Adam J. Zapala, Bar No. 245748
azapala@cpmlegal.com
Elizabeth T. Castillo, Bar No. 280502
ecastillo@cpmlegal.com
Lauren A. Devens, Bar No. 364511
ldevens@cpmlegal.com
COTCHETT, PITRE & MCCARTHY LLP
840 Malcolm Road
Burlingame, CA 94010

Korey A. Nelson*, Bar No. 30002
knelson@burnscharest.com
Amanda K. Klevorn*, Bar No. 35193
aklevorn@burnscharest.com
Lauren M. Perry*, Bar No. 40012
lperry@burnscharest.com
Rachel B. Hudson*, Bar No. 40827
rhudson@burnscharest.com
BURNS CHAREST LLP
201 Saint Charles Avenue
Suite 2900
New Orleans, LA 70170
Telephone: (504) 799-2845
Facsimile: (504) 881-1765

**pro hac vice applications forthcoming*

Attorneys for Plaintiff Toni Barnes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

TONI BARNES,

Plaintiff,

v.

APPLE, INCORPORATED,

Defendant.

Case No.: 26-cv-11591

COMPLAINT

JURY TRIAL DEMANDED

1. California Negligence
2. California Strict Products Liability – Design Defect (Risk-Benefit Test)
3. Violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*
4. Violation of California Business and Professions Code §§ 17200, *et seq.* (unlawful prong)
5. Violation of California Business and Professions Code §§ 17200, et seq. (unfair prong)

TABLE OF CONTENTS

TABLE OF CONTENTS I

INTRODUCTION 1

PARTIES 2

JURISDICTION AND VENUE 2

CHOICE OF LAW 2

FACTUAL ALLEGATIONS 5

I. The AirTag and the Find My Network 5

II. Apple knew the AirTag would be used as a tool for stalking. 6

III. Apple went so far as to tell the public that the AirTag was safe. 7

IV. Reports of people being stalked using AirTags began almost immediately after the AirTag was released. 8

V. Apple's touted "safeguards" are window dressing: these alleged safeguards do not meaningfully protect individuals from stalking. 8

A. Touted safeguards for iOS users are insufficient to protect against the AirTag's foreseeable harms. 9

B. Touted safeguards for Android users are insufficient to protect against the AirTag's foreseeable harms. 10

C. Touted safeguards independent of operating systems are insufficient to protect against the AirTag's foreseeable harms. 12

D. Apple could have implemented effective safeguards without compromising its product but chose not to. 13

E. Plaintiff Ms. Toni Barnes was harmed by Apple's AirTags. 15

CAUSES OF ACTION 16

RELIEF REQUESTED 20

JURY TRIAL DEMANDED 21

INTRODUCTION

1. This is a product liability action arising from Apple's design, manufacture, marketing, and sale of the AirTag, a coin-sized location tracker that Apple placed on the market in April 2021 knowing it could be hidden on a person and used to follow that person's movements without consent.

2. The AirTag is inexpensive, small enough to conceal almost anywhere, and connected to a location-reporting network built from hundreds of millions of Apple devices. Those features make it an effective tool for finding lost keys. The same features make it an effective tool for covertly tracking a human being.

3. Apple understood this before launch. Its own planning acknowledged that the safeguards it built into the AirTag were meant to "deter as opposed to prevent" malicious use. Apple nonetheless released the product with protections it knew would not stop a determined abuser.

4. The predictable result followed. Reports of AirTags hidden in purses, vehicles, and clothing began almost immediately. Between April 2021 and April 2024, Apple received more than 40,000 reports of unwanted tracking, an average of more than 1,000 per month.

5. Rather than fix the product before releasing it, Apple has spent the years since launch adding safety features piecemeal, often after public criticism. Each later change shows that a safer design was feasible all along. Many of the product's core safety deficiencies remain today.

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

7. Plaintiff was tracked without her knowledge or consent by means of an Apple AirTag. She brings this action to recover for the injuries that resulted and to require Apple to make its product reasonably safe.

PARTIES

8. Plaintiff Toni Barnes is a natural person and citizen of the State of Massachusetts.

9. Defendant Apple, Inc. is an American multinational technology company incorporated in California with its principal place of business in Cupertino, California. Apple is a citizen of California.

10. Apple generally oversees all aspects of the AirTag, including but not limited to its design, manufacture, marketing, and technical support and maintenance.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(a) because Plaintiff and Apple are citizens of different states and the amount in controversy exceeds $75,000, exclusive of interests and costs.

