IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

Rachel Fox,	)	
	)	
Plaintiff,	)	
	)	**Civil Action No.**
v.	)	
	)	**JURY TRIAL DEMANDED**
Apple, Inc.	)	
	)	
Defendant.	)	

COMPLAINT

COMES NOW, Plaintiff Rachel Fox ("Ms. Fox" or "Plaintiff") by and through counsel, and for her Complaint against Defendant Apple, Inc. ("Apple" or "Defendant") alleges the following:

INTRODUCTION

1. Apple must be held accountable for its continuing failure to adequately protect members of the public from being stalked with its AirTag.

2. In 2021, Apple released this product knowing full well that it could—and *would*—be purchased and used by abusive, dangerous individuals, to track, coerce, control, and otherwise endanger and abuse innocent victims.

3. And, in 2021, Apple *also* knew that adequate safeguards had not yet been implemented. Nonetheless, the AirTag was made available to the public. Since that time, Apple has played—and continues to play—catch up, quietly introducing new features that attempt to curtail the dangers of a product that is now five years old.

4. But Apple concedes that ***even today*** AirTags remain a profound risk to people like Plaintiff.

5. Apple's acts and practices, as detailed further herein, amount to acts of California negligence; California strict product liability; violations of California's Unfair Competition Law ("UCL") Cal. Bus. Profs. Code § 17200, et seq.; Texas negligence; Texas strict product liability; Texas intrusion upon seclusion; and Texas unjust enrichment. Plaintiff seeks 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. Plaintiff also seeks damages.

PARTIES

6. Plaintiff Rachel Fox is a citizen of the State of Texas, residing in The Colony, Denton County, Texas.

7. Defendant Apple, Inc. ("Apple") is an American multinational technology corporation organized under the laws of the State of California, with its principal place of business 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

8. This Court has subject matter pursuant to 28 U.S.C. § 1332(a). Plaintiff and Defendant are citizens of different States, and the amount in controversy is over $75,000.

9. This Court has personal jurisdiction over Defendant for the following reasons. At all relevant times, it has engaged in substantial business activities in the State of Texas, including selling and distributing AirTags in Texas. A substantial part of the events giving rise to the claims occurred in Texas. At all relevant times, Defendant transacted, solicited, and conducted business

in Texas through its employees, agents, and sales representatives, and derived substantial revenue from such business. Apple has sufficient minimum contacts with the State of Texas, including pursuant to the Texas long-arm statute, Tex. Civ. Prac. & Rem. Code § 17.042, such that the exercise of personal jurisdiction comports with due process. Apple purposefully directed its AirTag product into Texas, and Plaintiff's injuries arose out of Apple's forum-related activities.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(2) because a substantial portion of the acts and occurrences giving rise to this Complaint occurred in this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(1) because Defendant Apple Inc. is a corporation subject to personal jurisdiction in this district with respect to this action and therefore resides in this district under 28 U.S.C. § 1391(c)(2), including through its distribution and sale of AirTags to consumers throughout the State of Texas.

FACTUAL ALLEGATIONS

11. In response to an April 2, 2024 report aired in the United Kingdom on ITV News, titled AirTags becoming 'weapon of choice of stalkers' as GPS tracker cases rocket by 317%,[1] Apple made the following statement: "We have identified even more ways we can update Airtag safety warnings and help guard against further unwanted tracking"

[1] Available at https://www.youtube.com/watch?v=TBhYdgt1FhE



AirTags becoming 'weapon of choice of stalkers' as GPS tracker cases rocket by 317% | ITV News

Fig. 1 (April 2, 2024)

12. This promise of future, unspecified action comes far too late. Indeed, it is meaningless for Plaintiff, who already has been harmed in life-altering ways by Apple's recklessness. The time for ensuring adequate safety warnings and better ways to guard against unwanted tracking was years ago, in April 2021, prior to the release of the AirTag. It is unconscionable for Apple to allow a product to remain on the market that it still knows to be unsafe.

13. Indeed, Apple has always known that any safeguards it purported to build into AirTags would only, in Apple's own words "deter as opposed to prevent malicious use."

14. 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.[2]

[2] 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)

15. Apple's AirTags have become a critical—and shameful—part of this ecosystem. From April 20th, 2021, to April 5th, 2024, Apple received over 40,000 stalking reports, over 1,000 complaints per month on average.

16. Over the first year and a half after AirTag was released, law enforcement requested information from Apple almost 20 times more often for stalking incidents than for theft investigations.

17. The scope of Apple's stalking problem was therefore apparent to Apple from the outset. Indeed, only weeks after the AirTag's release, Apple CEO Tim Cook was briefed on press reports that the AirTag was a "new means of inexpensive, effective stalking." But Cook was advised that Apple could weather the storm: "At this time, we are not seeing this narrative gain steam in media or on social…."

18. Apple proceeded to lie to the public, claiming in its reactive PR campaign that stalking incidents were "rare" when at the same time it was collecting thousands of reports internally concerning what Apple euphemized as "unwanted tracking."

19. Apple allowed the epidemic of AirTag stalking to continue, never adequately updating the device's so-called "safety features," and never disclosing to the public the extent to which AirTag had become a unique and widely used tool of endangerment that allows stalkers to precisely target and track victims with an ease that had never before been possible.

20. Furthermore, Apple has failed to provide any support to victims of stalking and indeed operates in a way that protects stalkers from facing justice. It routinely refuses to cooperate with victims seeking help in prosecuting or seeking restraining orders against their stalkers. Apple regularly deletes pairing information that associates stalkers with the AirTags they used, giving victims only weeks to try to obtain the information from Apple before it destroys it. Apple often

refuses to comply with private subpoenas in civil restraining order cases. As a result of Apple's conduct, stalking victims have been unable to successfully obtain restraining orders or prosecute their stalkers.

21. 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.

22. 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.[3] One in seven stalking victims move as a result of their victimization.[4] Unsurprisingly, stalking victims suffer much higher rates of depression, anxiety, insomnia, and social dysfunction than people in the general population.[5]

23. 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.

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

---

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

[4] *Id*.

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

25. 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.

26. 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.

27. 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.

28. 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.

29. 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."

30. The concerns of these organizations—whom Apple did not consult—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. As noted above, Apple, itself, received over 1,000 reports per month from victims over a three-year period.

31. The consequences have been as severe as possible: multiple murders have occurred in which the murderer used an AirTag to track the victim. Similarly, individuals have been murdered—or murdered others—when using AirTags to track down stolen property and confront the thieves.

32. Its "stalker proof" protections exposed as totally inadequate, Apple has spent the last five years scrambling to address its failures in protecting people from unwanted, dangerous tracking. To date, most if not all, of these failures persist, and Apple continues to find itself in the position of reacting to the harms its product has unleashed, as opposed to prophylactically preventing those harms. As one commentator observed: "*You wouldn't allow a car to come to mass-market without having vigorous testing, so why are we allowing smart tech to just be released and then fixing safety features later?*"[6]

33. The effects are devastating. Finding a mysterious homing beacon hidden in your personal effects or your car is a terrifying experience. It forces an undeniable reckoning with the fact that someone—perhaps someone you know, perhaps not—is aware of your every move.

34. A victim's fear of a stalker being able to locate them with precision finding, over a period of weeks, months, or longer, is unique to AirTag. Before the release of AirTag, the types of electronic devices available to stalkers were generally limited to GPS trackers that were large and difficult to hide, very expensive, powered by batteries that lasted days rather than months, and were obtainable only through specialty outlets as opposed to nearly every electronics retailer in

[6] Ellie Fry, *Inside chilling rise of AirTag stalking as Apple device is branded 'gift to abusers'*, The Mirror (Apr. 24, 2023) (available at https://www.mirror.co.uk/tech/inside-chilling-rise-airtag-stalking-29746435)

America. AirTag changed all that. A person stalked with an AirTag forever lives with the constant fear that the stalker has hidden additional undiscovered AirTags among their belongings or will attempt to do so again in the future.

