitimate business interests, other than the conduct described above.

150. Apple's wrongful business practices constituted, and constitute, a continuing course of conduct of unfair competition since Apple is continuing to sell AirTags.

151. Plaintiff Hughes has standing to pursue this claim as she suffered injury in fact and has lost money or property as a result of Apple's actions as set forth herein. Specifically, Plaintiff Hughes has been forced to move at least once—and perhaps more times in the future—as a result of having her whereabouts monitored, by her stalker, via Apple's AirTags.

152. Pursuant to section 17203 of the UCL, Plaintiff Hughes, individually and on behalf of the iOS Stalked Class and the iOS At-Risk-Of-Stalking Class, seeks restitution and an order of this Court enjoining Apple from engaging in the unlawful business practices alleged herein in connection with the sale of AirTags.

COUNT XI
(California Bus. and Prof. Code § 17200, *et seq*. – Fraudulent Prong)
(On Behalf of the iOS Stalked Class and the iOS At-Risk-Of-Stalking Class)

153. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

154. Apple has engaged in numerous fraudulent statements and omissions in connection with the release and sale of AirTags.

155. First, Apple affirmatively sought to deceive the public by representing, and causing to be represented in the media, that AirTags are "stalker-proof" (*see* Paragraphs 32-33, *supra*). Such representations were meant to assuage or preempt concerns of advocacy groups, law enforcement, and members of the general public. This deceptive representation had its intended effect, and further still has the likelihood of deceiving these same entities, by and large.

156. Similarly, Apple's failure to candidly and publicly address the dangers associated with its AirTags—and its efforts to downplay same—deceive the general public (including Class members) by failing to alert them of the dangers associated with AirTags. This is problematic for all Class members, as they are unlikely to learn of the dangers associated with AirTags until they have become victims of stalking. At minimum, they will not learn about the dangers through any affirmative representations or public undertaking on the part of Apple.

157. Plaintiff Hughes and members of the iOS Stalked Class and the iOS At-Risk-Of-Stalking Class have been injured by Apple's fraudulent representations and omissions for the reasons set forth above. A material risk has manifested and/or is likely to manifest in the future, but Apple has done its best to hide this fact from Plaintiff and Class members.

158. These misrepresentations and omissions were an immediate cause—if not the predominant, decisive or even sole factor—of the injury-producing conduct.

159. Plaintiff Hughes has standing to pursue this claim as she suffered injury in fact and has lost money or property as a result of Apple's actions as set forth herein. Specifically, Plaintiff Hughes has been forced to move at least once—and perhaps more times in the future—as a result of having her whereabouts monitored, by her stalker, via Apple's AirTags.

160. Pursuant to section 17203 of the UCL, Plaintiff Hughes, individually and on behalf of the iOS Stalked Class and the iOS At-Risk-Of-Stalking Class, seeks restitution and an order of this Court enjoining Apple from engaging in the unlawful business practices alleged herein in connection with the sale of AirTags.

COUNT XII
(N.Y. Gen. Bus. Law § 349)
(On Behalf of the New York Class)

161. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

162. Plaintiff Jane Doe and New York Class members are "persons" within the meaning of New York General Business Law § 349(h).

163. Defendant is a "person," "firm," "corporation," or "association" within the meaning of N.Y. Gen. Bus. Law § 349.

164. Section 349 makes unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce."

165. Defendant's conduct constitutes "deceptive acts or practices" within the meaning of N.Y. Gen. Bus. Law § 349.

166. Defendant's conduct occurred in the conduct of trade or commerce and was consumer-oriented.

167. Defendant's conduct was misleading in a material way, because, *inter alia*, Apple materially misrepresented the dangers of AirTags to the public and further failed to provide adequate warnings and/or information about the risks of unwanted tracking.

168. By both making affirmatively misleading statements and by failing to adequately disclose risks inherent in AirTags, Apple caused injury to Plaintiffs and Class members, in the form of unwanted tracking of their personal and private locations, coupled with heightened risk of similar stalking in the future.

169. Because Defendant's willful and knowing conduct caused injury to Plaintiffs and Class members, the Class seeks recovery of actual damages or $50, whichever is greater, discretionary treble damages up to $1,000, punitive damages, reasonable attorneys' fees and costs, an order enjoining Defendant's deceptive conduct, and any other just and proper relief available under N.Y. Gen. Bus. Law § 349. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' and Class members' rights. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

RELIEF REQUESTED

Plaintiffs, on behalf of themselves and members of the general public, requests the Court to enter judgment against Defendant, and accordingly, request the following:

a. That judgment be entered against Defendant and in favor of Plaintiffs on the causes of action set forth in this Complaint;

b. That judgment be entered against Defendant for all injunctive, declaratory, and other equitable relief sought, including but not limited to an order enjoining Apple from further unlawful, unfair and/or fraudulent practices with respect to the design, manufacture, and release into the market of its AirTags;

c. That Plaintiffs and Class members be awarded actual, nominal, statutory, and/or punitive damages, in an amount to be determined at trial;

d. Reasonable attorney's fees and litigation costs, pursuant to Cal. Civ. Proc. Code § 1021.5; and

e. All other such other relief as may be appropriate.

JURY TRIAL DEMANDED

Plaintiffs demand a jury trial on all triable issues.

Dated: December 5, 2022

MILSTEIN JACKSON FAIRCHILD & WADE, LLP

/s/ Gillian L. Wade
Gillian L. Wade
Sara D. Avila
Marc A. Castaneda
10990 Wilshire Blvd., 8th Floor
Los Angeles, California 90024
Tel: (310) 396-9600
Fax: (310) 396-9635
gwade@mjfwlaw.com
savila@mjfwlaw.com
mcastaneda@mjfwlaw.com

Edwin J. Kilpela, Jr.
Elizabeth Pollock-Avery
Kenneth A. Held
LYNCH CARPENTER, LLP
1133 Penn Ave, 5th Floor
Pittsburgh, Pennsylvania 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
ekilpela@lcllp.com
elizabeth@lcllp.com
ken@lcllp.com

wh LAW
David Slade
Brandon Haubert
Jessica Hall
1 Riverfront Place, Suite 745
North Little Rock, AR 72114
Telephone: 501.891.6000
Facsimile: 501.222.3027
slade@wh.law
brandon@wh.law
jessica@wh.law

Attorneys for Plaintiffs Lauren Hughes and Jane Doe