12. This Court has personal jurisdiction over Apple because it is a citizen of California and because it conducts in California substantial business from which the claims in this case arise.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Apple resides in this District and is the only defendant in this action.

CHOICE OF LAW

14. California law governs Plaintiff's claims.

15. Apple's choice-of-law provision in its Terms of Service applies to the claims of all owners of an iPhone, iPad, or iPod Touch.

16. Owners of those products must accept the terms of Apple's Software License Agreement (the "SLA") in order to use their devices.

17. All relevant versions of the SLA contain the following choice of law provision: "**12. Controlling Law and Severability.** This License will be governed by and construed in accordance with the laws of the State of California, excluding its conflict of law principles."

18. Apple's iOS Operating System—the use of which is governed by the SLA—is integral to Plaintiff's claims.

19. Moreover, as set forth in further detail below, AirTags 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, using the "FindMy" feature, which is a part of Apple's iOS software.

20. It is important to emphasize that "FindMy" is a part of the larger infrastructure of Apple's iOS operating system. It could not exist without iPhones (or other Apple devices such as iPads and iMacs) that run iOS. Each phone's hardware, software, and firmware are harnessed by Apple in order to create the FindMy network.

21. When multiple Apple devices are aggregated together, the network is created. Apple users access the FindMy network in order to locate lost items by using the FindMy app, which is one among a suite of Apple-designed apps that are bundled into iOS and are included on every iPhone.

22. Once an AirTag is identified as being near an Apple device or multiple Apple devices, these devices—including any Apple iPhone that Plaintiff owned or owns—act as crowdsourced beacons, pinging with the AirTag to locate it for the AirTag's owner.

23. Plaintiff, who owned Apple devices during the relevant time period, necessarily had those devices "pinged" by her stalker's AirTags, and said device(s) were instrumental in betraying Plaintiff's location.

24. Critically, it was the Apple software on Plaintiff's own phone—that is, the iOS software that is subject to the SLA that connected to the AirTag that was used to stalk Plaintiff. That same iOS software then transmitted the AirTag's location back to Plaintiff's stalker. Put another way: if the "FindMy" app on Plaintiff's phone (and the iPhones of others) did not exist, then AirTags would not work.

25. As Apple itself explains on its webpage devoted to the AirTag, AirTag owners "Get by with a little help from hundreds of millions of friends. When you've left something far behind, like at the beach or the gym, the Find My network—hundreds of millions of iPhone, iPad, and Mac devices around the world—helps track down your AirTag."

26. Plaintiff was, against her wishes, part of that network of "hundreds of millions of friends." Apple harnessed her devices (among others) in order to effectuate her stalking.

27. Moreover, while it is Plaintiff's contention that Apple's warnings to its users are insufficient, it also is beyond dispute that Apple's iOS software is what provides the brunt (if not all) of those warnings to owners of iOS devices.

28. Because Plaintiff's claims are intertwined with the functionality of the iOS operating system, California law applies.

29. Under California's choice-of-law rules, "[w]hether a nonresident plaintiff can assert a claim under California law is a constitutional question based on whether California has sufficiently significant contacts with the plaintiff's claims." *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1040 (N.D. Cal. 2014) (citation modified).

30. The claims here—asserted on behalf of Plaintiff whose claims are not otherwise governed by Apple's choice-of-law provision, discussed above—meets this "sufficiently significant contacts" test, given Apple's myriad contacts with the State of California, which include, among other things, the following:

a. Apple is headquartered in California;

b. At all times relevant to this litigation, Apple has conducted a significant portion of its business in California;

c. Apple's decision to create the AirTag and to release the product into the stream of commerce emanated from California;

d. Apple designed the AirTag in California (indeed, the statement "Designed by Apple in California" is etched into the product itself);

e. The principal designers of the AirTag are located in California;

f. Apple's press and marketing relating to the AirTag was conceived and emanates from California; and

g. The functionality of AirTag, itself, was designed by Apple employees in California.

31. Because of the contacts that Apple, generally, and AirTags, specifically, have with California, there are sufficient significant contacts with California to allow non-Californian

residents (including Plaintiff)—who do not otherwise have privity of contract with Apple and the choice-of-law provision in its iOS terms—to bring their claims under California law.

FACTUAL ALLEGATIONS

I. The AirTag and the Find My Network

32. Apple announced the AirTag on April 20, 2021. Apple's press release described it as "a small and elegantly designed accessory that helps keep track of and find the items that matter most with Apple's Find My app."