35. And this fear necessarily leads to another: what will happen if one's stalker acts on this new information, showing up unannounced and unwanted with ill intent? What are the possible outcomes of being tracked without your knowledge or consent? The outcomes can be devastating.

36. Apple's acts and practices, as detailed further herein, amount to negligence, strict product liability, intrusion upon seclusion, and unjust enrichment. Plaintiff seeks 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. Plaintiff also seeks damages.

A. Apple AirTags, Generally

37. 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.[7]



Fig. 2

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



Fig. 3

38. 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.[8] 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.*

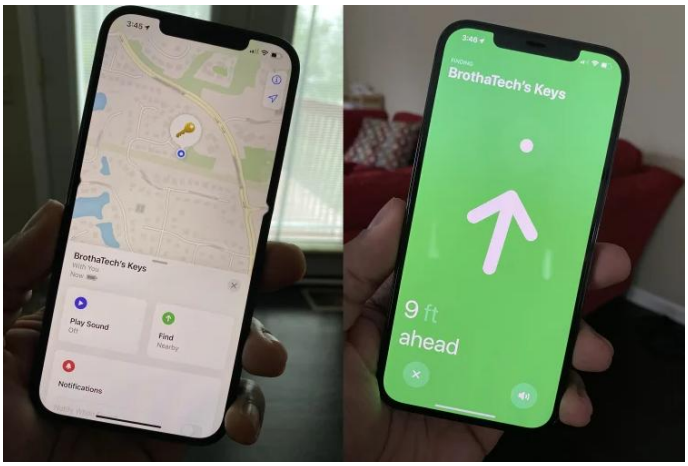


Fig. 4

[8] 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)

39. 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.[9] This network is vast: as of 2017, 64% of Americans owned an Apple product.[10]

40. 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."[11]

41. 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."[12]

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

42. 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.

---

[9] 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/)

[10] 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)

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

[12] "*Are Apple AirTags Being Used to Track People and Steal Cars?*" note 8, *supra*.

43. 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."[13]

44. 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."[14]

45. 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.

---

[13] 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)

[14] *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.[15]

46. Eva Galperin expressed her concerns even before the product's launch: "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."[16]

47. More recently, an advocate for the Cyber Helpline—a UK-based advocacy network for victims of online abuse—decried Apple's *post-hoc* safety measures as follows: "*You wouldn't*

---

[15] 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/)

[16] 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).

allow a car to come to mass-market without having vigorous testing, so why are we allowing smart tech to just be released and then fixing safety features later?"[17]

48. 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 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.[18]

C. Apple Affirmatively Sought to Dismiss and Minimize Concerns About the Threats Surrounding AirTags.

49. 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[19] touting the safety of the product.

---

[17] Ellie Fry, *Inside chilling rise of AirTag stalking as Apple device is branded 'gift to abusers'*, The Mirror (Apr. 24, 2023) (available at https://www.mirror.co.uk/tech/inside-chilling-rise-airtag-stalking-29746435)

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

[19] 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.



Fig. 5 20



Fig. 6 [21]

[20] 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/)

[21] 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)



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. 7 [22]



HOME > TECH NEWS

Apple Says AirTags Are Stalker-Proof, Not For Tracking Kids and Pets

An Apple executive spoke about what AirTags are meant to be used for.

BY DAVE LECLAIR
PUBLISHED APR 22, 2021

Fig. 8 [23]

[22] "*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/)
[23] 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/)

50. 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.

51. Despite these public assurances, internally Apple's executives were debating how to respond to negative press and whether critical information relevant to the AirTag should even be disclosed to the public.

52. On launch of AirTag, Apple would not inform victims of unwanted tracking until at least 3 continuous days of tracking, and even then, those alerts were only provided to victims who already happened to be Apple customers via their iOS devices. Less than four months after the AirTag's release, Apple shortened the alert period to provide alerts no sooner than 8-24 hours—a period still inadequate to warn victims that they were being stalked, for example, from a public place to where they lived, revealing their home address to the stalker before the victim receives any notice that someone can see their location.

53. 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

54. 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. A

> *New York Times* reporter successfully used them to track her husband's every move (for a story).[24]

55. 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."[25]

56. 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[.][26]

---

[24] 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)

[25] "*Are Apple AirTags Being Used to Track People and Steal Cars?*" note 8, *supra*.

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

57. As December 2022, stalking incidents had been reported in New York,[27] California,[28] Pennsylvania,[29] Mississippi,[30] and even at Disney World,[31] as well as one woman reporting a harrowing experience in Paris following a flight from the US.[32]

58. Since that time, an explosion of reporting has occurred—in just one metropolitan area (Tulsa, Oklahoma), police have investigated 19 cases involving AirTags, with many ending in violence. In one case, the stalker followed a woman to an Airbnb and punched her. Another report says a man used an AirTag to track his former partner to set her car on fire. And in another case, a woman found her boyfriend's ex and punched her in the face.[33]

59. Moreover, international incidents of stalking have spiked, with reports of malicious AirTag use in, *inter alia*, the United Kingdom[34] and India.[35]

---

[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)
[28] "*Are Apple AirTags Being Used to Track People and Steal Cars?*" note 8, *supra*.
[29] 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/)
[30] "*AirTags Are A Growing Headache For Apple Amid Disturbing Reports Of Tracking*," note 27, *supra*.
[31] 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/)
[32] 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/)
[33] Janna Clark, *'That's terrifying,' FOX23 investigates cases of AirTag stalking in Tulsa*, Fox 23 (May 15, 2023) (available at https://www.fox23.com/news/fox23-investigates/thats-terrifying-fox23-investigates-cases-of-airtag-stalking-in-tulsa/article_e7239350-f360-11ed-bf48-17a67258bf06.html)
[34] Ellie Fry, *Inside chilling rise of AirTag stalking as Apple device is branded 'gift to abusers'*, The Mirror (Apr. 24, 2023) (available at https://www.mirror.co.uk/tech/inside-chilling-rise-airtag-stalking-29746435)
[35] Ankita Chakravarti, *Ex-partner uses Apple AirTag to stalk Ahmedabad woman, device found hidden under driver's seat*, India Today (Sep. 5, 2023) (available at https://www.indiatoday.in/technology/news/story/ex-partner-uses-apple-airtag-to-stalk-ahmedabad-woman-device-found-hidden-under-drivers-seat-2430063-2023-09-02)

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

61. 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.[36]

62. 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.[37]

63. In July of 2023, a woman in Chicago was murdered by her estranged boyfriend after removing an AirTag that he'd secretly placed in her car.[38]

64. AirTag tracking has even led to murder when the AirTag's owner is simply trying to track down stolen property. For example, a Texas man shot and killed a suspected car thief, after following his stolen truck via an AirTag placed within the vehicle.[39] And a woman in California was killed after using an AirTag to track down her stolen car and confront the thieves.[40]

65. All of the above instances—while harrowing—do not come close to exposing the true scope of AirTag stalking. As noted above, from April 20th, 2021 to April 5th, 2024, Apple

---

[36] *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)

[37] 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)

[38] CBS Chicago Team, *Man killed girlfriend after she removed AirTag he'd secretly placed in her car, prosecutors say*, CBS Chicago (July 14, 2023) (available at https://www.cbsnews.com/chicago/news/armoni-henry-charged-murder-jailene-flowers-marianos-evergreen-park/)

[39] Aaron McDade, *A Texas man used an Apple AirTag to track down his stolen truck and shoot and kill the suspected thief, police say*, Business Insider (Mar. 30, 2023) (available at https://www.businessinsider.com/texas-man-airtag-finds-stolen-truck-shoots-kills-suspected-thief-2023-3).