33. The AirTag is a disc roughly the diameter of a U.S. quarter. It weighs about 11 grams, runs for roughly a year on a replaceable coin-cell battery, and retails for approximately $29 individually or less per unit in multi-packs.

34. Its size, weight, and battery life allow the AirTag to be hidden in a bag, a coat lining, a vehicle's interior or exterior, or other personal belongings, where it can operate unattended for months.

35. The AirTag has no GPS receiver and no cellular or internet connection of its own. Instead, it broadcasts a Bluetooth Low Energy signal carrying a rotating identifier.

36. Any nearby Apple device participating in Apple's Find My network (iPhones, iPads, and Macs) detects that signal, determines its own location, and transmits an encrypted location report to Apple's servers. Apple then makes that location available to the AirTag's registered owner through the Find My app.

37. This happens automatically and in the background. The owners of the relaying devices are not told that their devices are reporting the location of someone else's AirTag, and they cannot stop their devices from doing so for a particular AirTag.

38. Apple advertises the scale of this network as the AirTag's key advantage, telling buyers they can "get by with a little help from hundreds of millions of friends" because "the Find My network—hundreds of millions of iPhone, iPad, and Mac devices around the world — helps track down your AirTag." Later reporting places the number of participating Apple devices worldwide in excess of two billion.

39. The Bluetooth range is roughly 30 feet. Because Apple devices are so widespread in the United States, an AirTag in almost any populated area will pass within range of a participating device frequently, often continuously. The result is near-real-time location reporting for any person carrying a hidden AirTag, at little cost to the person tracking them.

40. When the owner gets close to the AirTag, a compatible iPhone can use ultra-wideband "Precision Finding" to display the distance and an on-screen arrow pointing directly to the AirTag's location.

41. Security researchers recognized the significance of this design. Eva Galperin, Director of Cybersecurity at the Electronic Frontier Foundation, observed that Apple "automatically turned every iOS device into part of the network that AirTags use to report the location of an AirTag," making that network "larger and more powerful than that used by the other trackers" and therefore "more powerful for tracking and more dangerous for stalking."

42. These characteristics (low price, small size, long battery life, a vast passive reporting network, and seamless integration with the iPhone) distinguish the AirTag from competing trackers and make it uniquely suited to covert surveillance of a person.

43. Setting up an AirTag requires only an Apple ID and a compatible iPhone or iPad. Apple does not verify the purchaser's identity, does not ask how the device will be used, and does not limit the number of AirTags one account can register.

II. Apple knew the AirTag would be used as a tool for stalking.

44. The danger of covert tracking was obvious before the AirTag reached store shelves, and outside experts said so publicly within days of its announcement.

45. The National Network to End Domestic Violence ("NNEDV") warned that the period when a victim leaves an abuser is among the most dangerous, and that "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."

46. NNEDV also identified a flaw in Apple's safety model: it was built around a stranger slipping a tracker into someone's bag, not around "the person you come home to every day" (an intimate partner with access to the victim's belongings, vehicle, and routine).

47. On May 5, 2021, a Washington Post technology columnist reported that he had tested AirTags by having a colleague "stalk" him, concluding that AirTags were "a new means of inexpensive, effective stalking" and that "Apple's efforts to stop the misuse of its trackers just aren't sufficient."

48. On May 13, 2021, Wired published "Apple's AirTags Are A Gift to Stalkers," urging Apple to give abuse survivors and experts "a central place in its development process" and warning that "[w]hen Apple fails to protect survivors, the consequences can be fatal."

49. Eva Galperin later stated that she was "concerned ahead of their release as soon as I figured out how they worked," and that the mitigations in place at launch "were woefully insufficient."

50. Apple's own internal communications acknowledge that the company "should have consulted domestic abuse organizations on the unwanted tracking policy before shipping, and from these organizations' point of view, this is not a rare event."

51. Within weeks of launch, Apple's Chief Executive Officer was briefed on press coverage describing the AirTag as "a new means of inexpensive, effective stalking." Upon information and belief, Apple's response focused on managing the public narrative rather than on adding safeguards.

III. Apple went so far as to tell the public that the AirTag was safe.

52. Rather than address these concerns, Apple sought to dispel them. Around launch, Apple made senior personnel, including its Vice President of Worldwide iPhone Product Marketing and its Senior Director of Sensing and Connectivity, available for interviews promoting the AirTag's privacy and anti-stalking design.

53. The resulting coverage repeatedly described the AirTag as "stalker-proof."

54. These statements conveyed to the public, including people who would never buy an AirTag but could be tracked by one, that the product's built-in protections would prevent it from being used to stalk them. They would not, and Apple knew they would not.