[40] *Woman shot, killed after tracking stolen vehicle with Apple AirTag*, Carolina Coast Online (Jun. 22, 2023) (available at https://www.carolinacoastonline.com/national/article_b0f7e0e2-1142-11ee-8773-fb021ce53b76.html)

received over 40,000 stalking reports, over 1,000 complaints per month on average. Since this number includes only reports made to Apple that it catalogued—and does not include the last two years of reports—the estimate likely dramatically undercounts the actual number of unwanted tracking incidents.

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

66. Apple does not view AirTag stalking as an engineering or business failure; rather, it views people being hunted as a press problem. An email to Tim Cook, sent only weeks after the AirTag's release, bemoaned a Washington Post article on the AirTag, which declared it "a new means of inexpensive, effective stalking," but rather than take the reporter's concerns to heart, the email ends on the following note: "At this time, we are not seeing this narrative gain steam in media or on social but we are carefully monitoring as media continue to review AirTag around the world."

67. While Apple was publicly claiming that AirTag-related stalking incident were rare, its internal data showed that Apple itself received over 40,000 unwanted tracking reports during the initial three-year period following AirTag's release (ending April 2024). Apple also knew that the vast majority of law enforcement complaints it received concerned stalking—nearly twenty times as many policy inquiries as any other crime.

68. Given that Apple's main concern with reports of AirTag stalking were related to public perception rather than the safety of victims, Apple spent the years following the AirTag's release scrambling to push through a series of half-measures and ad hoc security features to nominally shore up unwanted tracking protections so that it could present the appearance of action. However, Apple's own internal documents acknowledge that its safeguards would only "deter as opposed to prevent malicious use."

69. Moreover, there long has been a gross imbalance between the protections available to iOS/Apple users, versus those available to individuals with Android devices—historically rendering Android users nearly defenseless to tracking/stalking using an AirTag.

Remedies for iOS Users (and Their Limitations)

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

71. **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 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. 9 [41]

72. 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

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

potential danger.[42] 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,"[43] but users have no control over this. As a report by an industry expert noted, "Apple estimates it takes between four and eight hours to send an alert, which could be a potentially fatal span of time."[44]

73. 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.[45]

74. Most critically, these alerts can only be triggered by Apple's algorithms. An individual with an iPhone cannot trigger a scan independently. This means that a stalked individual is at the mercy of Apple's operating system to determine whether or not an AirTag is moving with her. And, just because an alert has been shown once, it does not follow that the alert will show up

---

[42] "*AirTags Are Dangerous — Here's How Apple Could Fix Them,*" note 24, *supra*.
[43] "*Are Apple AirTags Being Used to Track People and Steal Cars?*" note 8, *supra*.
[44] 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)
[45] 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 *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 24, *supra*.

again, meaning that a stalked individual may have lost her chance to identify or locate the AirTag if she does not move fast enough.

Remedies for Android Users (and Their Limitations)

75. 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 historically have not had that protection, as their devices run on the Android operating system, which is outside of the control of Apple. For two years following the release of AirTags, Apple did not work in conjunction with Google to provide automated alerts when Android users are being stalked. Instead, only in May 2023 did the two companies announce that they would collaborate on providing anti-stalking measures across platforms. And it is only recently that these protections were rolled out for Android users.

76. Thus, for at least two-and-a-half years, individuals who did not own iPhones, iPads, or iPod Touches have been much more vulnerable to being tracked using an AirTag. Android mobile devices have a 41.9% market share in the United States,[46] meaning that almost half of America's population would not receive any notification if they were being stalked by an AirTag.

77. In late 2022, Apple released an app ("Tracker Detect") for Android devices, but it was inadequate for multiple reasons.

78. *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,

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

worldwide.[47] Thus, virtually every Android phone user would be oblivious to being tracked by an AirTag.

79. *Second*, the app itself has been described as an example of Apple "fulfilling its obligations *to the least extent possible*."[48]

> 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.[49]

80. 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 had to 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.

81. Nor is this technology particularly helpful in densely populated areas, where myriad AirTags are likely to be present. Downloading Tracker Detect was fruitless for determining whether a specific AirTag was in the vicinity. All it could tell was that AirTags, in general, were nearby.

82. In May 2023, Google and Apple submitted a proposed industry specification to help address the disconnect between the (deficient) warnings that iOS users would receive and the (all-but-nonexistent) warnings that Android users would receive in the event of being stalked by an

---

[47] https://play.google.com/store/apps/details?id=com.apple.trackerdetect&hl=en_US&gl=US
[48] "*Apple has an AirTag Problem—here's how to solve it,"* note 44, *supra.*
[49] *Id*.

AirTag. Per a Google press release, the proposed specification "will allow Bluetooth location-tracking devices to be compatible with unauthorized tracking detection and alerts across Android and iOS platforms."[50]

83. Subsequently, at the end of July 2023, Google announced that devices running Android 6.0+ would begin receiving automatic alerts for unknown trackers—specifically, for AirTags tracking Android users.[51] Assuming this roll out occurs successfully, this presumably brings Android users up to parity with Apple users in terms of operating-system-level security, but does so roughly two-and-a-half years *after* the introduction of AirTags to the marketplace, and underscores the failures on Apple's part with regard to Android users up until late summer 2023.

84. Further, as the EFF has noted, Apple's commitments to this new specification are undergirded by a separate profit motive: the company has listed several patent disclosures that it claims apply to the new specification.[52] Per the EFF:

> That's a way of notifying competitors, and the public, that Apple believes it owns patents that cover the use of this technology. That means Apple could, in the future, choose to charge patent royalties to anyone using this technology, or file a patent infringement lawsuit against them.
>
> The decision to assert patents over this specification is unnecessary and unfortunate. The public will suffer a significant loss if Apple asserts that it has patent rights to what should be an open, free repository of information meant to help companies and everyday people prevent stalking and malicious tracking. Apple could

---

[50] Google Security Blog, *Google and Apple lead initiative for an industry specification to address unwanted tracking*, (May 2, 2023) (available at https://security.googleblog.com/2023/05/google-and-apple-lead-initiative-for.html)

[51] Google Blog, *3 ways unknown tracker alerts on Android help keep you safe*, (Jul. 27, 2023) (available at https://blog.google/products/android/unknown-tracker-alert-google-android/)

[52] Alexis Hancock and Eva Galperin, *The Industry Discussion About Standards For Bluetooth-Enabled Physical Trackers Is Finally Getting Started*, EFF.org (Aug. 14, 2023) (available at https://www.eff.org/deeplinks/2023/08/industry-discussion-about-standards-bluetooth-enabled-physical-trackers-finally)

> threaten or sue people who use agreed-upon technology to prevent unwanted tracking.
>
> Apple stands alone in its insistence that it may use intellectual property rights to threaten people with patent lawsuits, or demand fees, for using privacy-protecting technology. The IETF convening included Samsung, Google, Mozilla, and many other patent-owning entities, all of whom chose not to engage in this type of threatening behavior.
>
> Apple's decision to bring patent rights into this conversation is disappointing. The company should withdraw its patent disclosures and make a public statement that it won't make intellectual property claims against companies or users who don't want to be surreptitiously tracked.
>
> The technology required for Detecting Unwanted Location Trackers can, and should, be free to all.[53]

85. Apple's conduct thus disincentivizes other stakeholders from using this new specification to protect Android users from being stalked, and undermines the very efforts it claims are necessary to keep people safe.

86. Most frustrating of all, Apple did not have to wait for Google to provide an Android app that scanned for AirTags in the background. As early as March 2022, Google noted that *it already was possible for Apple's app to run in the background*.

> "Domestic violence advocacy groups have raised valid concerns about these products, and we encourage the manufacturers [*i.e.,* Apple] to update their apps to improve proactive scanning," said spokeswoman Kaori Miyake.[54]

87. Rather than fix this glaring infirmity immediately, Apple spokesman Alex Kirschner responded as follows:

---

[53] *Id*.

[54] Geoffrey A. Fowler, *Am I being tracked? Anti-stalking tech from Apple, Tile falls short.*, Washington Post (Mar. 31, 2022) (available at https://www.washingtonpost.com/technology/2022/03/31/airtags-stalking/)

> "We're committed to making improvements that continue to guard against unwanted tracking, and we are evaluating ways to make unwanted tracking features stronger for Android users. *Continuous background scanning with Tracker Detect on Android would negatively impact battery life and other features that use Bluetooth*. The most power-efficient way to enable this type of background scanning for AirTag is to implement it at the Android operating system level."[55]

88. Apple prioritizing battery life—or its patent rights—over safety is unconscionable. As is its insistence that Google bears responsibility to implement background scanning *for an Apple product* that was dangerously rushed to market. Apple could have made its product safer for all individuals, yet it chose not to, and allowed two and a half years to elapse until its competitor bridged the gap. Apple has shifted the burden of safety onto its rivals, with the added caveat that it may force them to pay—in the future—for this privilege.

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

89. **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.

90. However, the alert sound is roughly 60 decibels, which is approximately as loud as a normal conversation between two people, or background music.

91. 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

[55] *Id.*

make these days. It also stopped playing long before [the tester] was able to find it."[56] Ultimately, "[w]hether you hear the AirTag chime feels like a crapshoot."[57]

92. 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."[58]

93. 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."[59]

94. 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.[60] 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

---

[56] "*AirTags Are Dangerous — Here's How Apple Could Fix Them,*" note 24, *supra*.
[57] *Id*.
[58] *Id*.
[59] 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.)
[60] 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)

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*."[61]

95. 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.[62] Currently, there is no ability for a victim to remotely disable an AirTag, meaning that victims are faced with a dilemma of either potentially contaminating evidence, or continuing to have their location exposed to their stalker.

96. 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.[63]

97. A summary of the deficiencies of the various safety features is set forth in the following chart:

---

[61] 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)

[62] "*AirTags are being used to track people and cars. Here's what is being done about it*," note 16, *supra*.

[63] *Id.*

Safety Feature	Operating System	Deficiency
Unknown AirTag Screen Alerts	iOS	• **Alert is not immediate.** Originally, the alert would not be triggered until 72 hours. Presently, the time has been shortened to between 4 and 8 hours, but this is still too dangerous a wait time. • **Can be disabled inadvertently.** iPhone owners who disable "Location Services" in their phone settings (which is often done for separate, privacy-related reasons) will also be unable to receive Unknown AirTag Alerts, but this consequence is not explained to users. • **Cannot be triggered independently.** A common problem is that Apple's alert cannot be triggered by the tracked individual. Instead, it pops up at random. Thus, the tracked individual often cannot rely on Apple's alerts if she wishes to seek further help. Or at least, she only may do so if the alert randomly pops up again, in the presence of the person from whom the tracked individual is seeking help (law enforcement; mechanic; friend; etc.). • **Reliability.** The iOS AirTag detection software has reported problems regarding (1) consistency and (2) accuracy.
Sound Alerts	iOS and Android	• **Alert is not immediate.** See supra. • **Cannot be triggered independently.** See supra. • **Volume is insufficient.** The AirTag alert volume is, at maximum, 60 decibels. This is not loud enough to ensure that an individual is alerted, particularly if the AirTag is muffled due to being placed on the outside of an individual's car, within a purse, wrapped in a noise-cancelling fabric, etc. • **Sound is not distinct.** The AirTag chime is indistinguishable from the myriad other sound alerts that people's phones, computers, smartwatches, and the like emit on a constant basis. Nothing about the AirTag chime alerts individuals to the significance of its purpose and context. Many individuals where not aware of the significance of the AirTag sound alert upon hearing it. • **Duration.** The AirTag beep is not continuous and will stop before a targeted person can locate the AirTag.

		• **Can be disabled with ease.** As noted above, the AirTag remains functional even when the speaker has been disabled, which fact has been cognized by many would-be abusers, who have posted online tutorials on how to disable AirTag speakers for more effective stalking.
Disabling AirTags	iOS and Android	• **Physical possession of the AirTag is required.** If an individual wishes to disable an AirTag that is being used to stalk her, she must do so manually. This means that she needs to (1) find the AirTag, and (2) pop off the cover to remove the battery.[64] However, finding the AirTag is not always possible; or else it might require significant cost – for example, multiple people have been told by mechanics that their whole car would have to be stripped to look for the AirTag (a considerable cost). Further, physically dismantling the AirTag necessarily compromises evidence that would later needed in any law enforcement action.
AirTag Identifier Reset	iOS (and potentially Android)	• **Resetting identifiers also resets Apple's unknown tracker search logic.** Publicly available reporting,[65] indicates that an AirTag's identifier(s) automatically change at regular intervals, in order to be privacy protective of the owners. The problem, however, is that when those identifiers re-set, it appears to thwart Apple's "tracking alert logic."[66]
AirTag Firmware Updates	iOS (and potentially Android)	• **Relies on AirTag owners (i.e., stalkers) to implement.** Many of Apple's attempts to retroactively improve AirTag safety occur via updates of AirTag firmware. For example, firmware update 2.0.24 enabled a feature wherein iPhone owners who are being tracked could use a precision finding feature to locate an unwanted

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

[65] https://www.macworld.com/article/345863/how-to-find-block-disable-airtag-moving-with-you.html ("Another reason why you may not be able to find the AirTag is that it may have changed its identifier (which happens regularly). The Bluetooth ID produced by an AirTag, and by all Apple devices that participate in Find My crowdsourcing, changes on a regular basis to avoid becoming a reverse tracking item: if it were persistent, then someone could track your devices based on the "anonymous" Bluetooth ID. That means that your iPhone or iPad has to notice an AirTag moving with it over a relatively short period of time."

[66] *Id*.

		AirTag.[67] But such firmware updates do not happen automatically, or "over the air." Instead, they require the AirTag owners to implement the updates. In the stalking context, this means that these safety updates must be implemented by the very people who the updates are meant to thwart.
Tracker Detect App	Android	• **Low Awareness.** The Tracker Detect App is not bundled into Android operating systems or suite of apps that come with non-Apple manufacturers. In order to use this safety measure, individuals would have to know about it, in the first place, and then seek it out and download it. • **Does not run in the background.** Unlike Apple's iOS-specific alerts, Tracker Detect is not "always on," meaning that the user must independently trigger the scan. Thus, the app is only as effective as the user's intuition. • **Triggering sound alerts.** The Tracker Detect user must wait 10 minutes before having a "detected" AirTag emit a sound.[68] This is particularly important, as Tracker Detect does not allow for precision finding (i.e., the app does not guide the user towards the AirTag's location). Thus, the only way for a user of Tracker Detect to locate the AirTag is through triggering the sound.