55. Apple has also publicly described AirTag stalking as "rare." Apple's own data showed otherwise: Apple received over 40,000 unwanted-tracking reports in the three years after

launch, and the law-enforcement requests it received concerning AirTags involved stalking far more often (by some accounts nearly twenty times more often) than any other category of crime.

IV. Reports of people being stalked using AirTags began almost immediately after the AirTag was released.

56. Reports of AirTag stalking appeared within months of release and have continued since. AirTags have been found hidden in purses, coat pockets, vehicle wheel wells and bumpers, children's backpacks, and sewn into clothing linings.

57. By late 2021, the New York Times reported "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."

58. AirTag tracking has preceded serious violence, including homicides. Reported cases include a January 2022 shooting in Akron, Ohio, in which the killer had hidden an AirTag in the victim's car; a June 2022 killing in Indianapolis, Indiana, in which the perpetrator tracked the victim to a bar with an AirTag; and a July 2023 killing near Chicago, Illinois, of a woman who had removed an AirTag her estranged boyfriend had placed in her car.

59. One local police department alone (Tulsa, Oklahoma) reported investigating 19 AirTag cases by May 2023, many involving violence.

60. As noted, from April 2021 through April 2024 Apple received more than 40,000 reports of unwanted tracking. Because many victims never discover the device and many never report, that figure understates the true scope of the problem.

V. Apple's touted "safeguards" are window dressing: these alleged safeguards do not meaningfully protect individuals from stalking.

61. True, Apple built certain safeguards into the AirTag. But they fall far short of protecting the people being tracked. Apple's own internal documents concede that those safeguards were designed only to "deter as opposed to prevent malicious use."

62. The protections Apple has offered have also been sharply unequal. For years, people who carried Android devices had far fewer protections than iPhone users, leaving them nearly defenseless against tracking with an AirTag.

A. Touted safeguards for iOS users are insufficient to protect against the AirTag's foreseeable harms.

63. Apple's principal efforts to mitigate unwanted tracking are features built into its iOS operating system.

64. **Device-based notifications**. An iPhone, iPad, or iPod Touch running iOS 14.5 or later is programmed to display an alert when it detects an unknown AirTag moving with it. The alert reads: "AirTag Found Moving With You. The location of this AirTag can be seen by the owner."

65. The alert is not immediate. At launch, Apple's algorithm waited 72 hours before notifying anyone, meaning a person could be followed for three days before receiving any warning. Apple has since shortened the delay, and has estimated that an alert takes between four and eight hours, which is itself a potentially fatal window. Some people report receiving no alert after a full day of being tracked. According to Apple, timing varies with the device's operating system and location settings, factors the tracked person does not control.

66. And the alert reaches only people who carry a compatible Apple device running iOS 14.5 or later. People using older devices or older software receive no notification. The alert's option to make the AirTag play a sound has also proven unreliable: one reporter testing the feature described an AirTag "literally inches away" from the phone that "wouldn't connect" despite repeated attempts.

67. Most critically, the alert is triggered only by Apple's algorithm. A person cannot start a scan on her own, so she is entirely dependent on Apple's software to decide whether an AirTag is traveling with her. An alert that appears once may never appear again, so a person who misses or dismisses it may lose her only chance to identify and locate the AirTag.

68. A person who turns off Location Services, a common privacy step, also turns off unwanted-tracking alerts. Apple does not explain this consequence to users.

69. An AirTag's Bluetooth identifier changes at regular intervals to protect the owner's privacy. Upon information and belief, each change resets Apple's detection logic, which requires the person's device to notice the AirTag moving with it over a relatively short period, and thereby delays or defeats the alert.

B. Touted safeguards for Android users are insufficient to protect against the AirTag's foreseeable harms.

70. Android devices run on an operating system Apple does not control. For roughly two years after the AirTag's release, Apple did not work with Google to provide automatic alerts to Android users being tracked. Only in May 2023 did the two companies announce that they would collaborate on cross-platform protections.

71. Android devices hold roughly 40 percent of the U.S. mobile market. For more than two years, therefore, a large share of the American public would have received no notification at all if they were being tracked with an AirTag.

72. In December 2021, Apple released an Android app called "Tracker Detect." It was inadequate for several reasons.

73. First, the app is useful only to someone who already suspects she is being tracked and knows to look for it in the Google Play Store. Apple has done little to make Android users aware of the threat or of the app, which has been downloaded only about one million times worldwide. Most Android users being tracked would have no idea.