F. At All Relevant Times, Alternative Feasible Designs Were Available, Which Could Have Made AirTags Safer

98. Apple's carelessness in designing, marketing, and releasing the AirTag with inadequate protections against stalking and unwanted tracking is magnified by the fact that alternative designs for the AirTag and its accompanying software were available that would have mitigated these risks with no substantial impairments to the AirTag's advertised, legitimate functions.

[67] https://support.apple.com/en-us/102183
[68] https://thebinaryhick.blog/2022/01/08/androids-airtags-oof/

99. In fact, Apple knew that several alternative designs and software changes were available, because Apple itself incorporated numerous software changes and design features following the AirTag's release, once it realized that its launch features were inadequate, due to well-publicized reports of AirTags being used for stalking and harassment.

100. For example, at release, an individual being tracked by an AirTag had to wait 3 days before receiving any alert. Apple later shortened this period to 8-24 hours of continuous tracking.

101. Apple could have launched the AirTag alongside an app for Android devices that would have provided alerts to individuals that did not possess iOS devices but were nonetheless vulnerable to unwanted tracking. Apple's post-release development and release of the TrackerDetect app shows that it was aware that leaving Android users vulnerable was a serious defect in the AirTag's safety feature. In fact, even the TrackerDetect app demonstrates a failure on Apple's part and the feasibility of a safer alternative design, given that subsequently, Apple partnered with Google and others to create an industry standard that would enable Android owners to receive alerts on their phones.

102. Additionally, Apple could have designed its unwanted tracking alerts so that dismissed alerts are stored and available for recalled viewing at an alternate time and location by victims. Instead, victims who received an alert and dismissed it, either through accident or confusion, were left with no option to view the alert again or follow the instructions Apple provided once the alert was tapped.

103. Apple could have designed a method whereby victims of unwanted tracking could remotely disable an AirTag in their vicinity once an alert had been received. Instead, victims are required to locate the AirTag and physically remove the device's battery before tracking can be

disabled. Individuals that cannot locate the AirTag, or who are concerned about potentially tampering with evidence, have no choice but to accept being tracked.

104. Apple could allow a victim who receives an alert to have a feature where that victim could "mute" their location for a time period, allowing the tracked individual to reach a safe location and identify the AirTag in question.

105. Apple could adjust its notifications so that an alert triggers a victim's location is being viewed by their stalker via an AirTag, rather than after 8 hours of continuous tracking.

106. Apple could adjust the AirTag's tracking features so that moment-by-moment tracking is available only for a limited period of time before being locked. A user that wished to have the feature unlocked would have to call Apple Support and provide a statement that includes their: (a) name; (b) phone number; (c) address; (d) Apple ID; (e) device serial number; and (f) the reason for requesting moment-to-moment tracking. Individuals with a legitimate use for the AirTag would be unlikely to run into this ceiling, while stalkers would be limited in their ability to track and harass victims without providing potentially incriminating evidence.

107. Alternatively, Apple could lock moment-to-moment AirTag tracking behind a subscription paywall, requiring a recurring fee and registration information from users who wanted more than occasional location updates. This would have limited the accessibility of AirTags as a tool for stalkers and provided law enforcement with suspect information in the event of stalking and unwanted tracking, while still preserving the device's advertised function.

108. Additionally, Apple could have designed the AirTag so that any attempts to tamper with its speakers would disable the device's tracking capabilities.

109. These alternative designs, some of which ultimately were adopted by Apple, show that the AirTag was and remains defectively designed, and Apple's decision to market and release the AirTag indicates a conscious disregard for the privacy and security of individuals like Plaintiff.

G. Victims of AirTag Stalking Have Little Meaningful Recourse in the Criminal Justice System, and These Victims Are Further Undermined by Apple's Disingenuous Statements About Its Commitments to Working With Law Enforcement.

110. 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,[69] 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.[70]

111. 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,

---

[69] 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).

[70] 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)

according to data from the Department of Justice's Bureau of Justice Statistics (BJS).[71] That number is believed to be much higher, however, as BJS statistics indicate just 40% of stalking cases are reported to police.[72] According to the Stalking Prevention, Awareness, and Resource Center (SPARC), one in six women and one in 17 men are stalking survivors. Roughly 15% of those individuals said the stalking forced them to move.[73] Yet, once reported to the police, only 8% of stalking perpetrators are arrested.[74]

112. This fact bears particular emphasis given that one of Apple's principal responses in the wake of the AirTags fallout has been that "[w]e have been actively working with law enforcement on all AirTag-related requests we've received….Apple can provide the paired account details in response to a subpoena or valid request from law enforcement. We have successfully partnered with them on cases where information we provided has been used to trace an AirTag back to the perpetrator, who was then apprehended and charged."[75] This statement is critically misleading for several reasons.

113. ***First***, as noted above, the number of stalkers who face criminal prosecution is shamefully low. This stems from the fact that stalking behavior is not criminalized in many jurisdictions meaning that no charges *could* be brought. Further, even when the stalking is punishable under state law, police are often disinterested in pursuing the matter further, meaning that no fulsome investigation—let alone an arrest—occurs. Apple seeks to hand its obligations off

---

[71] 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)
[72] *Id*.
[73] *Id*.
[74] *Id*.
[75] Apple, *An update on AirTag and unwanted tracking*, Apple.com (Feb. 10, 2022) (available at https://www.apple.com/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/)

to law enforcement, but this is a deeply flawed approach, given the uneven patchwork of criminal laws around the country.

114. News reports of AirTag stalking are replete with examples of victims either not filing reports or being rebuffed by police:

- "Kimberly Scroop, from California, says the police refused to take a report when she alerted them to an AirTag tracking her location. She claims officers even went as far to say that nothing illegal had occurred, despite stalking being a crime in the state of Arizona, where she tried to report the incident…. Kimberly went to the police station [after finding the AirTag] to report the device, hoping whoever might be tracking her could see that she was going straight to the authorities. When she showed the officers the screenshots of the map tracking her location, they had 'no idea what an AirTag was'…."They essentially told me, 'We don't know what the technology is, and if you don't know who it is, what do you expect us to do?' but I thought that was their job," she says.…"I explained again, and they wouldn't even let me go past the front desk. They wouldn't write my name down. Nothing."[76]
- "Back in Chicago, the police did take a report of Angelina's case, but she says officers were also unsure what an AirTag was, and didn't know what to file the crime as. Despite her managing to find the device, as well as the AirTag's serial number and partial phone number the device was registered to, Angelina says the

[76] Ellie Fry, *Inside chilling rise of AirTag stalking as Apple device is branded 'gift to abusers'*, The Mirror (Apr. 24, 2023) (available at https://www.mirror.co.uk/tech/inside-chilling-rise-airtag-stalking-29746435)

> cops told her there wasn't much they could do, but said a detective would follow up. She hasn't heard from them since."[77]

- "[S]ince Carney did not file a police report, for fear of retribution, she has not been able to find out for sure who is behind the rogue AirTag found in her bag."[78]

115. ***Second***, and more importantly, Apple does *not* provide fulsome sets of information in response to law enforcement requests, and instead engages in obfuscatory tactics that prevent disclosure of critical information.