74. Second, the app does the bare minimum. It has been described as Apple "fulfilling its obligations to the least extent possible." It is essentially a single button that scans the surrounding area; it does not scan in the background or send push notifications.

75. That limitation can be deadly. iPhones scan for unknown AirTags continuously, but an Android user must deliberately open Tracker Detect and start each scan by hand, and the app does not scan again until she does. A person who does not know she is being tracked has no reason to decide when and where to scan.

76. Third, the app is of little help in crowded places, where many AirTags may be present. It reports only that AirTags are nearby, not whether a particular one is following the user. It offers no precision finding to guide the user to the device, and the user must wait about ten minutes before she can make a detected AirTag play a sound, which is the only way the app helps her find it.

77. In May 2023, Apple and Google proposed an industry specification to close the gap between the limited warnings iOS users received and the nearly nonexistent warnings Android users

received. Google described the proposal as allowing location trackers "to be compatible with unauthorized tracking detection and alerts across Android and iOS platforms."

78. In late July 2023, Google announced that Android devices running Android 6.0 or later would begin receiving automatic alerts for unknown trackers, including AirTags. That change came more than two years after the AirTag reached the market, and only through Google's effort.

79. Apple's participation in the specification also came with strings attached. Apple filed patent disclosures claiming rights over the specification, signaling that it could later seek royalties from, or sue, others who use the technology. The Electronic Frontier Foundation called the move "unnecessary and unfortunate," noted that Apple "stands alone" among participating companies in asserting such rights, and urged that the technology for detecting unwanted trackers "can, and should, be free to all."

80. Apple's assertion of patent rights discourages other companies from adopting the specification to protect Android users, undercutting the very protections Apple claims are needed.

81. Apple did not need to wait for Google at all. As early as March 2022, Google noted that Apple's app could already run in the background, and a Google spokeswoman stated: "Domestic violence advocacy groups have raised valid concerns about these products, and we encourage the manufacturers to update their apps to improve proactive scanning."

82. Apple declined. Its spokesman responded that "[c]ontinuous background scanning with Tracker Detect on Android would negatively impact battery life and other features that use Bluetooth," and that "[t]he most power-efficient way to enable this type of background scanning for AirTag is to implement it at the Android operating system level."

83. Apple thus placed battery life and its patent position ahead of the safety of people being tracked, and shifted responsibility for protecting Android users onto a competitor. Apple could have made the AirTag safer for everyone. It chose not to, and more than two years passed before a competitor filled the gap.

C. Touted safeguards independent of operating systems are insufficient to protect against the AirTag's foreseeable harms.

84. **Sound alerts.** Apple states that an AirTag separated from its owner for an extended time (between 8 and 24 hours, by Apple's account, and originally three days) will play a chime so it can be found.

85. The chime is roughly 60 decibels, about as loud as an ordinary conversation or background music.

86. The chime is not distinctive and is easily mistaken for the many other beeps electronic devices make. One reporter who tested it found that "the sound was easy to confuse with all the other beeps and boops gadgets make these days" and that it "stopped playing long before [the tester] was able to find it." The reporter concluded that "[w]hether you hear the AirTag chime feels like a crapshoot."

87. The chime is of even less use to a person who is hard of hearing or in a noisy setting, or when the AirTag is hidden where the sound will be muffled or out of earshot, such as the outside of a car. As one commentator put it: "If [an AirTag is] behind your license plate and you're driving, you're never going to hear that."

88. Many stalking victims who received an alert reported that they could not find the AirTag after searching, leaving them unsure whether it was still nearby.

89. The speaker can also be removed. Tutorials for disabling it are readily available online, and modified "silent AirTags" have been sold on mainstream sites such as eBay and Etsy. A silenced AirTag continues to track normally, and no software update can make a physically altered AirTag chime again.

90. **Disabling the AirTag.** Even a person who finds the AirTag must then decide what to do with it. The only way to stop it is to physically open it and remove the battery, which also alerts the AirTag's owner and, as law enforcement agencies have noted, may contaminate the device as evidence. Finding it is not always possible: some people have been told by mechanics that their car would need to be stripped to search for a hidden AirTag, at considerable cost.

91. Other responses carry their own risks. As the director of the Stalking Prevention Awareness and Resource Center has cautioned, if the stalker sees the AirTag arrive at a police station, "that can escalate the situation and put a victim more in danger."

92. **Firmware updates.** Many of Apple's after-the-fact safety improvements, such as the update allowing tracked iPhone users to use precision finding to locate an unwanted AirTag, are delivered through AirTag firmware updates. Those updates are not pushed automatically; they depend on the AirTag's owner. In the stalking context, the safety update therefore depends on the very person it is meant to stop.

93. **Identifying the person responsible.** Apple has stated that it can provide paired-account details to law enforcement in response to valid legal process. But Apple's own law-enforcement guidelines state that AirTag pairing history is retained for only up to 25 days, and a request requires the AirTag's serial number, which a victim can obtain only by finding the device.

94. Victims seeking evidence for civil protective orders face similar obstacles. Upon information and belief, Apple routinely deletes pairing data and often declines to respond to private subpoenas in such proceedings.

95. Apple has repeatedly announced additional safety changes since launch, including in February 2022 and again in 2024, confirming that its original safeguards were inadequate. Apple continues to sell the AirTag today with safeguards that remain inadequate to protect the public from covert tracking.

D. Apple could have implemented effective safeguards without compromising its product but chose not to.

96. At all relevant times, Apple could have designed the AirTag and its supporting software to substantially reduce the risk of covert tracking without materially impairing the product's legitimate purpose of locating lost items.

97. Apple's own post-launch changes prove feasibility. Apple shortened the alert and chime windows, built an Android app, enabled Precision Finding for tracked users, and helped develop a cross-platform detection standard. Each of these could have been in place at launch.

98. Feasible safer alternatives include, without limitation:

a. **Cross-platform protection at launch.** Releasing automatic, background unwanted-tracking alerts for Android users at the same time as for iPhone users.

b. **Faster alerts.** Notifying a person within minutes of an unknown AirTag traveling with them, or whenever the AirTag's owner views its location, rather than after hours of continuous tracking.

c. **On-demand scanning.** Letting any person manually scan for nearby AirTags from their phone at any time.

d. **Persistent alerts.** Storing unwanted-tracking alerts so a person who dismisses one can later review it and its instructions.

e. **Remote disabling and location muting.** Allowing a person who receives an alert to disable the AirTag remotely, or temporarily block it from reporting their location, without having to find it.

f. **Tamper-resistant alerts.** A louder, more distinctive, longer-playing chime, and a design that stops reporting location if the speaker is removed or disabled.

g. **Identity verification and accountability.** Requiring verified owner identity at setup, and retaining pairing records long enough for victims and law enforcement to use them.

h. **Limits on continuous tracking.** Restricting moment-to-moment location updates to a limited period unless the owner re-authenticates or provides identifying information, and limiting the number of AirTags that can follow the same non-owner device.

i. **Automatic safety updates.** Delivering safety-critical firmware updates without depending on action by the owner's device.

j. **Protection for people without smartphones.** Designing safeguards (such as a frequent, loud audible alert and public education on physical detection) that do not presuppose the victim carries a compatible smartphone.

99. None of these measures would prevent a person from finding their own lost keys or luggage. Each would make it materially harder to use the AirTag to secretly follow another person.

100. Apple had the engineering resources, technical capability, and knowledge to implement these alternatives before launch. It chose not to.

E. Plaintiff Ms. Toni Barnes was harmed by Apple's AirTags.

101. Plaintiff Barnes was formerly in a romantic relationship with an individual (hereinafter referred to as the "Former Partner") with whom she co-parents her five-year-old minor son.

102. At all relevant times, Plaintiff Barnes used an Apple iPhone.

103. Sometime before January 9, 2026, the Former Partner hid an Apple AirTag on or in the belongings of Plaintiff Barnes' son.

104. On or about January 9, 2026, Plaintiff Barnes was with her son at a local mall. The Former Partner used the AirTag to monitor her location and restrict her movements, telling her she could not leave the mall or take her son to her home.

105. The Former Partner told Plaintiff Barnes not to remove the AirTag's battery and that his tracking of her using the AirTag was legally authorized.

106. As a result, Plaintiff Barnes was subjected to constant surveillance during her parenting time.

107. A few days later, Plaintiff Barnes found an AirTag in her son's pocket and removed the battery.

108. On or about January 13, 2026, the Former Partner accused Plaintiff Barnes of removing the AirTag from her son's pocket and breaking it.

109. The Former Partner's accusations showed that he was actively monitoring the AirTag's status and location in real time.

110. The Former Partner sent Plaintiff Barnes text messages referring to the AirTag, blamed her for damaging it, and threatened legal action against her for damaging it.

111. The Former Partner sent Plaintiff Barnes screenshots of AirTag location data, showing that he was tracking her whereabouts.

112. Upon information and belief, the Former Partner used up to four separate AirTags to track Plaintiff Barnes. Upon information and belief, the Former Partner may have originally started stalking Plaintiff Barnes using AirTags as far back as the summer of 2025.

113. Plaintiff Barnes was able to locate and turn over two AirTags to local police, including an AirTag she found located in the left rear passenger door handle of her vehicle.

114. Plaintiff Barnes did not receive notifications on her iPhone about the AirTags. She located the AirTag in her vehicle because it was emitting a noise.

115. The AirTag tracking is part of a six-year pattern of stalking and control of Plaintiff Barnes by the Former Partner. Plaintiff Barnes is afraid of the Former Partner who has also used fake social media profiles to stalk her and once threatened her by chasing her with a knife. The Former Partner has a history of committing violent acts against others as well.

116. Plaintiff Barnes has suffered severe fear and emotional distress, including a worsening of her PTSD symptoms, as a result of the stalking by the Former partner using the AirTags.

117. When traveling with the AirTag, Plaintiff Barnes' whereabouts were transmitted to Apple.

118. Plaintiff Barnes had a reasonable expectation that her location would not be continuously monitored and reported to another person or company.

119. Upon information and belief, Plaintiff Barnes' own Apple device, running Apple's iOS software, detected the AirTag and relayed its location to Apple's servers. Apple then processed those location reports and delivered them to her stalker through the Find My app. Plaintiff Barnes' location was not merely discoverable by her stalker; it was collected, aggregated, and transmitted to him by Apple's systems and to Apple in the process.

CAUSES OF ACTION

COUNT I

Negligence

120. Plaintiff repeats and realleges each of the foregoing paragraphs as though fully set forth herein.

121. In designing, marketing, and introducing the AirTag into the market, Apple owed Plaintiff a duty to exercise reasonable care to guard against the device's foreseeable use as an instrument of stalking. That duty arises from Apple's singular capacity to locate individuals through its expansive network of Apple devices and from the covert, counter-intuitive manner in which AirTag tracking operates.

122. Apple breached that duty by bringing the AirTag to market with safety features inadequate to detect, deter, or defeat its use for stalking—including notification delays that permit tracking to continue undetected, alerts that fail to convey their meaning to ordinary users, the absence of any means for a target to scan for or disable an unknown AirTag without first locating and physically possessing it, and the capacity for a stalker to deploy multiple devices simultaneously.

123. Apple's breach was a proximate and legal cause of the injuries Plaintiff suffered.

124. As a direct and proximate result of Apple's conduct, Plaintiff seeks injunctive relief together with compensatory and punitive damages in an amount to be proven at trial. Punitive damages are warranted because Apple acted with malice, oppression, and a willful and conscious disregard for the rights and safety of Plaintiff and others foreseeably endangered by its product, and because such an award is necessary to deter Apple from persisting in the conduct alleged.

COUNT II

Strict Products Liability—Design Defect (Risk-Benefit Test)

125. Plaintiff repeats and realleges each of the foregoing paragraphs as though fully set forth herein.

126. Apple designs, manufactures, distributes, and sells the AirTag.

127. The AirTag was defectively designed, and its design defect was a substantial factor in causing Plaintiff's harm.

128. The risks inherent in the AirTag's design outweigh its benefits. Weighing the gravity of the harm the design enables (its ready use for stalking and other crimes), the likelihood that such harm will occur, the feasibility and cost of safer alternative designs available when the device was

manufactured, and the limited utility of the device relative to those risks, the balance weighs in Plaintiff's favor and establishes that the AirTag's risks outweigh its benefits.

129. As a direct and proximate result of Apple's conduct, Plaintiff seeks injunctive relief together with compensatory and punitive damages in an amount to be proven at trial. Punitive damages are warranted because Apple acted with malice, oppression, and a willful and conscious disregard for the rights and safety of Plaintiff and others foreseeably endangered by its product, and because such an award is necessary to deter Apple from persisting in the conduct alleged.

COUNT III

Violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, et seq.

130. Plaintiff repeats and realleges each of the foregoing paragraphs as though fully set forth herein.

131. The Legislature has declared that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communication and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

132. Section 637.7(a) prohibits the use of an electronic tracking device to determine the location or movement of a person. An "electronic tracking device" is "any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals." Cal. Penal Code § 637.7(d).

133. The AirTag is an "electronic tracking device" within the meaning of Section 637.7(d), and it was used to determine Plaintiff's location and movements in violation of Section 637.7(a).

134. Apple does more than place the AirTag into the stream of commerce. Through its Find My network, Apple itself determines the location of every AirTag; and through its unknown-tracker notifications, Apple associates particular AirTags with particular, identifiable individuals—

including by alerting Plaintiff that a specific device was traveling with her. Apple engaged in this conduct without Plaintiff's consent and despite having been warned, before and after the AirTag's release, that the device is a dangerous tool enabling stalkers and abusers.

135. As a result of Apple's violations of Section 637.7, and pursuant to Cal. Penal Code § 637.2, Plaintiff is entitled to: (1) a declaration that Apple's conduct violates CIPA; (2) statutory damages and/or trebled actual damages; (3) injunctive relief, including an order enjoining Apple from using AirTags to geolocate individuals in violation of CIPA; (4) injunctive relief, including an order requiring Apple to destroy all data created or obtained through its unlawful tracking of Plaintiff; and (5) an award of attorney's fees and costs of litigation as provided by CIPA, the private attorney general doctrine codified at Cal. Civ. Proc. Code § 1021.5, and all other applicable law.

COUNT IV

Violation of California Business and Professions Code § 17200, et seq.—Unlawful Prong

136. Plaintiff repeats and realleges each of the foregoing paragraphs as though fully set forth herein.

137. As alleged above, Apple's conduct violates California law, including CIPA, and constitutes negligence and product liability. Each of these independent violations serves as a predicate violation of the UCL's unlawful prong.

138. Plaintiff has standing to pursue this claim because she suffered injury in fact and lost money or property as a result of Apple's conduct, including the time and resources she expended locating and recovering the concealed AirTags and reporting them to law enforcement.

139. Pursuant to Section 17203, Plaintiff seeks restitution and an order enjoining Apple from engaging in the unlawful business practices alleged herein in connection with the sale of AirTags.

COUNT V

Violation of California Business and Professions Code § 17200, et seq.—Unfair Prong

140. Plaintiff repeats and realleges each of the foregoing paragraphs as though fully set forth herein.

141. Apple's business practices are unfair because its conduct in releasing the AirTag into the marketplace is immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers and to those foreseeably harmed by the device, and because the gravity of that harm is not outweighed by the utility of Apple's conduct.

142. Apple's business practices are also unfair because they undermine public policy tethered to specific statutory and constitutional provisions, including CIPA and the California constitutional right to privacy.

143. Apple's business practices are further unfair because the resulting injury is substantial, is not outweighed by any countervailing benefit to consumers or competition and could not reasonably have been avoided by those harmed.

144. Reasonable alternatives were available to further Apple's legitimate business interests without the conduct described above, and Apple's wrongful practices constitute a continuing course of unfair competition because Apple continues to sell AirTags.

145. Plaintiff has standing to pursue this claim because she suffered injury in fact and lost money or property as a result of Apple's conduct, including the time and resources she expended locating and recovering the concealed AirTags and reporting them to law enforcement.

146. Pursuant to Section 17203, Plaintiff seeks restitution and an order enjoining Apple from engaging in the unfair business practices alleged herein in connection with the sale of AirTags.

RELIEF REQUESTED

Plaintiff requests that the Court enter judgment against Defendant and grant the following relief:

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,

unfair, and/or fraudulent practices with respect to the design, manufacture, and release of its AirTags;

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

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

e. All other relief the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all triable issues.

Dated: October 07, 2026

Respectfully submitted,

/s/ Adam J. Zapala

Adam J. Zapala, Bar No. 245748
azapala@cpmlegal.com
Elizabeth T. Castillo, Bar No. 280502
ecastillo@cpmlegal.com
Lauren A. Devens, Bar No. 364511
ldevens@cpmlegal.com
COTCHETT, PITRE & MCCARTHY LLP
840 Malcolm Road
Burlingame, CA 94010

Korey A. Nelson*, Bar No. 30002
knelson@burnscharest.com
Amanda K. Klevorn*, Bar No. 35193
aklevorn@burnscharest.com
Lauren M. Perry*, Bar No. 40012
lperry@burnscharest.com
Rachel B. Hudson*, Bar No. 40827
rhudson@burnscharest.com
BURNS CHAREST LLP
201 Saint Charles Avenue
Suite 2900
New Orleans, LA 70170
Telephone: (504) 799-2845
Facsimile: (504) 881-1765

**pro hac vice applications are forthcoming*

Attorneys for Plaintiff Toni Barnes