116. It is not entirely clear why Apple would not—as a matter of course—provide identifying information as to the owner of an AirTag in response to a law enforcement subpoena, but the answer may lie in the guidance that Apple provides to law enforcement regarding its response protocols to requests for AirTag information:

> With a serial number, Apple may be able to provide the paired account details in response to a subpoena or greater legal process. *AirTag pairing history is available for a period up to 25 days*.[79]

117. Thus, in reality—and exclusively due to Apple's data retention policies vis-à-vis its product that has a known use-case for stalking—Apple can only provide useful information in a criminal investigation if (1) the AirTag at issue was paired within the past 25 days and (2) the subpoena or other valid request was received within that same window. This also assumes that the victim managed to locate and obtain possession of the AirTag, as the device's serial number is required in order to locate the data in the first place.

---

[77] *Id*.
[78] *AirTag stalking victims unconvinced by Apple fixes*, France 24 (Feb. 15, 2023) (available at https://www.france24.com/en/live-news/20230215-airtag-harassment-victims-unconvinced-by-apple-s-fixes)
[79] Apple, *Legal Process Guidelines* (available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf)

118. These limitations are crippling to a criminal investigation, not to mention an effective prosecution. Apple's statements about cooperation with law enforcement are deeply misleading.

119. As one reporter summarizes: "What all this shows is how such a relatively innocuous piece of technology can have massive unintended consequences, but *Apple's response to the privacy nightmare it's created has been slow and piecemeal. While the company touts that it will give up any information to law enforcement regarding tracking, Apple's strategy puts the onus on regular people to be aware of the technology and actively scan for it on their person*."[80]

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

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

121. 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.[81]

---

[80] Kyle Barr, *Apple Quietly Rolls Out New Updates That Could Prevent AirTag Stalking*, Gizmodo (Dec. 22, 2022) (available at https://gizmodo.com/apple-airtags-stalking-tracking-1849922603)

[81] 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)

122. 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."[82]

123. 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 taking to protect themselves from abusers. The release of this data could expose them to stigma, discrimination, physical violence, emotional distress, and other harms."[83]

124. 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."[84]

125. 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

---

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

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."[85]

126. 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 consumers or competition. This practice is an unfair act or practice [in violation of the FTC Act]"[86]

I. Plaintiff Rachel Fox's Experience With AirTags.

133. Plaintiff Rachel Fox was stalked via an AirTag for an unspecified period potentially lasting months or longer.

134. In or around late-August 2023, after returning home from a dinner with friends, she received a notification that an AirTag was tracking her location. The notification showed that she had been tracked at least from the restaurant to her home, meaning that her home's location was now exposed.

135. Following the prompts on her phone, she caused the AirTag to play sound, alerting her that the AirTag was in her vehicle, but after thoroughly searching her vehicle was unable to

---

[85] 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)

[86] *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.

locate the device. She immediately called the police. An officer responded and spent significant time searching her vehicle but also could not locate the AirTag.

136. Ms. Fox spent several days in a state of panic and anxiety. She frantically researched online how to locate the AirTag and remotely disable or deactivate it. She discovered during her research that it was not possible to remotely disable or deactivate an AirTag and that she needed to physically access the device to stop her stalker from tracking her.

137. Ms. Fox purchased an endoscopic camera and stethoscope to try to locate the AirTag within small spaces in her vehicle. She called in sick to work, and over the next three days, she spent approximately 8 hours of time searching the car before she eventually located the AirTag hidden in the foam within the driver's seat. At that time, she removed the battery to the device.

138. Ms. Fox notified the police, who attempted to obtain information from Apple concerning the owner. Apple, however, would not reveal the owner's identity to the police.

139. To this day, Ms. Fox has been unable to identify her stalker. She does not know whether her stalker is continuing to track her location and lives in fear that the tracking may still be ongoing. The stalker could not have placed the AirTag in the location within her seat while she was at the dinner the night she received the first alert. Ms. Fox believes that the device was concealed in her vehicle months before she received any alert. She is afraid that other AirTags could be hidden somewhere that would allow the stalker to track her without her being notified.

140. Following the discovery of the AirTag, Ms. Fox suffered from numerous panic attacks and other symptoms of severe harm as a result of the tracking. She has purchased a security camera to monitor her house.

CAUSES OF ACTION[87]

COUNT I
California Law
(Negligence)

141. Plaintiff repeats and realleges all preceding paragraphs contained herein.

142. Apple owed Plaintiff 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 Plaintiff's behavior through AirTags' access to Apple's vast network of mobile devices, which in turn are used to locate Plaintiff with unparalleled reach and precision. It is further supported by the surreptitious and non-intuitive nature of Defendant's tracking.

143. Furthermore, Apple's duty of care extends to Plaintiff because Apple put Plaintiff at an unreasonable risk of harm through the reasonably foreseeable actions of third-party stalkers. Apple's duty of care is cognizable because (1) the harm resulting from the malicious use of Apple's AirTags by third parties to stalk Plaintiff was foreseeable to Apple; (2) Plaintiff has suffered harm resulting from such stalking; (3) there is a logical causal connection between Apple's design, marketing, and introduction into the market of its AirTags and the intervening stalking that harmed Plaintiff; (4) there is moral blame attached to Apple's conduct in light of its efforts to minimize concerns about threats surrounding AirTags and its failure to cooperate with law enforcement in response to AirTag stalking; (5) the policy of preventing future harm, in the context of unwanted and unconsented location tracking, is enshrined in legislatively declared policy, including inter alia the Constitutional Right to Privacy (see California Constitution Article 1, Section 1) and Cal.

[87] Plaintiff asserts that California law applies to the entirety of Plaintiff's claims. In the alternative, Plaintiff asserts claims under Texas law.

Pen. Code § 630, et seq.; and (6) any burden on imposing such a duty on Apple is outweighed by compelling policy interests that will benefit the public by such imposition.

144. Apple breached its duty of care by rushing AirTags to market with insufficient safeguards to prohibit their use for stalking purposes.

145. This breach of duty on the part of Apple was the proximate or legal cause of injury suffered by Plaintiff. At minimum: (1) introducing a tracking device into the stream of commerce; (2) which Apple knew would create a risk of being purchased and used for stalking; and (3) which did result in that anticipated misuse plainly caused the harm suffered by Plaintiff. Regardless of whether or when Plaintiff became aware of the AirTag or AirTags tracking her, the AirTag, itself, was the sine qua non of her harm.

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

COUNT II
California Law
(Strict Liability – Design Defect – Risk-Benefit Test)

147. Plaintiff repeats and realleges all preceding paragraphs contained herein.

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

149. The AirTag was defectively designed.

150. Plaintiff was harmed as a result of the AirTag's design defect.

151. The AirTag's design defect was a substantial factor in causing Plaintiff's harm.

152. The benefits of Apple's AirTag design do not outweigh the risks of the design. 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 Plaintiff, and make clear that the risks associated with the AirTag outweigh the benefits.

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

COUNT III
California Law
(California Bus. and Prof. Code § 17200, *et seq.* – Unlawful Prong)

154. Plaintiff repeats and realleges all preceding paragraphs contained herein.

155. As set forth above, Apple's conduct amounts to acts of negligence and product liability. Each of these independent violations of law also serves as predicate violations of the UCL's unlawful prong.

156. Plaintiff has standing to pursue this claim as Plaintiff suffered injury in fact and has lost money or property as a result of Apple's actions as set forth herein. Specifically, as a result of being stalked, and in an effort to protect herself from further harm from her stalker that may be facilitated by the AirTag, Ms. Fox missed three days of work, purchased an endoscopic camera and stethoscope in order to locate the AirTag, and purchased a security camera to monitor her yard.

157. Pursuant to section 17203 of the UCL, Plaintiff seeks an order of this Court enjoining Apple from engaging in the unlawful business practices alleged herein in connection with the sale of AirTags.

COUNT IV
California Law
(California Bus. and Prof. Code § 17200, *et seq.* – Unfair Prong)

158. Plaintiff repeats and realleges all preceding paragraphs contained herein.

159. 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.

160. Apple's business practices are also unfair because they undermine public policy, which is tethered to specific statutory provisions, including but not limited to the California Invasion of Privacy Act (Cal. Pen. Code § 630, et seq.) and the California Constitutional Right to Privacy.

161. Further, 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.

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

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

164. As set forth in the above, which is fully incorporated herein, Plaintiff has standing to pursue this claim as Plaintiff suffered injury in fact and has lost money or property as a result of Apple's actions.

165. Pursuant to section 17203 of the UCL, Plaintiff seeks an order of this Court enjoining Apple from engaging in the unlawful business practices alleged herein in connection with the sale of AirTags.

COUNT V
Texas Law
(Negligence)

166. Plaintiff repeats and realleges all preceding paragraphs contained herein.

167. Apple owed Plaintiff a duty of reasonable care in its design, marketing, and introduction into the market of its AirTags. Under Texas law, the existence of a duty depends primarily on the foreseeability of the Plaintiff's injury. *Greater Houston Transp. Co. v. Phillips*, 801 S.W.2d 523, 525 (Tex. 1990) ("Of all these factors, foreseeability of the risk is the foremost and dominant consideration.'").

168. As discussed above, Apple's course of action in designing, marketing, and rushing AirTags to market without adequate safety features; without the safety features Apple itself determined were needed to protect people from unwanted tracking; and without the safety features it represented to the public were present for AirTag created a foreseeable risk of injury of the type Plaintiff suffered here. Apple absolutely knew, prior to releasing AirTags into the market, that third parties would use its product to illegally track and stalk people. But, instead of developing its safety features more robustly, Apple released AirTags with safety features it knew were inadequate and underdeveloped. As a result, Apple increased Plaintiff's risk of harm and had a duty to protect Plaintiff from the risk of harm it created.

169. Additionally, the risk and likelihood of injury weighed against the social utility of the actor's conduct, the magnitude of the burden of guarding against the injury, and the consequences of placing the burden on Apple.

170. Apple is the party who designed, controls, and sells for profit the technology that collects and shares the precise physical locations of non-consenting and/or unaware humans to any third party who purchases the product and plants it on someone's person or vehicle. The duty is also evidenced by the surreptitious and non-intuitive nature of AirTag tracking and Apple's unique and unparalleled ability to monitor Plaintiff's and third-party stalker behavior through AirTags' access to Apple's vast network of mobile devices.

171. Apple's duty of care is further supported by the fact that the harm was extremely likely, if not virtually certain, to occur; because the magnitude of the burden to guard against the foreseeable injury is most feasible with respect to Apple as the party who designed and controls the products and networks enabling AirTags and as the party who profits from the sale of AirTags; and because public and legislative policy considerations (including the reasonable expectations of parties and society) favor placing the burden on Apple.

172. The legislative policy of Texas further supports that Apple has a duty to protect individuals from unauthorized electronic surveillance of their persons, movements, and private affairs: Under Texas Penal Code § 16.06, it is a criminal offense if one "knowingly installs an electronic or mechanical tracking device on a motor vehicle owned or leased by another person." In addition, the Texas Constitution further guarantees the sanctity of the home and person from unreasonable privacy intrusion. *E.g., Vaughn v. Drennon*, 202 S.W.3d 308, 320 (Tex. App. 2006). Apple manufactured and placed into commerce small, highly affordable, tracking devices with inadequate safeguards against unauthorized use for precisely the purposes these enactments were

designed to prevent. Apple did so with knowledge, alleged and detailed above, that its product would be used to commit the very conduct criminalized by statute (in Texas and more broadly across the U.S.). A manufacturer in Apple's position has a duty under Texas public policy to take reasonable steps to protect the class of persons these statutes were designed to protect.

173. Apple further owed Plaintiff a duty of care arising from its voluntary undertaking in designing, marketing, and deploying the inadequate safeguards associated with AirTags. Under Texas law, "one who voluntarily undertakes an affirmative course of action for the benefit of another has a duty to exercise reasonable care that the other's person or property will not be injured thereby." *Dukes v. Philip Johnson/Alan Ritchie, Architects, P.C.*, 252 S.W.3d 586, 597 (Tex. App. 2008). Apple did not merely manufacture a product, but affirmatively undertook to design and deploy a compact, low-cost, location-tracking device equipped with safeguards that it represented to the public as protective against stalking and other misuse. By voluntarily implementing those safeguards, Apple assumed a duty to perform that undertaking with reasonable care, and Apple's failure to exercise such care increased Plaintiff's risk of harm being stalked by an AirTag.

174. Apple breached its duty of care by rushing AirTags to market with inadequate safeguards to prevent their use for stalking purposes.

175. This breach of duty by Apple was the proximate cause of Plaintiff's injury because: (i) Apple's conduct in rushing its AirTags to market without adequate safety features was a substantial factor in causing Plaintiff's injury and without it, Plaintiff's injury would not have occurred; and (ii) Plaintiff's injury was the natural, foreseeable, and probable consequence of Apple's conduct in rushing its AirTags to market without adequate safety features. At minimum, Apple introduced its tracking device into the stream of commerce; Apple knew third parties would inevitably purchase and use the tracking device for stalking and could have but did not develop

adequate safety features; and that anticipated misuse did, in fact, occur and caused the harm suffered by Plaintiff.

176. Apple's breach of duty is further apparent because Apple created and sold an electronic tracking device which it knew would be installed on a motor vehicle owned or leased by another person. See Texas Penal Code § 16.06.

177. The intervening acts of third-party stalkers do not relieve Apple of liability because they were a foreseeable (and foreseen) result of Apple's negligence. *E.g., Boggs v. Bottomless Pit Cooking Team*, 25 S.W.3d 818, 823-824 (Tex. App. 2000) ("when the third party's criminal conduct is a foreseeable result of the prior negligence, the criminal act does not excuse the previous tortfeasor's liability.").

178. The stalking conduct here was foreseeable. It was the precise risk Apple's design enabled and against which Apple could have but knowingly failed to guard against. Where a defendant's conduct increases the foreseeable risk of harm through the actions of a third party, the defendant remains liable for that harm.

179. As a direct and proximate result of Apple's negligence, Plaintiff suffered actual damages, including costs associated with missing 3 days of work; materials purchased to search for the AirTag; additional purchases to secure her home; medical expenses; mental suffering; depression; loss of enjoyment of life; anxiety; fear; and severe emotional distress.

180. Plaintiff further seeks punitive damages in an amount to be determined at trial because Apple's actions constituted gross negligence because Apple's conduct created a significant risk of serious injury to Plaintiff and because Apple was actually aware of that risk and able to mitigate it but did not do so. Punitive damages are warranted to deter Apple from engaging in future misconduct.

COUNT VI
Texas Law
(Strict Liability – Design Defect – Risk-Benefit Test)

181. Plaintiff repeats and realleges all preceding paragraphs contained herein.

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

183. To recover for a products liability claim alleging a design defect under Texas law, a plaintiff must prove that: (1) the product was defectively designed so as to render it unreasonably dangerous; (2) a safer alternative design existed; and (3) the defect was a producing cause of the injury for which the plaintiff seeks recovery. *Timpte Indus. v. Gish*, 286 S.W.3d 306, 311 (Tex. 2009).

184. Apple's AirTags were defectively designed so as to be unreasonably dangerous because each of the following factors favors Plaintiff:

a. the utility of the AirTag to the user and to the public as a whole weighed against the gravity and likelihood of injury from its use;

b. the availability of a substitute product which would meet the same need and not be unsafe or unreasonably expensive;

c. Apple's ability to eliminate the unsafe character of the product without seriously impairing its usefulness or significantly increasing its costs;

d. the user's anticipated awareness of the dangers inherent in the product and their avoidability because of general public knowledge of the obvious condition of the product, or of the existence of suitable warnings or instructions; and

e. the expectations of the ordinary consumer. *Id.*

185. As detailed above, a safer alternative design existed at the time Apple began selling its unreasonably dangerous AirTags with insufficient safety features.

186. The AirTag's design defect was the producing cause of Plaintiff's injury because it was a substantial factor in bringing about Plaintiff's injury and Plaintiff's injury would not have occurred if Apple's defective and unreasonably dangerous AirTag had not been released into the market. *BIC Pen Corp. v. Carter*, 346 S.W.3d 533, 541 (Tex. 2011).

187. As a direct and proximate result of Apple's negligence, Plaintiff suffered actual damages, including costs associated with missing 3 days of work; materials purchased to search for the AirTag; additional purchases to secure her home; medical expenses; mental suffering; depression; loss of enjoyment of life; anxiety; fear; and severe emotional distress.

188. Plaintiff further seeks punitive damages in an amount to be determined at trial because Apple's actions constituted gross negligence, because Apple's conduct created a significant risk of serious injury to Plaintiff, and because Apple was actually aware of that risk and able to mitigate it but did not do so. Punitive damages are warranted to deter Apple from engaging in future misconduct.

COUNT VII
Texas Law
(Intrusion upon Seclusion)

189. Plaintiff repeats and realleges all preceding paragraphs contained herein.

190. Apple intentionally intruded on and into Plaintiff's solitude, seclusion, and private affairs by intentionally geolocating Plaintiff.

191. Apple committed an unauthorized intrusion or prying into the Plaintiff's seclusion by creating a product which could (and did) track, store, and constantly transmit Plaintiff's precise physical location to anyone who purchased and planted an AirTag on Plaintiff's person or vehicle.

192. The matter intruded on—Plaintiff's constant, precise physical location—was private, and the intrusion was unreasonable, unjustified, and unwarranted.

193. Plaintiff had a reasonable expectation of privacy in her constant, precise, physical location.

194. This sort of intrusion—transmitting one's constant, precise physical location to known or unknown third parties without one's knowledge or consent—would be highly offensive and objectionable to a reasonable person, and likely to cause mental suffering. This is evidenced by, inter alia, Supreme Court precedent (most recently and forcefully articulated in *Carpenter v. United States*), 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.

195. As a direct and proximate result of Apple's negligence, Plaintiff suffered actual damages, including costs associated with missing 3 days of work; materials purchased to search for the AirTag; additional purchases to secure her home; medical expenses; mental suffering; depression; loss of enjoyment of life; anxiety; fear; and severe emotional distress.

196. Plaintiff further seeks punitive damages in an amount to be determined at trial because Apple's actions constituted gross negligence, because Apple's conduct created a significant risk of serious injury to Plaintiff, and because Apple was actually aware of that risk and able to mitigate it but did not do so. Punitive damages are warranted to deter Apple from engaging in future misconduct.

COUNT VIII
Texas Law
(Unjust Enrichment)

197. Plaintiff repeats and realleges all preceding paragraphs contained herein.

198. Apple should not have released AirTags into the stream of commerce because of its known susceptibility to the dangers and risks detailed herein, including that it could easily be used by third parties to track people without knowledge or consent.

199. Apple's conduct was wrongful in that it could have developed more robust safety mechanisms to prevent unwanted tracking that it knew was virtually certain to occur. Instead, Apple rushed its AirTags to market without adequate safety features, putting profits above known and material safety risks. Thus, Apple received financial benefits in the form of the money it avoided spending to develop more robust safety features and in the form of increased profits resulting from added time the product was available for purchase on the market. If Apple has behaved as it should have, it would have expended much more money and resources developing more robust safety features and the AirTag would not have been available on the market as early or as long as it was.

200. As a direct and proximate result of Apple's design, manufacture, and sale of the AirTag, Apple received a benefit to Plaintiff's detriment—through the sale of Plaintiff's precise, constant, physical location data—which is unjust for it to retain.

201. Apple was aware of the benefit it would receive in rushing AirTags to market with insufficient safety features.

202. Under the circumstances, Apple's retention of the benefit violates fundamental principles of justice, equity, and good conscience because Apple procured the benefit through wrongful conduct.

203. Apple has been unjustly enriched. Plaintiff has a right to restitution in an amount to be proven at trial.

RELIEF REQUESTED

Plaintiff requests the Court to enter judgment against Defendant, and accordingly, requests the following:

a. That judgment be entered against Defendant and in favor of Plaintiff 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 or unfair practices with respect to the design, manufacture, and release into the market of its AirTags;

c. That Plaintiff be awarded all damages and punitive damages, in an amount to be determined at trial;

d. All other such other relief as the Court may deem appropriate.

Dated: August 17, 2026

Respectfully submitted,

/s/Justin S. Abbarno

Justin S. Abbarno (24127438)
Mark A. DiCello *
Robert F. DiCello *
Kenneth P. Abbarno *
Mark M. Abramowitz *
DICELLO LEVITT LLP
8160 Norton Parkway Third Floor
Mentor, Ohio 44060
P: (440) 953-8888
F: (440) 953-9138
jabbarno@dicellolevitt.com
madicello@dicellolevitt.com
rfdicello@dicellolevitt.com
kabbarno@dicellolevitt.com
mabramowitz@dicellolevitt.com

Greg G. Gutzler *
DICELLO LEVITT LLP
485 Lexington Avenue
Suite 1001
New York, New York 10017 P: (646) 933-1000
F: (440) 953-9138
ggutzler@dicellolevitt.com

Scott Gilmore *
DICELLO LEVITT LLP
801 17th Street Northwest Number 430
Washington, D.C. 20006
P: (202) 975-2288
F: (440) 953-9138
sgilmore@dicellolevitt.com

Edwin J. Kilpela, Jr.*
WADE KILPELA SLADE LLP
6425 Living Pl. Suite 200
Pittsburgh, PA 15206
Telephone: (501) 417-6445
ek@waykayslay.com

Attorneys for Plaintiff Rachel Fox

JS 44 (Rev. 03/24)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

RACHEL FOX

(b) County of Residence of First Listed Plaintiff Denton County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
DICELLO LEVITT LLP
8160 Norton Parkway, Third Floor, Mentor, Ohio 44060
P: (440) 953-8888

DEFENDANTS

APPLE, INC.

County of Residence of First Listed Defendant Santa Clara County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☒ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☒ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding | ☐ 2 Removed from State Court | ☐ 3 Remanded from Appellate Court | ☐ 4 Reinstated or Reopened | ☐ 5 Transferred from Another District *(specify)* | ☐ 6 Multidistrict Litigation - Transfer | ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332, et seq. (Product Liability)

Brief description of cause:
Negligence

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
Aug 17, 2026

SIGNATURE OF ATTORNEY OF RECORD
/s/ Justin S. Abbarno

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Eastern District of Texas

RACHEL FOX

Plaintiff(s)

v.

APPLE, INC.

Defendant(s)

Civil Action No. 4:26-cv-01083

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Apple, Inc.
c/o CT Corporation System
330 N Brand Blvd, Suite 700,
Glendale, CA 91203

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Justin S. Abbarno
DICELLO LEVITT LLP
8160 Norton Parkway Third Floor
Mentor, Ohio 44060

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 4:26-cv-01083

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: