PRIVACY FOR SALE: HOW THE FTC CAN TAKE PRECISE LOCATION DATA OFF THE MARKET

Andrea Hanus[*]

ABSTRACT

The Federal Trade Commission's ("FTC's") ability to protect consumers amidst the growing number of privacy invasions is at a crossroads. As consumer data is increasingly collected and commercialized, the question becomes whether the FTC's Section 5 enforcement authority is up to the challenge. A recent FTC complaint shed light on how the familiar issue of properly defining privacy harms impedes agency and lawmakers' abilities to protect consumers from privacy violations. And yet, the growing threat against personal autonomy and medical privacy has made the need for such protections more evident than ever. This Note will conceptualize the privacy harms caused by the sale of location data and argue that those harms are well within the FTC's Section 5 unfairness enforcement authority. It will conceptualize and define the privacy harms caused by the sale of location data by presenting examples of recent events in which data sales resulted in real-world harm. These harms will then be connected to precedent in various legal doctrines and FTC enforcement actions to argue that recognition of these less traditional harms is not really novel at all. All of which bolsters the claim that it is within the FTC's authority to enforce against these less traditional, but no less important, privacy harms. Arguably most importantly of all, this Note will suggest that an expanded definition of harm for FTC enforcement will not only protect consumers from sale of their location data, but will also protect against a much broader spectrum of privacy violations.

[*] J.D., Boston University School of Law, 2024; M.S., International Business, University of Delaware, 2021; B.A., International Relations & Public Policy, University of Delaware, 2020. Thank you to Professor Woodrow Hartzog, whose generous guidance greatly enriched this Note. Thank you to all the members of the *Boston University Law Review* for their immeasurable time and efforts. And finally, an expression of endless gratitude to my parents, Dan and Lisa Hanus, for their love and support, without which none of this would be possible.

CONTENTS

INTRODUCTION

The ever-growing presence of technology in the world has resulted in every person's actions, communications, decisions, and movements being translated into data points. The collection and sale of geolocation data, particularly, has the potential to cause massive harm. The location intelligence industry is currently estimated to be a $16 billion market and is expected to expand to a $51 billion market by 2030.[1] This little-monitored industry includes various players who collect, use, or sell location data. Most location data collection begins with the well-known request from an app for permission to access your location data, but most users are unaware that some of those apps are then selling that data to companies that aggregate it and sell it in bulk.[2] As this data collection invades every sector of life and privacy, its secrecy combined with its seeming inevitability result in the practice going unchecked.[3]

An inordinate amount of easily identifiable, precise location data on millions of Americans is being collected and sold on a massive scale and remains largely unregulated.[4] Moreover, the third-party purchasers of this sensitive data create additional, unknown harms in their use of the data. However, absent federal privacy legislation, it is important to ask how to protect people from the clear invasions of privacy that are occurring whenever they carry their phones in their pockets. The Federal Trade Commission ("FTC") is the answer, and it has already begun taking steps to enforce against this practice by recognizing the sale of location data as an unfair trade practice subject to its enforcement authority.[5] The FTC brought an action against Kochava, a location data broker, claiming that Kochava's practice of selling precise location data is unfair

[1] GRAND VIEW RSCH., LOCATION INTELLIGENCE MARKET SIZE, SHARE & TRENDS ANALYSIS REPORT BY VERTICAL (BFSI, IT & TELECOM), BY APPLICATION (REMOTE MONITORING, RISK MANAGEMENT), BY SERVICE (SYSTEM INTEGRATION, CONSULTING), AND SEGMENT FORECASTS, 2023-2030, at 35 (2022) (finding market recognition of location technology's ability to enhance customer experience, help businesses identify hidden patterns, and improve decision making will result in steadily increasing growth of location intelligence market, particularly in North America, due to "IT infrastructure, better connectivity, and rapid adoption of new technologies").

[2] Jon Keegan & Alfred Ng, *There's A Multibillion-Dollar Market for Your Phone's Location Data*, MARKUP (Sept. 30, 2021, 3:51 PM), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data [https://perma.cc/4CPF-KKT3] (noting location data is sold to investors, political campaigns, businesses, law enforcement agencies, and others).

[3] *See id.* ("[T]here few if any rules limiting who can buy your data.").

[4] *See id.* ("'There is virtually nothing in U.S. law preventing an American company from selling data on two million service members, let's say, to some Russian company that's just a front for the Russian government . . . .'").

[5] *See* Complaint for Permanent Injunction and Other Relief at 10, FTC v. Kochava Inc., No. 2:22-cv-377 (D. Idaho May 4, 2023) [hereinafter Kochava Complaint] (arguing Kochava's sale of access to its data feeds of precise geolocation data is unfair because such feeds can used to identify and track consumers to sensitive locations).

because of how it exposes consumers to harm.[6] However, Kochava argued that this enforcement deviates far beyond the FTC's authority to enforce against unfair trade practices and the harms alleged by the FTC are not substantially injurious to consumers.[7] While the FTC has jurisdiction to fill gaps as a de facto privacy regulator, challenges often arise against expansion of its enforcement to new and dangerous practices, including the sale of location data.[8] This Note will argue that, despite these challenges, the FTC's recent recognition that the sale of location data is unfair because of the substantial injury it causes to consumers is justified by its broad grant of power to protect consumers from harm and is actually not novel at all. And, notably, at the beginning of this year, the FTC entered into its first consent agreement with a location data broker—providing additional support for the FTC's expanded scope of authority in this realm.[9]

The capacity of the FTC to use its Section 5 power to enforce against unfair trade practices is determined primarily by the FTC itself.[10] However, at a minimum, federal law requires a showing of "substantial injury to consumers."[11] Thus, conceptualizing the harm done by selling a person's precise location data is the key to the FTC's ability to enforce against the practice and protect against this privacy violation. Yet, enforcement against privacy violations has traditionally been stalled by the difficulties in defining privacy harms. As Daniel

[6] *Id.* at 9 (conceptualizing substantial injury to consumers necessary for FTC enforcement as "exposure to stigma, discrimination, physical violence, emotional distress, and other harms . . . exacerbated by the fact that . . . Kochava lacks any meaningful controls over who accesses its location data feed").

[7] Memorandum in Support of Motion to Dismiss Pursuant to Fed. R. Civ. P. 12(b)(6) at 8-10, 16-17, FTC v. Kochava Inc., No. 2:22-cv-377 (D. Idaho filed Oct. 28, 2022) [hereinafter Kochava Motion to Dismiss] (emphasizing "unfairness must be grounded in a well-established legal policy" to reduce risk FTC enforcement will be applied in unexpected ways (internal quotations omitted)).

[8] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 590 (2014) [hereinafter Solove & Hartzog, *New Common Law of Privacy*].

[9] Decision and Order, X-Mode Social, Inc., No. 212-3038 (F.T.C. filed Jan. 9, 2024) [hereinafter X-Mode Decision and Order], https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-D%26O.pdf [https://perma.cc/KE9A-25XN]; Press Release, FTC, Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter and Commissioner Alvaro M. Bedoya In the Matter of X-Mode Social, Inc. and Outlogic, LLC at 1 (Jan. 9, 2014) [hereinafter Statement of Chair Lina M. Kahn on X-Mode] (available at https://www.ftc.gov/system/files/ftc_gov/pdf/StatementofChairLinaM.KhanandRKSandAB-final_0.pdf) (highlighting press release from FTC chair highlighting importance of consent agreement with a location data broker); *see also* Complaint at 1, InMarket Media, LLC, No. 202-3088 (F.T.C. filed Jan. 18, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-InMarket MediaLLC.pdf [hereinafter InMarket Media Complaint] (raising unfairness complaint and entering into subsequent consent agreement with a digital marketing platform for its monetization of location data "to facilitate targeted advertising").

[10] *See* 15 U.S.C. § 45(a)(2) (empowering FTC to prevent persons and businesses from using unfair methods of competition and unfair practices).

[11] 15 U.S.C. § 45(n).

J. Solove and Danielle Citron have stated, harm is the gatekeeper of the ability to enforce against privacy violations.[12] However, the current prevalence of location-data sales has provided a multitude of real-world examples of the harms caused by putting people's precise location data in the hands of nefarious parties. The injuries and harms caused by location data sales are related or identical to harms previously recognized by either the FTC or by other legal doctrines. While the harms that occur when a person's precise location data is sold—such as emotional distress, discrimination, stigma, and invasion of privacy—may not fit into the traditional box of "concrete" harms subject to FTC enforcement, they are still within the FTC's enforcement authority.

This Note will argue that the harms from the sale of location data are unfair and also intimately related to many harms previously and properly recognized by the FTC and other legal doctrines. Thus, the FTC's recognition and enforcement against these harms is not novel but rather well established.

Part I of this Note will highlight the efforts of the FTC to enforce against the growing spectrum of consumer harms from privacy invasions, including, notably, its recent disputed complaint against Kochava suggesting a novel theory of Section 5 injury from the sale of location data and its successful consent agreement with X-Mode for similar unfair practices.[13] Part II will lay out a multitude of location data collection and sale practices and the consequences resulting from those practices. Part III will then connect the real-world harms from the sale of location data to persuasive precedent in tort, constitutional, and contract legal doctrines, as well as unfairness complaints brought by the FTC, to suggest that enforcement against the unfairness of the sale of location data is within the bounds of the FTC's authority.

I. THE FTC'S SCOPE OF SECTION 5 ENFORCEMENT

The FTC's ability to enforce against the privacy violations from the sale of location data outlined in Section I.B. is rooted in its Section 5 powers to enforce against unfair and deceptive trade practices.[14] These powers allow the FTC to bring a consumer protection action against any commercial entity when it believes the commercial entity has acted unfairly or deceptively.[15] These actions

[12] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 796 (2022) [hereinafter Citron & Solove, *Privacy Harms*] ("Harm is an element of many causes of action. Courts, however, refuse to recognize privacy harms that do not involve tangible financial or physical injury. But privacy harms more often involve tangible injuries, which courts address inconsistently and with considerable disarray." (footnotes omitted)).

[13] *See* Kochava Complaint, *supra* note 5, at 10; Statement of Chair Lina M. Kahn on X-Mode, *supra* note 9, at 1.

[14] 15 U.S.C. § 45(a)(1) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

[15] *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/6RJZ-FVX8].

most often result in consent orders where the commercial entity "settles" with the FTC and agrees to partake in certain activities and refrain from others.[16]

The FTC's efforts to enforce against various unfair and deceptive trade practices have ventured across industries and adapted through technological advances. The FTC's ability to apply its Section 5 powers in such a vast way can be attributed to the creation of the power, as well as subsequent judicial support for the claim, and that definition and selection of unfair and deceptive practices rests with the FTC.[17]

However, the FTC's Section 5 enforcement and decision-making power was not always favored by companies and their political forces. After a period of broad FTC enforcement, congressional members began to challenge the FTC's seemingly unchecked Section 5 power.[18] This congressional pushback resulted in the FTC releasing a policy statement defining what it means for a trade practice to be unfair.[19] The 1980 FTC Policy Statement on Unfairness outlined three tests that must be satisfied for a practice to be unfair.[20] For a commercial practice to be unfair to consumers, "[i]t must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided."[21] This definition and test for unfairness was later codified to state that the FTC has "no authority . . . unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits."[22] This Note will show that substantial injuries exist when companies or individuals sell the precise location data of consumers, and that those injuries are recognizable as unfair by the FTC.

---

[16] *Id.* (allowing FTC to issue complaint when it has "reason to believe" violation has occurred and discussing opportunity for violator to sign consent agreement with final order).

[17] J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FED. TRADE COMM'N (May 30, 2003), https://www.ftc.gov/news-events/news/speeches/ftcs-use-unfairness-authority-its-rise-fall-resurrection [https://perma.cc/9KF5-QRXJ] (describing 1972 Supreme Court decision which stated FTC, "[T]he Commission, like a court of equity, considers public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws.").

[18] *Id.* (noting Congress once refused to provide funding and shut down FTC for several days, then acted to restrict FTC's authority to use unfairness in new advertising rulemaking).

[19] Letter from Michael Pertschuk, Chairman, FTC, et al. to Wendell H. Ford, Chairman, Consumer Subcomm. of the S. Comm. on Com., Sci., & Transp. & John C. Danforth, Ranking Minority Member, Consumer Subcomm. of the S. Comm. on Com., Sci., & Transp. (Dec. 17, 1980) (policy statement on unfairness), *in* Int'l Harvester Co., 104 F.T.C. 949 app. at 1070-76 (1984) [hereinafter FTC Policy Statement on Unfairness] (clarifying FTC enforcement authority following congressional concerns and plans to hold oversight hearings on unfairness).

[20] *Id.* at 1073-74 (describing three-factor standard for unfairness).

[21] *Id.* at 1073.

[22] 15 U.S.C. § 45(n).

A. *The Narrow Interpretation of Substantial Injury in Practice*

While the FTC determines which practices, and thus harms, to enforce against under Section 5, it tends to limit its enforcement to traditional, concrete harms such as financial injury.[23] Thus, issues arise in holding companies accountable for modern unfair practices when the consumer injuries are not necessarily traditional monetary harms.

The FTC has adopted a narrow interpretation of injury and mostly enforces against financial injuries, or the risk of such injuries, under Section 5 unfairness enforcement.[24] This self-limiting practice is exemplified in the 1980 Policy Statement, which states that most injuries are established through monetary harm, and "[e]motional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."[25] Further, the policy statement specifically refers to acts that "offend[] the tastes or social beliefs of some viewers" as often beyond the types of practices the FTC will seek to ban.[26]

A narrow interpretation of injury by the FTC has led to enforcement against the miniscule financial harms instead of the more serious, but untraditional, privacy harms. For example, in *Mey v. Got Warranty, Inc.*,[27] the injury recognized from unwanted calls to cellphones was the depletion of the phone's battery and the cost of electricity to charge the phone, rather than the real psychological or emotional harms caused by the invasive calls and constant disturbances.[28] The practice of limiting enforcement efforts to traditional harms functions only to perpetuate the harm-based gatekeeping of privacy enforcement by preventing the full potential of privacy statutes from being realized.[29]

B. *FTC's Ability to Determine the Scope of Enforcement*

The FTC itself crafted all the line drawing and limitations placed on the FTC's Section 5 unfairness enforcement described in the last Section, even if at times

---

[23] Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 980 (2021) [hereinafter Richards & Hartzog, *Duty of Loyalty*] ("The consumer protection approach misses all kinds of self-dealing behavior because it looks specifically for outright deception or concrete harm, often in the form of financial injury or extreme emotional suffering.").

[24] Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 639 (highlighting FTC focus on "[m]onetary, health and safety risks" for unfairness enforcement).

[25] FTC Policy Statement on Unfairness, *supra* note 19, at 1073.

[26] *Id.* (highlighting limiting function "substantial injury" serves in unfairness enforcement because of limited interpretation by FTC).

[27] 193 F. Supp. 3d 641, 644-45 (N.D. W. Va. 2016).

[28] *See id.* (noting unwanted phone calls deplete limited minutes for consumers with prepaid cellphone plans); Citron & Solove, *Privacy Harms*, *supra* note 12, at 826-27 ("We have seen the emergence of an odd sort of legal fiction, where the law redresses 'harm' that is not the real interest interfered with as a means to redress a harm at the heart of the matter.").

[29] *See* Citron & Solove, *Privacy Harms*, *supra* note 12, at 826 ("[F]ailing to recognize privacy harm shuts down important cases and prevents many privacy statutes from being effectively enforced.").

it was motivated by congressional influence. The FTC has always determined the scope of its power, and while most entities simply accept and comply with Section 5 consent orders, some entities are beginning to challenge the FTC's authority to determine the scope of unfair trade practices. This has become a particularly important question in the relatively new sphere of privacy and data security enforcement, and Wyndham Worldwide Corp. was the first to challenge the FTC's broad authority.[30]

In *FTC v. Wyndham Worldwide Corp.*, the FTC claimed Wyndham acted both deceptively and unfairly in their data security practices.[31] Wyndham, "[u]nlike nearly all other defendants in FTC actions . . . did not settle with the FTC."[32] Wyndham claimed the FTC did not have the authority to enforce against data security practices, the FTC must formally promulgate rules to bring such unfairness claims, and the FTC action did not give them fair notice.[33] However, the court disagreed. They reinforced the FTC's broad scope of power, stating the FTC does have the authority to regulate data security and it can do so on a case-by-case basis without the need for prior rulemaking.[34]

The arguments put forth in *Wyndham* and the subsequent resolution of the case impact not only the FTC's data security enforcement capacity, but its "whole domain of data protection, including privacy."[35] *Wyndham* supported the idea that the FTC Act intentionally gives the FTC broad enforcement capabilities to allow for flexible consumer protection. As Daniel J. Solove and Woodrow Hartzog have portrayed, the "FTC's unfairness authority is [] comprehensive."[36] A 1914 House Report said as much in defining unfair practices as impossible to

[30] Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2231 (2015) [hereinafter Hartzog & Solove, *The Scope and Potential of FTC Data Protection*] (observing FTC's pre-*Wyndham* power to regulate privacy and data security went unchallenged).

[31] 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) ("[T]he FTC alleges . . . Defendants' failure to maintain reasonable and appropriate data security for consumers' sensitive personal information." (internal quotations omitted)).

[32] Hartzog & Solove, *The Scope and Potential of FTC Data Protection*, *supra* note 30, at 2239.

[33] *Wyndham*, 10 F. Supp. 3d at 607 (resolving each of these issues in favor of FTC).

[34] *Id.* at 612-15, 617-21.

[35] Hartzog & Solove, *The Scope and Potential of FTC Data Protection*, *supra* note 30, at 2243 (explaining crux of argument is whether FTC's authority can extend into areas already regulated elsewhere).

[36] *Id.* at 2247 ("Notably, the FTC can find a practice unfair even when it is otherwise legally permissible.").

define.[37] Similarly, the Second Circuit reinforced that, in regard to unfairness, "[t]he Commission has a wide latitude in such matters."[38]

C. *Movement Forward*

Although the FTC has often limited itself to enforcing against traditional harms, it is within the scope of its Section 5 power to enforce against the growing sphere of modern privacy harms as well. The *Wyndham* court suggested as much in a footnote, stating that nonmonetary harm is not "as a matter of law, unsustainable under Section 5 of the FTC Act."[39] The FTC's broad authority to adapt and refine its regulations of unfair trade practices allows for flexibility in its recognition of the growing sphere of privacy harms. While the FTC has historically limited its recognition of substantial injury to financial harms, it signaled a shift in its unfairness enforcement in its complaint against Kochava in 2022.[40]

The FTC brought a complaint against Kochava for its unfair sale of precise geolocation data.[41] Kochava compiles data from various data brokers and markets its customized data feeds to clients.[42] Kochava also boasts that it "'delivers raw latitude/longitude data . . . [on] 35 million daily active users, on average observing more than 90 daily transactions per device.'"[43] In its complaint, the FTC raised a novel theory of Section 5 injury from the sale of sensitive data.[44] The Commission stated that Kochava's sale of location data allows for users to be tracked "to and from sensitive 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."[45] The FTC

---

[37] *See* H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.) ("It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again.").

[38] Hartzog & Solove, *The Scope and Potential of FTC Data Protection*, *supra* note 30, at 2248 (quoting FTC v. Standard Educ. Soc'y, 86 F.2d 692, 696 (2d Cir. 1936)).

[39] *Wyndham*, 10 F. Supp. 3d at 623 n.15.

[40] *See* Kochava Complaint, *supra* note 5, at 8 (recognizing "exposure to stigma, discrimination, physical violence, emotional distress, and other harms" as substantial injuries).

[41] *Id.* at 1.

[42] Lesley Fair, *FTC Says Data Broker Sold Consumers' Precise Geolocation, Including Presence at Sensitive Healthcare Facilities*, FED. TRADE COMM'N: BUS. BLOG (Aug. 29, 2022), https://www.ftc.gov/business-guidance/blog/2022/08/ftc-says-data-broker-sold-consumers-precise-geolocation-including-presence-sensitive-healthcare [https://perma.cc/4EAK-A96E].

[43] *Id.* (highlighting expansiveness and precision of data).

[44] Kochava Complaint, *supra* note 5, at 1; *see* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 640 (recognizing particular categories of unfairness enforcement and injury and inability of Kochava complaint to fit into any of these categories).

[45] Kochava Complaint, *supra* note 5, at 1-2.

contends this practice "injures or is likely to injure consumers through exposure to stigma, discrimination, physical violence, emotional distress, and other harms."[46] Thus, the FTC recognized nontraditional, emotional injuries beyond that of the usual financial injuries. This complaint was a significant shift forward in the FTC's willingness to enforce against injuries beyond traditional harms.

However, the District of Idaho stalled this progress by granting Kochava's motion to dismiss the FTC's complaint.[47] The court held "[t]he FTC ha[d] not adequately alleged a likelihood of substantial consumer injury."[48] But, in dismissing the FTC's case, Judge B. Lynn Winmill suggested the theory that "a company could substantially injure consumers by selling their sensitive location information and thereby subjecting them to a significant risk of suffering concrete harms at the hand of third parties."[49] The court, however, did not accept that such a risk existed with Kochava's practices because "third parties must take additional steps to link Kochava's geolocation data to particular individuals."[50] Additionally, the court encouragingly stated that consumer injury under Section 5 is not limited to tangible harms, but held the harms from the sale of location data were not sufficiently severe to constitute substantial injury.[51] The court further elaborated that the "[p]rivacy interests in the kind of location data Kochava sells are therefore weaker than, for example, privacy interests in confidential financial or medical information," seemingly reinforcing the distinction between "concrete" harms and the nontraditional harms caused by privacy violations.[52]

Although the court ultimately ruled to dismiss the FTC's complaint against Kochava for failing to allege a likelihood of substantial injury, it also afforded the FTC the opportunity to amend its complaint.[53] This grant of leave to amend provided an opportunity for the FTC to prove the likelihood of substantial injury to consumers from the sale of location data.

In their amended complaint, the FTC presented factual support for the likelihood that Kochava's practices cause substantial injury to consumers.[54] The FTC emphasized that Kochava "provides data that directly links the precise geolocation data to identifying information about individual consumers, such as

[46] *Id.* at 9.

[47] *See* FTC v. Kochava Inc., No. 2:22-cv-00377, 2023 WL 3249809, at *2 (D. Idaho May 4, 2023) (granting motion to dismiss with leave to file amended complaint).

[48] *Id.* at *5.

[49] *Id.* at *6.

[50] *Id.*

[51] *Id.* at *7-9 (addressing one of FTC's arguments that alleged breach of privacy constituted substantial harm to consumers).

[52] *Id.* at *9.

[53] *Id.* at *3.

[54] *See generally* Amended Complaint for Permanent Injunction and Other Relief, FTC v. Kochava Inc., No. 2:22-cv-377 (D. Idaho filed Aug. 29, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/26AmendedComplaint%28unsealed%29.pdf [hereinafter Kochava Amended Complaint].

names, addresses, email addresses, and phone numbers," and advertises this ability to "track and identify individual consumers."[55] The agency even cited marketing materials advertising that Kochava determines home locations of users "by looking at the resting lat/long of a give device between the hours of 10pm and 6am."[56] Additionally, the FTC outlined the "audience segments" offered by Kochava, which include segments such as "Expecting Parents . . . based on consumers' usage of pregnancy, ovulation, or menstruation tracking apps," pregnant consumers, Jewish consumers, and as specific as "pregnant Muslim women."[57] To dispute the argument that the harm caused by this data is merely hypothetical, the FTC used a free sample of Kochava's data to identify a device that visited a reproductive clinic and its single-family residence.[58] The FTC used this information to again argue that Kochava's data products "are used by Kochava's customers to identify and target consumers based on sensitive characteristics and cause or are likely to cause substantial injury in the form of stigma, discrimination, physical violence, emotional distress, and other harms."[59] The court's decision whether or not to validate the FTC's claim of unfairness remains to be seen. However, in January of 2024, the FTC further advanced this claim when it filed a complaint against X-Mode Social regarding its location data sales practices and subsequently entered into its first settlement agreement with a location data broker.[60]

The FTC described X-Mode's practice of "collect[ing] consumer location data through third-party apps," which "includes a unique persistent identifier for the mobile device" and selling it to clients.[61] X-Mode additionally offers to categorize devices into "'audience segments' based on interests or characteristics purportedly revealed by the locations."[62] The FTC raised unfairness claims regarding X-Mode's location data sales using much the same language as it used in its complaints against Kochava.[63] It focused on the data's ability to track consumers "to sensitive 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."[64] And the FTC stated those practices

[55] *Id.* at 2.

[56] *Id.* at 24.

[57] *Id.* at 19-21.

[58] *Id.* at 8-11.

[59] *Id.* at 30.

[60] *See generally* Complaint, X-Mode Social, Inc., No. 2123038 (F.T.C. filed Jan. 9, 2024), https://www.ftc.gov/legal-library/browse/cases-proceedings/2123038-x-mode-social-inc [hereinafter X-Mode Social Complaint]; X-Mode Decision and Order, *supra* note 9, at 1-2.

[61] X-Mode Social Complaint, *supra* note 60, at 2.

[62] *Id.*

[63] *See* Kochava Amended Complaint, *supra* note 54, at 19-21; X-Mode Social Complaint, supra note 60, at 9-10 (describing location data sales practices that involve sensitive locations which can cause unique consumer harms).

[64] X-Mode Social Complaint, *supra* note 60, at 9.

cause or are likely to cause an array of nontraditional harms, such as "loss of privacy, exposure to discrimination, physical violence, emotional distress, and other harms."[65]

X-Mode entered into a consent agreement with the FTC which outlined "general rules for all location data" and "heightened rules for sensitive location data" that it must follow.[66] Thus, the FTC has now successfully settled with one location data broker regarding a claim of unfair acts causing nontraditional injuries. But, while X-Mode's agreement to settle the case and consent to the rules outlined by the FTC is further support of the FTC's ability to enforce against the nontraditional harms caused by the sale of location data, it will not face judicial review.[67] The FTC's pending case against Kochava, however, will, and that decision could determine whether the FTC's recognition of these nontraditional harms is a valid exercise of its power. A ruling against the FTC could potentially stall any progress made by the FTC through its consent agreement with X-Mode or any other progress that might be made under this theory.[68]

On the other hand, a ruling for the FTC could affirm its efforts to enforce against location data sales and recognize nontraditional privacy harms. This Note serves to bolster those efforts by disputing the court's previous holding in the Kochava case that the sale of location data does not create significant risk of harm and is not sufficiently severe to constitute substantial injury under the FTC's Section 5 enforcement powers. It serves to promote the idea that the FTC's powers include an ability to enforce against nontraditional harms, as it properly did in its consent agreement with X-Mode. While Judge Winmill opened the door to recognizing harms beyond just the tangible, the court also reaffirmed the idea that nontraditional harms are weaker than traditional concrete harms. This Note will show that the nontraditional harms caused by the sale of location data by parties like Kochava and X-Mode are sufficiently substantial to properly form the basis of FTC unfairness enforcement, and should be recognized.

[65] *Id.* at 8.

[66] Adam Schwartz, *FTC Bars X-Mode from Selling Sensitive Location Data*, ELEC. FRONTIER FOUND. (Jan. 23, 2024), https://www.eff.org/deeplinks/2024/01/ftc-bars-x-mode-selling-sensitive-location-data [https://perma.cc/8962-2RRU]; *see* X-Mode Decision and Order, *supra* note 9, at 8-11.

[67] *See* Agreement Containing Consent Order, X-Mode Social, Inc., No. 212-3038 at 2 (F.T.C. filed Jan. 9, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Social-ACCO.pdf (waiving X-Mode's right to seek judicial review of Decision and Order).

[68] *See* InMarket Media Complaint, *supra* note 9, at 7-8 (providing additional support for the validity of such injuries in its January 18, 2024, complaint and consent agreement by recognizing the "loss of privacy about the day-to-day movements of millions of consumers and an increased risk of disclosure of such sensitive information" as a substantial injury from improper use of location data).

II. HARMS FROM THE SALE OF LOCATION DATA

The news is bustling with stories of companies collecting and selling data in increasingly unexpected and frightening ways.[69] These stories exemplify the harm that already exists and will continue to be perpetrated when location data is sold without regulation.[70] While many data collectors and aggregators claim that these harms are eliminated because data points remain anonymous and thus the subject of the data's privacy is protected, the expansiveness of available data points makes true anonymization without reidentification nearly impossible.[71] "Anonymous" data can often be reidentified by connecting it to information across several databases and with outside information to reveal the identity of the data point.[72] The Privacy Project from the *New York Times* ("Times Privacy Project") reviewed the data from one such dataset of "anonymous" location data points to demonstrate the lack of actual anonymity.[73] The single dataset Times journalists were given access to held "more than 50 billion location pings from the phones of more than 12 million Americans" across multiple major cities.[74] The billions of data points contained no identifiable information, yet the Times Privacy Project was able to identify a senior official at the Department of Defense and his wife, a Washington Post journalist, and even Tiger Woods.[75]

So, not only are sales of precise location data becoming increasingly more common, but any efforts to mitigate the harm that can occur from the data have become meaningless against the growing capacity to reidentify. Importantly,

---

[69] *See, e.g.*, Jaclyn Diaz, *Amazon, TikTok, Facebook, Others Ordered to Explain What They Do with User Data*, NPR (Dec. 15, 2020, 3:36 AM), https://www.npr.org/2020/12/15/946583479/amazon-tiktok-facebook-others-ordered-to-explain-what-they-do-with-user-data [https://perma.cc/82FR-DHEW] (providing examples of online platforms gathering and transferring user data, such as facial features).

[70] *See* discussion *infra* Sections II.A-C (highlighting harms perpetuated by sale of location data in three different contexts).

[71] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1723-27 (2010) (identifying various reidentification techniques and how they can identify data points even when administrators thought they removed any identifying information by "discovering pockets of surprising uniqueness remaining in the data").

[72] *Id.* at 1707-08, 1724-27 (explaining concept of reidentification and two reidentification techniques, including linking data with outside information and interlocking different data sets).

[73] Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html (investigating smartphone tracking industry by obtaining file full of location pings of smartphones as they moved through major cities, provided by whistleblower alarmed by their location-data company's abuse).

[74] *Id.*

[75] *Id.* (identifying people from "anonymous" data file often simply by "ascertaining a home location and an office location" between which usually only one person would travel daily, thus disputing claim that location data sets cannot identify individual data points because they are "anonymous").

recent legal developments regarding the right of personal and medical privacy have created a frightening urgency to build safeguards around people's sensitive information like precise location. Awareness of this issue and the need for regulation has increased with the *Dobbs* decision,[76] as an additional risk of injury has been created regarding medical care and personal autonomy. As states ban abortion, private companies and law enforcement may be poised to purchase location data to mount prosecutions against those who seek abortions or those who help them.[77] The need to prevent people's sensitive data from being marketed to anyone willing to pay is as important now as it has ever been.

A person's privacy in movement and location is of crucial importance now that governments are attempting to make a doctor's visit a matter of public concern. This Section will exemplify the exigent and widespread issue that is the distribution of people's precise location data and will demonstrate the need for the FTC to step in and enforce against such practices. This Section outlines the harms from the tracking of locations, from the tracking of people, and the government's involvement in the distribution and sale of precise location data.

A. *Location Harm—The Tracking of Locations*

While location-data tracking always involves people as the defining data set, sometimes the privacy harm arises inherently from revealing the locations to and from which those people travel. The locational privacy of individuals is being invaded not because of who they are but because of where they are.[78] Even if this location tracking is not targeting individuals, the harm done from surveilling sensitive locations to acquire information on any and every person who enters is easy to ascertain.[79] Inherent in the ability of many of these practices to continue is the fact that most often people are not even aware it is happening at all.[80] But, imagine a situation where you are followed to every place you go and your presence at those locations is meticulously tracked. The data collector constantly

---

[76] Dobbs v. Jackson Women's Health Organization, 142 S. Ct. 2228 (2022).

[77] David Sherfinski & Avi Asher-Schapiro, *Analysis: U.S. Abortion War Spotlights Women's Risk from Online Tracking*, REUTERS (May 5, 2022, 6:18 PM), https://www.reuters.com/legal/litigation/us-abortion-war-spotlights-womens-risk-online-tracking-2022-05-05/ [https://perma.cc/3LCX-VK8Q] (acknowledging how "law enforcement agencies and private data brokers are tracking social media use, location data, online purchases and search histories to map and profile people" and if states ban abortion this method could be used to enforce abortion bans).

[78] *See* discussion *supra* notes 69-77 (illustrating practices of selling data originating from sensitive locations, such as abortion facilities).

[79] *See* discussions *supra* notes 61-71 (explaining sale or distribution of sensitive location data can lead to criminal prosecution, harassment, and security risks).

[80] Karl Bode, *Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes*, VICE (Oct. 22, 2021, 9:00 AM), https://www.vice.com/en/article/93b9nv/internet-service-providers-collect-sell-horrifying-amount-of-sensitive-data-government-study-concludes [https://perma.cc/V6KH-5FBW] (highlighting how internet service providers hide their data collection and sale practices "in fine print of their privacy policies").

trails you with their notebook jotting down your seventeen-minute trip to the grocery store, your extended lunch break when you told your boss you had an appointment, or even your visit to the podiatrist to check out a nasty blister. It's unnerving to consider every location we visit being public knowledge, yet our phones track that information on a more comprehensive scale than we can imagine.[81] The tracking of seemingly meaningless locations manages to set off alarm bells in our minds, and yet there is a very real practice of companies distributing and selling location data for sensitive and even confidential locations without limitation.[82] These practices have the potential to cause massive harm.[83]

The sale of data sets of precise location pings at medical care facilities is one of these growing practices. The data broker SafeGraph has taken on the practice of profiting from the sale of location information regarding abortion clinics.[84] They claim to obtain their data from "ordinary apps installed on peoples' phones."[85] They then gather and sort that data in order for any individual or company to purchase data based on certain patterns. SafeGraph specifically classifies "Planned Parenthood" as a tracking pattern to be purchased.[86] Motherboard, an investigative group dedicated to technology, paid just over $160 to purchase a week's worth of data showing "where groups of people visiting the locations came from, how long they stayed there, and where they then went afterwards."[87] In other words, any buyer of SafeGraph's "Planned Parenthood" pattern would receive a data set of people who visited Planned Parenthood, allowing them to determine possible appointment lengths, and therefore appointment types, as well as even home addresses of the people who came from their home or went back to their home after the appointment. Even if the data was anonymous, the path to deanonymization of people visiting a

[81] *See, e.g.*, *supra* notes 58-61 and discussion thereof (providing scope of location information regarding abortion facilities available to data broker company).

[82] *See* discussions *supra* notes 58-71 (detailing practices of five companies selling or distributing location data in various contexts, such as abortion clinics, emergency rooms, and military bases).

[83] *See* discussions *supra* notes 58-71 (illustrating harm deriving from sale or distribution of sensitive location information).

[84] Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022, 12:46 PM) [hereinafter Cox, *Abortion Clinic Data*], https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood [https://perma.cc/TB6Z-DYCB] (highlighting how SafeGraph collects users' location data from regular applications and then repackages location data into various products to be purchased).

[85] *Id.* (explaining phones can transmit data to third parties via applications such as prayer or weather applications).

[86] *Id.* (highlighting how SafeGraph allows purchasers to buy data based on "brands" like "Planned Parenthood" or "Family Planning Centers").

[87] *Id.*

sensitive location like Planned Parenthood is clear.[88] And SafeGraph is not the only data broker with this specific practice of selling location data pertaining to abortion clinics, as Placer.ai has a similar practice.[89]

To understand the harm from these tracking practices, consider the concerns of people who may need to travel across state lines for abortions and then return to a state where abortions are banned. The fact that their locations can be gathered and sold for that entire journey reasonably creates apprehension and fear. Thus, there is good reason for regulators to have a sense of urgency in protecting against these risks.[90]

The sale of such targeted location data sets, and the legal ramifications in light of *Dobbs*, is frightening in and of itself. There is, however, a wide array of uses of these sensitive location data sets that, once purchased, cause unique harms as well. Advertisers also exploit these data sets for political or profit-driven purposes.

Copley Advertising, as an example, "surveilled women and other people visiting abortion clinics, geofenced advertising around those clinics, and then enabled anti-abortion organizations to run anti-abortion ads to people sitting in clinic waiting rooms."[91] Copley tagged these users and ran advertisements on their devices for up to thirty days.[92] Similarly, the marketing firm Tell All Digital partnered with law firms to send personal injury law firm advertisements to people in emergency rooms.[93] They geofenced the emergency rooms and identified a person's location from their "'phone ID' from Wi-Fi, cell data or an app using GPS."[94] These practices not only reveal private health information, but they are also a form of digital harassment.[95]

---

[88] *See* discussion *supra* notes 51-55 (highlighting how easily "anonymous" location data can be reidentified with publicly available information, such as home addresses).

[89] Justin Sherman, *The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics*, LAWFARE (Sept. 19, 2022, 8:31 AM), https://www.lawfareblog.com/data-broker-caught-running-anti-abortion-ads—-people-sitting-clinics [https://perma.cc/DD35-XRYJ] (reporting Senator Elizabeth Warren sent letters to Placer.ai "about their sales of location data pertaining to abortion clinics").

[90] *See* Cox, *Abortion Clinic Data*, *supra* note 84 (highlighting need to regulate sale of location data where such practice can heighten security risks of those seeking abortion outside of state and their healthcare providers).

[91] Sherman, *supra* note 89.

[92] *Id.* (illustrating how Copley Advertising used geofencing technology to allow antiabortion organizations to target abortion clinic visitors).

[93] Bobby Allyn, *Digital Ambulance Chasers? Law Firms Send Ads to Patients' Phones Inside ERs*, NPR (May 25, 2018, 2:38 PM), https://www.npr.org/sections/health-shots/2018/05/25/613127311/digital-ambulance-chasers-law-firms-send-ads-to-patients-phones-inside-ers [https://perma.cc/8VDS-VMXM] (highlighting practice of Tell All Digital to geofence around specific locations and then market data to advertisers that may be interested in targeting people within them).

[94] *Id.*

[95] *See id.* (recognizing harm of selling sets of data revealing person's presence at emergency room, which exposes sensitive, private medical information).

These practices also present a severe risk of harm for confidential locations beyond medical care facilities. The fitness tracking application, Strava, recently revealed the location and staffing of military bases and spy outposts.[96] Strava released a data visualization map that "shows every single activity ever uploaded to Strava—more than 3 trillion individual GPS data points."[97] They found that use of the application at United States military bases revealed markers of the location of the bases, and when a viewer zooms in on the map, it can even reveal the internal layout of the base or outpost.[98] While this location data was not being sold, the mere ability to collect and distribute this data is harmful.[99]

As the practices of just five companies illustrate, the exploitation of people's movements and location data for profit (or even not for profit) can have dire legal, emotional, and national security consequences. People are being exposed to potential criminal prosecution and harassment often without an understanding that their presence at a sensitive location is being tracked in the first place. And inherent in all of this is an extreme security risk for individuals.[100]

B. *Personal Harm—The Tracking of People*

As discussed above, the collection of data for sensitive or confidential locations is harmful, but that harm presents as the destruction of the individual autonomy and security of the people being tracked. The precision of this location data, as described by the Times Privacy Project,[101] is frightening. Present throughout this entire discussion is the escalation of risk created by the ability to deanonymize this information.[102] Thus, the tracking of people based on demographics or specific purposes presents equally if not more harmful consequences.

---

[96] Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases*, GUARDIAN (Jan. 28, 2018, 4:51 PM), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases [https://perma.cc/RMF7-GSRG] (explaining how active service military personnel were subset of Strava users whose activity published to application revealed bases and outposts).

[97] *Id.*

[98] *Id.* (publishing photos of maps where Strava users' paths light up remote regions in various locations where confidential bases existed).

[99] Richard Pérez-Peña & Matthew Rosenberg, *Strava Fitness App Can Reveal Military Sites, Analysts Say*, N.Y. TIMES (Jan. 29, 2018), https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html (citing opinions of security analysts regarding Strava maps, including warning such data exposure "could leave troops open to attack").

[100] *See, e.g.*, *id.* (reporting on risk Strava maps pose to individual military personnel, even outside of war zones).

[101] Thompson & Warzel, *supra* note 73 (highlighting precision of data journalists received from location-tracking industry, including precise time and location that allowed identification of individual protesters).

[102] *See id.* (citing law professor's opinion emphasizing difficulty of anonymizing "precise, longitudinal geolocation information").

The tracking and targeting of specific populations' location data, such as religious minorities, the LGBTQIA+ community, or other vulnerable populations, may create the greatest potential for harm. Discriminatory surveillance based on people's characteristics or statuses is a dangerous power that can have devastating impacts.[103] While some may argue that this sorting is just an ordinary practice, it can and has been used to minimize opportunities for some groups, increase risk of government tracking, and generally disqualify whole populations from basic protections.[104] Surveillance has long had a disparate impact on minority populations, so the potential harms caused by the sale of the location data of specific populations cannot be ignored.[105]

One instance of such location data targeting involved the purchase and deanonymization of the location data of a Catholic priest. A Catholic Substack publication, *The Pillar*, acquired and combined data from various sources to publicly "out" a priest as potentially gay, leading to his resignation.[106] They reported using location data tied to Grindr and other applications to track the priest between his private residence and gay bars.[107] This data was presented as anonymous, but as repeatedly shown, there is no such thing.[108] And this practice is not rare. A nonprofit in Denver recently spent millions of dollars to obtain location data of priests using gay dating applications and cross-referenced it with location data to identify clergy members.[109] This exemplifies the exact practice that sparks fear in those aware of this new surveillance frontier and risks

[103] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1956-58 (2013) (exemplifying harm that can result from using surveillance to sort people into categories, such as "use of census records by the American, Canadian, and German governments during the Second World War to identify citizens to relocate to the Japanese internment camps in North America and the concentration camps in Europe").

[104] *Id.* (identifying harmful uses such as "selective promotions to more or less desirable customers," or government profiling for criminal risk).

[105] Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance*, CENTURY FOUND. (Dec. 21, 2017), https://tcf.org/content/report/disparate-impact-surveillance/ [https://perma.cc/YLL4-QECS] (highlighting unequal consequences of heavy surveillance in minority neighborhoods, especially in context of police enforcements and public benefits).

[106] Joseph Cox, *The Inevitable Weaponization of App Data Is Here*, VICE (July 21, 2021, 12:10 PM) [hereinafter Cox, *Weaponization of App Data*], https://www.vice.com/en/article/pkbxp8/grindr-location-data-priest-weaponization-app [https://perma.cc/2WH4-R7U3] (highlighting story of how Catholic publication that used location data to identify priest, illustrating "sensitive location data from a smartphone app [can be used] to track and publicly harass a specific person" despite assurances from data companies it was not possible).

[107] *Id.*

[108] *See, e.g.*, *id.* (reporting *The Pillar*'s ability to identify priest and his movement among "anonymous" dataset with several reference points, such as his residence).

[109] Michelle Boorstein & Heather Kelly, *Catholic Group Spent Millions on App Data that Tracked Gay Priests*, WASH. POST (Mar. 9, 2023, 8:52 AM), https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/ [https://perma.cc/RL9Q-UG2U] (reporting on Catholic nonprofit's use of location data for its "mission," which includes identifying and sharing dating profiles of priests).

"doxxing" individuals based on sold location data. Similar practices could be used to target any person that falls within a specific population and to publicize intimate details of that person's life for whatever political or personal reasons.[110]

Location data is also increasingly being used to target voters, which opens the door for targeting based on political belief.[111] Political data companies are using location data as a part of their services designed for political campaigns, and data brokers are also tailoring their products to the industry by offering data segments based on "Likely Republican Voter," "Likely Democrat Voter," "likely to vote for Republican candidates based on attending Republican focused political events and events and venues affiliated with conservative topics," or specific "Political Rally Attendees."[112] The political targeting firm DSPolitical even advertised the ability to advertise to people at polling locations.[113] Specifically, the conservative PAC Catholic Vote targeted "ads declaring the Democratic U.S. Senate candidate 'anti-Catholic'" at people who frequented catholic churches.[114] The practice of using location data in "voter files" raises concerns for political targeting and misinformation campaigns. Not only could these services be abused to discriminate on the basis of political beliefs, but they can, and have, been used to target people in the midst of political participation.

Beyond discriminatory harm, there are horror stories of individual persons acquiring location data on another person and inflicting concrete harm. An instance of such harm arose when T-Mobile was fraudulently induced to provide the location of a user's phone to "a debt collector with a history of stalking and domestic violence."[115] The man harassed the user at her place of work and her home at all hours of the night.[116] This harassment led to the victim's teenage daughter moving away out of fear.[117] While this data was improperly and illegally obtained rather than purchased by the harasser, T-Mobile, along with AT&T and Sprint, also sold their customers' real-time location data to a network

---

[110] *See id.* (quoting advisor to digital rights organization describing *The Pillar*'s practice as "character assassination of a private citizen").

[111] Jon Keegan, *How Political Campaigns Use Your Phone's Location to Target You*, MARKUP (Nov. 17, 2022, 11:15 AM), https://themarkup.org/privacy/2022/11/08/how-political-campaigns-use-your-phones-location-to-target-you [https://perma.cc/T6J8-D9AK].

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] Joseph Cox, *T-Mobile 'Put My Life in Danger' Says Woman Stalked with Black Market Location Data*, VICE (Aug. 21, 2019, 12:36 PM) [hereinafter Cox, *Woman Stalked with Black Market Location Data*], https://www.vice.com/en/article/8xwngb/t-mobile-put-my-life-in-danger-says-victim-of-black-market-location-data [https://perma.cc/BS9U-4HU8] (reporting on stories of individuals whose location information was disclosed by phone carriers to third parties with harmful intentions).

[116] *Id.* (detailing level of harassment user experienced after her location data was disclosed to debt collector).

[117] *Id.*

of 250 bounty hunters and related businesses.[118] The ease of access to such vast amounts of real-time location data resulted in some of this data being resold to unauthorized parties.[119] As these practices show, people's precise location data can be used to target individuals or populations of people to bring about harm. People are being discriminated against, exposed to stalking and harassment, and losing any sense of security, often without the understanding that their personal, precise location is being collected and sold or distributed to unknown third parties.

C. *Government Involvement*

Many data brokers selling precise location data allow for their data sets to be purchased by anyone, which opens the door for government agencies to purchase this data for use in situations where such tracking would normally trigger Fourth Amendment protections.[120] Many data brokers have expansive agreements with government agencies that give them access to troves of this data.[121] The concerns discussed regarding the sale of location data for sensitive sites and location data of vulnerable populations can be exacerbated when the government is the purchaser of the data.

As Neil Richards explains, government surveillance poses two kinds of dangers: threatening political freedom and giving the government greater power over its citizens.[122] Government surveillance threatens political freedom by "chilling our ability to think, read, or communicate politically unpopular ideas," thus removing our ability to form "the critical perspective from which to dissent and demand better."[123] And more fundamentally, government surveillance gives the government power over individuals' personal information which can lead to "blackmailing and discrediting, discrimination, and persuasion."[124] Inherently,

---

[118] Joseph Cox, *Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years*, VICE (Feb. 6, 2019, 5:10 PM), https://www.vice.com/en/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years [https://perma.cc/LTZ3-DAMR] (explaining service providers sold location data through data seller to hundreds of bounty hunters which included "highly sensitive and accurate GPS data . . . [that] could locate someone so accurately so as to see where they are inside a building").

[119] *Id.* (stating some bounty hunters resold location data to other unauthorized parties).

[120] *See* discussion *supra* notes 104-06 (noting use of geofence warrants involving sweeping searches by government agencies and its implication of Fourth Amendment rights).

[121] *See* discussion *supra* notes 87-102 (illustrating practices of data platform and broker companies selling precise location datasets containing more than one million data points to government agencies, such as Department of Homeland Security).

[122] NEIL RICHARDS, WHY PRIVACY MATTERS 134, 141-62 (2021) [hereinafter RICHARDS, WHY PRIVACY MATTERS] (elaborating on how "unconstrained surveillance" can pose different types of threats).

[123] *Id.* at 143-44.

[124] *Id.* at 146.

government involvement in the sale and distribution of location data raises the stakes and can have harmful discriminatory implications.[125]

Prior to the FTC's enforcement action against X-Mode, an investigation by *Vice* revealed X-Mode's connections to "[government] contractors, and by extension, the military."[126] X-Mode and another data stream with connections to counterterrorism, counterinsurgency, and special reconnaissance military branches, Babel Street, supplied location data gathered from ordinary applications to the U.S. military.[127] The CEO of X-Mode says that they track "25 million devices inside the United States every month, and 40 million elsewhere . . . [and its tool for obtaining location data] is embedded in around 400 apps."[128] They then sell that information to their clients who were found to, at least at one point, include a company that "builds combat aircraft for the U.S. Air Force" and supports "in the development of cyber and electronic warfare capabilities," and a research company that offers data analytics to Army, Navy, and Air Force intelligence analysts.[129]

Three of the hundreds of applications X-Mode collected precise location data from were a Muslim prayer application, a Muslim dating application, and "a dating app for 'bi, gay, and open-minded men.'"[130] Thus, X-Mode was providing a direct connection between data sets filled with the precise location data of Muslim people without concern for any protections that such data may be afforded before being provided to the government.[131] The use of these tools to locate specific people is not theoretical. A private threat intelligence firm,

[125] *See, e.g.*, discussion *supra* notes 100-101 (discussing purchase and use of Muslim individuals' precise location data by U.S. military and intelligence analysts).

[126] *See* Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020, 10:35 AM) [hereinafter Cox, *U.S. Military Buys Location Data*], https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x [https://perma.cc/E7VN-HWL9] (discussing methods of location data acquisition by X-Mode, which involves installing software development kits in third-party applications).

[127] *Id.* (reporting Babel Street provides product Locate X, which can be purchased and allows users to "draw a shape on a map, see all devices Babel Street has data on in that location, and then follow a specific device around to see where else it has been").

[128] *Id.* (showing data transfer from third-party applications to X-Mode includes "name of the Wi-Fi network the phone was currently collected to, a timestamp, and information about the phone such as its model").

[129] *Id.*

[130] *Id.*; Jon Keegan & Alfred Ng, *Gay/Bi Dating App, Muslim Prayer Apps Sold Data on People's Location to a Controversial Data Broker*, MARKUP (Jan. 27, 2022, 8:00 AM), https://themarkup.org/privacy/2022/01/27/gay-bi-dating-app-muslim-prayer-apps-sold-data-on-peoples-location-to-a-controversial-data-broker [https://perma.cc/BL6D-3JGE].

[131] Cox, *U.S. Military Buys Location Data*, supra note 126 (noting although X-Mode encourages compliance with relevant data protection laws, some applications working with X-Mode did not have adequate "disclosures around the sale of location data" to notify users).

HYAS, pitches their business' ability to use X-Mode data to track people to their "doorstep."[132]

Similarly, the data broker Fog Data Science has been selling precise location data to federal, state, and local law enforcement agencies.[133] Fog Data obtains their location data from thousands of apps and claims to have "'billions' of data points about 'over 250 million' devices and that its data can be used to learn about where its subjects work, live, and associate."[134] Fog Data sells access to this data via its web application, Fog Reveal, which is available to police departments across the country for less than $100,000 per year.[135] Fog Data has contracted with "at least 18 local, state, and federal law enforcement clients," and provides easy access to this data for any individual.[136]

Records obtained by the ACLU also showed that the Department of Homeland Security ("DHS"), specifically Customs and Border Protection and Immigration and Customs Enforcement, has purchased access to troves of people's precise cell phone locations collected by apps.[137] DHS is spending millions of dollars to buy this data from two data brokers: Venntel and Babel Street.[138] Venntel has claimed to collect "more than 15 billion location points from over 250 million cell phones and other mobile devices *every day*."[139] The DHS's intended use for this information is clear from their 2018 proposal to use location data to combat illegal immigration.[140] The DHS is not the only federal agency to purchase location data. The FBI Director, Christopher Wray, testified

---

[132] Joseph Cox, *Private Intel Firm Buys Location Data to Track People to Their 'Doorstep'*, VICE (Sept. 2, 2020, 1:10 PM), https://www.vice.com/en/article/qj454d/private-intelligence-location-data-xmode-hyas [https://perma.cc/26A8-Q2DN] (highlighting how HYAS differs from other industries buying location data, especially in that HYAS obtains location data specifically intending to "pinpoint[] particular people").

[133] Bennett Cyphers, *Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police [https://perma.cc/PL24-S79Q] (identifying past or current clients of data broker company, such as state highway patrols).

[134] *Id.*

[135] *See id.* (explaining Fog Data's "panoptic surveillance apparatus" is offered to state highway patrols, local police departments, and country sheriffs).

[136] *Id.* (stating Fog Data provides its users ability to "point and click to access detailed histories of regular people's lives").

[137] *See* Shreya Tewari & Fikayo Walter-Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022), https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data [https://perma.cc/BU5B-GBMC] (revealing results of ACLU FOIA lawsuit regarding government's ability to obtain private data, noting ICE and CBP's warrantless purchase of access to individuals' sensitive location information).

[138] *Id.*

[139] *Id.* (adding Venntel's services provide ability to "track specific individuals or everyone in a particular area, learning details of our private activities and associations").

[140] *See id.* (citing 2018 DHS internal document proposing use of location data to identify patterns of illegal immigration).

that while the FBI does not currently purchase location data, the agency has done so in the past "for a specific national security pilot project."[141]

Additionally, the data vendor Geofeedia, which collected location data from Facebook, Instagram, and Twitter, provides location data to over 500 law enforcement and public safety agencies.[142] Geofeedia "tout[s] its product as a tool to monitor protests."[143] The ACLU found that the product was used by law enforcement agencies during protests in Baltimore, Ferguson, and Oakland.[144] Fortunately, Facebook, Instagram, and Twitter terminated Geofeedia's access to their platforms, but only after the ACLU and others reported law enforcement's easy access to such information.[145]

While government agencies have been circumventing their requirement to obtain a warrant for data of this kind, significant harm can arise from government misuse of such precise location data even when it is procured with a warrant. These general-location geofence warrants, the constitutionality of which are hotly debated, raise concerns regarding the consequences of being able to scale such precise location data on large amounts of people at one time.[146] Google is one such data collector that responds to warrants for location information and releases information on dozens or even hundreds of devices within a designated area.[147] These geofence warrants do not release just a specific user's information, but rather information on all devices within an area during a set time period—creating an obvious concern for the "innocent" people

---

[141] Dell Cameron, *The FBI Just Admitted It Bought US Location Data*, WIRED (Mar. 8, 2023, 2:45 PM), https://www.wired.com/story/fbi-purchase-location-data-wray-senate/ [https://perma.cc/UCT2-GRP6] (reporting on Senate hearing where Senator Ron Wyden questioned FBI director Christopher Wray regarding whether FBI purchases U.S.-phone geolocation information).

[142] Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed To Target Activists of Color*, ACLU (Oct. 11, 2016), https://www.aclu.org/news/privacy-technology/facebook-instagram-and-twitter-provided-data-access [https://perma.cc/562H-JK4W].

[143] *Id.*

[144] *Id.*

[145] *Id.* (noting Facebook and Instagram had cut Geofeedia's access to public user posts, and Twitter had taken some steps to "rein in" Geofeedia without ending relationship); *see also* Lora Kolodny, *Facebook, Twitter Cut Off Data Access for Geofeedia, a Social Media Surveillance Startup*, TECHCRUNCH (Oct. 11, 2016, 4:42 PM), https://techcrunch.com/2016/10/11/facebook-twitter-cut-off-data-access-for-geofeedia-a-social-media-surveillance-startup/ [https://perma.cc/N6XG-F3T7] (reporting on statement from Twitter announcing it would immediately suspend Geofeedia's commercial access to its data).

[146] Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2510-11 (2021) (recognizing controversy surrounding geofence warrants and Fourth Amendment implications).

[147] Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html (interviewing Google employees familiar with geofence warrant process).

who happen to be in the area.[148] In one instance where a geofence warrant was granted, an Arizona man was wrongfully detained for nearly a week after his phone was tracked to the site of a murder.[149]

These examples of realized or potential dire consequences from the sale of location data raise serious red flags regarding this seemingly unchecked and unregulated practice. It is a present threat that is causing real-world harm, as a multitude of entities are using location data to track and target individuals based on the sensitive locations they travel to, the activities they participate in, and even how they identify. The pressing question remains of how to protect individuals from these invasive harms. The FTC has stepped up to the task, yet some still argue that this novel enforcement effort is too far beyond the FTC's authority.[150] However, as this Note will show, this argument is without merit, and privacy harms of this kind can and should be recognized as unfair.

III. Connection to Other Persuasive Precedent

Harms created from the sale and distribution of precise location data can be seen and felt in the real world, but similar nontraditional harms have also been legally recognized in other contexts. Legal doctrine outside the FTC's Section 5 enforcement efforts supports the idea that "legal harm" can include injuries not so cut and dry as financial or physical harm. This recognition supports the proposition that nontraditional concepts of privacy harms can and should be recognized by the FTC as well. This idea has invaded judicial decisions across tort law, constitutional law, and contract law, and thus the FTC should be able to take advantage of this expanded conceptualization of harm as well. With the growing occurrence of privacy violations from new technologies and data practices, it is high time for the FTC to use other precedent to furnish support for its recognition of nontraditional privacy harms. New privacy violations require the recognition of new privacy harms.

Furthermore, the FTC has accepted and implemented theories from other legal doctrines before. The FTC has previously borrowed precedent from tort law to influence substantive FTC enforcement actions. In its approach to unfair data-security practices, the FTC does not require an actual breach, nor does a breach automatically trigger unfairness enforcement; rather, the FTC recognizes unfair practices based on whether or not reasonable data security measures were in place.[151] The FTC states that "[t]he touchstone of the Commission's approach

---

[148] *See id.*

[149] *Id.* (showing how dangerous location data can be in certain circumstances, such as when Jorge Molina was charged with murder based on circumstantial evidence gathered by geofence warrant).

[150] *See supra* note 5 and accompanying text.

[151] *See* FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (2014) (establishing FTC's approach to data security considers that "company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities").

to data security is reasonableness."[152] The FTC adopts a negligence-like standard of reasonableness equivalent to that used in tort law.[153] Thus, how other legal doctrines treat harm can be relevant to the FTC's conceptualization of harm and determination of harm for their own enforcement.

A. *Tort Law*

Privacy torts have represented an expansion of injury conceptualization to incorporeal injuries.[154] In their article, *The Right to Privacy*, Samuel D. Warren and Louis D. Brandeis recognized an "injury to feelings" when practices interfere with a person's estimate of self.[155] When discussing privacy harms, they argued that the law protects against harms beyond just the financial or physical, an argument broadly accepted in tort law.[156] This argument has historical roots in a discussion in *Prince Albert v. Strange*, where the harm recognized was the undermining of control over the extent to which personal information is circulated.[157] An analogy can be drawn between the harm recognized in 1848 from the publication of personal etchings to the harm caused by the distribution of personal location data: both implicate a lack of control over personal information. Further, privacy torts have long recognized feelings of "violation, mortification, fear, humiliation, and embarrassment" that arise from this lack of control as cognizable harms.[158] Tort law continues to recognize injuries beyond the financial and has taken major steps to support recognition of proper privacy harms. Specifically, three privacy torts support the acknowledgement of comparable harms caused by the sale of location data: intrusion upon seclusion, public disclosure of private facts, and breach of confidentiality.

The intrusion upon seclusion tort recognizes a cause of action when there is an intentional intrusion upon a plaintiff's solitude, seclusion, or private affairs, where the plaintiff has a reasonable expectation of privacy.[159] This tort has recognized an intrusion in instances of surveillance of a nurse's office where exams are done, surveillance of mixed sex or women's bathrooms, surveillance of locker rooms, and various other intrusions into locations without a protected

[152] *Id.*

[153] *See id.*

[154] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 194 (1890) (expanding incorporeal rights from corporeal property).

[155] *Id.* at 219.

[156] *See id.* at 196 ("[M]odern enterprise and invention have, through invasions upon [man's] privacy, subjected him to mental pain and distress far greater than could be inflicted by mere bodily injury.").

[157] *See id.* at 195, 202-05 ("Thoughts, emotions, and sensations demanded legal recognition.").

[158] Citron & Solove, *Privacy Harms*, *supra* note 12, at 843.

[159] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

property interest.[160] This tort has also recognized an intrusion of a reasonable expectation of privacy without physical trespass, including instances of wiretaps or monitoring without trespass, collection of biometric data, or filming plaintiffs in an enclosed backyard.[161] This tort also has extended to the investigation or examination of private concerns such as personal, psychological, or emotional integrity.[162] The long list of sensitive concerns afforded privacy includes accessing private emails, taking information from state personnel records, reading a private diary, downloading nude photos while servicing a computer, garnering confidential medical information, detailed investigating of personal or sexual relationships, surveilling sexual activities in office, overzealous public monitoring, and various other invasions.[163] The intrusion upon seclusion tort establishes that surveillance of private concerns is a recognizable privacy violation. And, although the intrusion upon seclusion tort focuses on collection, the sale of location data requires collection of data in a way that intrudes on private concerns in much the same way.

The public disclosure of private facts tort also recognizes a variety of damages from privacy violations when private concerns are disclosed.[164] Some cases have recognized website publicity as comparable to a newspaper, or similar dissemination to a "widely circulated group."[165] Just as newspaper distribution of private concerns can cause a variety of harms, the data brokers' creation of websites with access to troves of location data sets is a similarly harmful disclosure. This tort recognizes a variety of damages that result from the broad scope of harm caused by the public disclosure of private concerns, such as psychic damages (fear of physical security, fear of identity theft, harassment, mental distress, anxiety, and withdrawal from society) and reputational damages.[166] And while the public disclosure of private facts tort requires the disclosure be highly offensive to the "ordinary sensibilities of an ordinary person,"[167] precedent suggests that information like the precise location of a person at any given moment could very well meet this standard. Disclosures

---

[160] *See* DAVID. A. ELDER, PRIVACY TORTS § 2:5 (2021) (providing examples of decisions where plaintiffs had causes of action for physical intrusions upon their persons or into physical location where they had reasonable expectations of privacy but no protected property interests).

[161] *See id.* at § 2:6 (providing examples of "offensive non-trespassory intrusions").

[162] *Id.* ("The courts have generally recognized that one's '"personality" or psychological integrity' is as important as one's locational privacy. . . . The interest in psychic integrity or 'psychological solitude' has been recognized in numerous cases." (footnotes omitted)).

[163] *Id.*

[164] RESTATEMENT (SECOND) OF TORTS § 652D (1997) ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy . . . .").

[165] ELDER, *supra* note 160, at § 3:3.

[166] *See id.* at § 3:8 (noting possibility of recovery for psychic damage or reputational injury).

[167] *Id.* at § 3:6.

regarding medical history, sexuality, and abortion counseling have all been recognized as highly offensive,[168] and this type of sensitive information can be expected to be procured through location data.

Breach of confidentiality is a common law tort that can extend to certain relationships where there is a disclosure of private information—mostly in professional, not familial or personal settings.[169] And while courts have not yet treated companies with personal data as having a duty to maintain confidentiality, these companies are in a position of trust and exercise power over data in much the same way as professional relationship subject to confidentiality duties.[170] Some have argued that companies that collect and use personal data should be responsible for an equivalent fiduciary duty.[171] Other relationships that have been recognized as fiduciary—lawyers, clergymen, employers, former spouses—always have an element of confidential information.[172] The overarching purpose of the breach of confidentiality tort is to recognize the injury that can result from a breach of trust and power. The same trust and power that data collectors, who have the power to obtain and sell massive amounts of location data from devices and apps that user's trust, abuse.

Thus, the injuries that tort law doctrine recognizes are directly related to the various harms caused by the sale of location data. The sale of location data results in surveillance of private concerns, disclosure of those private concerns, and breaches of trust which result in the same harms recognized by privacy torts in these actions. And this analogy supports the argument that the harms caused by the sale of location data are recognizable as unfair by the FTC.

B. *Constitutional Law*

Constitutional law has also protected against many harms similar to those caused by the sale of location data. The various examples of the consequences resulting from the sale of location data discussed above are analogous to harms that constitutional legal doctrine seeks to protect against. The sale of location data resulting in people receiving personal injury attorney ads following a visit to the emergency room, receiving antiabortion messages following a visit to

---

[168] *See id.* (providing examples of cases imposing liability for dissemination of details of medical health, "outing" gay employee, and disclosing abortion counseling).

[169] G. Michael Harvey, *Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. PA. L. REV. 2385, 2398-2401 (1992) (advocating for legally enforceable duty of confidentiality attaching to certain relationships, including "physician-patient, psychiatrist-patient, school-student, attorney-client, priest-penitent, banker-customer, and reporter-source"). *See generally* Alan B. Vickery, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426 (1982) (identifying contours of then-emerging breach of confidence tort).

[170] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 103 (2004).

[171] *See, e.g.*, *id.* (arguing law should recognize that companies collecting and using individuals' personal data stand in fiduciary relationship with those individuals).

[172] *See* ELDER, *supra* note 160, at § 5:1.

abortion clinics, or being tracked at protests by law enforcement represents how the use of precise location data can alter people's decision making. An awareness that one's movements are being tracked will inevitably create hesitancy in future actions and travel. This is the same harm Neil Richards recognizes as a primary danger of government surveillance because of how it drives us to social conformity.[173] This harm is recognized as a "chilling effect" and implicates a person's First Amendment rights.[174] Also, as shown above, location data can be sorted and sold by demographic. Tracking individuals according to religion or medical status is a discriminatory practice that coincides with discriminatory harms, which constitutional law has sought to protect against.

Civil liberties in a world of advancing technology are increasingly complex. However, the First Amendment has afforded people the protection of their intellectual privacy, which includes the freedom to think, read, and communicate privately.[175] The chilling of those First Amendment activities has been recognized as irreparable injury in constitutional law.[176] Digital monitoring, such as the collection and sale of precise location data to government agencies, can make people less likely to engage in certain conversations, express certain views, and share personal information.[177] Data privacy harms are analogous to those recognized as chilling effects and constitute irreparable injuries in constitutional law.

Civil rights doctrine has also aimed to address discrimination harms. It emphasizes the need for equal access to the places where people learn, work, socialize, and vote.[178] Surveillance has been known to disproportionately impact marginalized people.[179] And sometimes surveillance is used intentionally to

---

[173] *See* RICHARDS, WHY PRIVACY MATTERS, *supra* note 122, at 143.

[174] Jennifer M. Kinsley, *Chill*, 48 LOY. U. CHI. L.J. 253, 257-58 (2016) (recognizing First Amendment protects against impacts on "hypothetical expression," and "chilling effect doctrine" reasons laws that "chill" speech are unconstitutional).

[175] NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 6 (2015) [hereinafter RICHARDS, RETHINKING CIVIL LIBERTIES].

[176] *See, e.g.*, Dombrowski v. Pfister, 380 U.S. 479, 490 (1965) (reasoning showing of "substantial loss or impairment of freedoms of expression" from chilling effect constitutes irreparable injury).

[177] *See* RICHARDS, RETHINKING CIVIL LIBERTIES, *supra* note 175, at 142-43.

[178] Danielle Citron & Mary Anne Franks, *Cyber Civil Rights in the Time of COVID-19*, HARV. L. REV. BLOG (May 14, 2020), https://blog.harvardlawreview.org/cyber-civil-rights-in-the-time-of-covid-19/ [https://perma.cc/W3VD-B5KQ] (arguing civil rights need to expand to digital spaces as exemplified during COVID-19 pandemic).

[179] *See* Mary Anne Franks, *Democratic Surveillance*, 30 HARV. L. REV. 425, 428-29 (2017) (highlighting how Black people have endured "extensive and intimate state invasions of privacy," poor people have been investigated in matters such as "childrearing [and] housing arrangements," and women have faced "state scrutiny and control of their most private decisions").

target in a discriminatory way.[180] Thus, some people's choices and movements carry disproportionate risks of harm, and that discriminatory outcome is a harm itself under constitutional law.[181]

Thus, the harms that constitutional law recognizes are directly related to the various harms caused by the sale of location data. The sale of location data results in invasive surveillance and targeted tracking which create the same harms recognized by constitutional law's chilling effect doctrine and discrimination prevention. And this analogy further supports the argument that the harms caused by the sale of location data are recognizable as unfair by the FTC.

C. *Contract Law*

Contract law also recognizes certain harms and damages that result from broken trust or emotional distress. As previously discussed, fiduciary relationships recognize that trustees in a position of special trust owe certain special duties to beneficiaries.[182] A collector and aggregator of location data has similar special duties to users, especially considering the lack of user awareness regarding the collection of their sensitive data.[183] The argument that data collectors have a special relationship with users that creates special duties is not new.[184] Many scholars have suggested that data collectors are "information fiduciaries" subject to duties of care and loyalty.[185] Generally, if the goal of fiduciary duties is to recognize the harm that can be caused when people in a position of special trust do not act in the interests of those who trust them, a wide array of relationships could be argued to have enforceable fiduciary responsibilities.[186] Contract law recognizes the emotional harm that results from the violation of duties established in those special relationships.

180 *See* Cox, *Weaponization of App Data*, *supra* note 106 (providing example of how use of Grindr app could be used to target gay individuals); Cyphers, *supra* note 133 (noting Fog Reveal service could be used to search for visitors in Planned Parenthood, immigration law offices, or protests against police violence).

181 Franks, *supra* note 179, at 443, 448-49 (listing harms including "loss of employment and educational opportunities, restrictions on the freedom to move, associate, or dress as one wishes, interference with parenting abilities, and loss of general confidence").

182 *See* Harvey, *supra* note 169, at 2400 (noting duty of confidentiality in professional and quasiprofessional relationships).

183 *See* Citron & Solove, *Privacy Harms*, *supra* note 12, at 860-61 (arguing "list of relationships recognized as fiduciary ones is open-ended").

184 *See* Richards & Hartzog, *Duty of Loyalty*, *supra* note 23, at 987-88 ("The idea of subjecting data collectors to a duty of loyalty is not entirely new. The concept has been circulating for some time in a variety of forms and levels of specificity.").

185 *Id.* at 988.

186 *Id.* at 969 ("At face, loyalty is about preventing opportunistic behavior."); Ethics Unwrapped, *Fiduciary Duty*, ETHICS UNWRAPPED: MCCOMBS SCH. OF BUS., https://ethicsunwrapped.utexas.edu/glossary/fiduciary-duty [https://perma.cc/49V7-PJZL] (last visited Feb. 16, 2023) (defining fiduciary duty as legal obligation to act in best interest of another).

Contract law also allows for the recognition of emotional harm and award of emotional distress damages in certain circumstances.[187] The general rule is that emotional distress damages are not permitted for breach of contract except when the contract is personal in nature—emphasizing the unique responsibilities that arise when personal or sensitive relationships are involved.[188] The relationship between users and entities collecting their sensitive location data is not contractual, but there is a special relationship, and the nature of the data is analogous to what might be shared through personal contracts. For example, personal contracts such as a promise to marry or a failure to properly prepare a corpse have been found to allow emotional distress damages because of the personal human interactions involved.[189]

Thus, the harms that contract law recognizes are also directly related to the various harms caused by the sale of location data. When organizations gather and sell the location data of consumers who rely on and trust them, a breach-related harm occurs that mirrors the emotional harms recognized by contract law's breach of trust and emotional distress damages from personal contracts. This analogy further supports the argument that the harms caused by the sale of location data are recognizable as unfair by the FTC.

The real-world instances of the sale and distribution of location data showed that the harm done by the sale of location data is present, but various legal doctrines show that it is also legally recognizable. Because the FTC has previously taken advantage of legal arguments drawn outside of their own unfairness enforcement, these connections between harms caused by the sale of location and harms recognized by other legal doctrines strongly support the FTC's ability to enforce against them. The recognition of nontraditional harms by other legal doctrine continues to chip away at the argument that the FTC has no ability to recognize these nontraditional harms, and the forthcoming analysis of how the harms caused by the sale of location data fit into the FTC's current body of enforcements will show that the recognition is also actually well-established.

IV. FTC ENFORCEMENT OF SIMILAR INJURIES

The analogy drawn between the consequences of location data sales and legal doctrine supports the theory that the sale of location data does not create meaningless or unrecognizable harms. But it is still necessary to establish that these are harms that the FTC can and should protect consumers against. While the FTC rarely receives much resistance to their Section 5 enforcement consent orders, resistance often comes when companies or people believe the FTC is

[187] *See* Citron & Solove, *Privacy Harms*, *supra* note 12, at 844 (noting enough foundation in law for courts to explore issue of emotional distress damages from breach of contracts).

[188] *Id.* (highlighting courts' willingness to occasionally recognize emotional damages in contract law, such as when breach is willful or contracts are personal in nature).

[189] Charlotte K. Goldberg, *Emotional Distress Damages and Breach of Contract: A New Approach*, 20 U.C. DAVIS L. REV. 57, 58 n.5 (1986-87).

acting far beyond their authority in raising a novel theory of unfairness or deception.[190] Kochava is one such party that challenged the FTC's authority.

Kochava moved to dismiss the FTC's complaint against it for several reasons, most notably because their conduct was not "substantially injurious to consumers" and the FTC's "attempted creation of new law" did not afford them "fair notice."[191] The court agreed that, even if the FTC's allegations were proven true, the FTC did not sufficiently allege a likelihood of substantial injury.[192] Thus, as mentioned earlier, the FTC filed an amended complaint with detailed factual support for its argument that Kochava's data products directly link precise location data to consumers and cause nontraditional consumer injuries, such as "stigma, discrimination, physical violence, emotional distress, and other harms."[193] A crucial aspect of the argument that these harms are substantially injurious and within the FTC's enforcement authority is the suggestion that this theory of harm is not so different from many harms previously enforced against by the FTC. While I argue in support of this seemingly novel theory of unfairness, it is actually not novel at all. And, as long as the ruling in the case against Kochava does not reverse its progress, the FTC's consent agreement with location data broker X-Mode is now creating new precedent for this theory.

The FTC has broad authority to determine what acts or practices are unfair. However, the FTC often follows their own precedent in recognizing unfairness injuries. Past FTC complaints can therefore be a valuable guide in determining whether a consumer injury resulted from an unfair trade practice. Any expansion on past unfairness complaints can also be justified by the public policy concerns surrounding the issue. The FTC has stated that the public policy surrounding an issue can be "so clear that it will entirely determine the question of consumer injury."[194] Additionally, the FTC nominally considers if the conduct is "immoral, unethical, oppressive, or unscrupulous."[195] So, in analyzing the various injuries and practices that the FTC has considered to be unfair, it is important to consider the various policy and ethical considerations that may have motivated the FTC's decision to enforce their authority, as that, too, can provide guidance on the FTC's unfairness enforcements. And the policy and ethical considerations for the recognition of additional, nontraditional privacy harms go far beyond just the actions of Kochava or X-Mode. As the market for sensitive data grows and political forces continue to undermine personal privacy, the FTC's role as a protector of consumers requires consideration of all privacy harms being caused by commercial entities, not just the financial ones.

190 *See, e.g.*, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (rejecting defendant's argument FTC could not use Section 5 for data security harms); FTC v. Kochava Inc., No. 2:22-cv-377, 2023 WL 3249809, at *1 (D. Idaho May 4, 2023).

191 Kochava Motion to Dismiss, *supra* note 7, at 2, 9-11. Notably, this motion was denied.

192 *Kochava*, 2023 WL 3249809, at *16.

193 Kochava Amended Complaint, *supra* note 54, at 28.

194 FTC Policy Statement on Unfairness, *supra* note 19, at 1075.

195 *Id.* at 1076.

Because of the common-law characteristics of FTC enforcement, FTC unfairness enforcement tends to follow certain trends. These trends and developments have been helpfully outlined and categorized by Solove and Hartzog.[196] Some of these enforcement categories are particularly applicable to the recognition of the unfair harm caused by the sale of location data, and I suggest two additional applicable categories have developed since the publication of their article.

A. *Deceitful Data Collection*

As outlined by Solove and Hartzog, various acts of deceitful data collection have been found to be unfair.[197] For example, the FTC brought an enforcement action in *In re Aspen Way*, stating that a company's installation of spyware and subsequent data gathering without notice was unfair.[198] The FTC deemed surreptitious data gathering to be unfair due to the substantial harm caused by the "invasive surveillance . . . and concerns that '[c]onsumers cannot reasonably avoid [the] injuries'" that are invisible to them.[199] The practice of invasive surveillance that cannot be reasonably avoided being recognized as harmful by the FTC supports FTC enforcement of the unfair sale of location data.

Similar to Aspen Way, data brokers are invasively collecting precise location data in a way that cannot be reasonably avoided. The discrete use of phone apps to surveil people's movements in sensitive locations, or simply at all times, is incredibly invasive. Often, people are unaware that their phones are collecting their precise locations, and so it seems impossible to argue that the practice can be reasonably avoided. The collection of precise location data to be sold is a comparable practice with comparable harms to the various FTC unfairness enforcements against deceitful data collection.

B. *Improper Use of Data*

Another unfairness enforcement category discussed by Solove and Hartzog is the various improper uses of data following collection.[200] Following Aspen Way's deceitful collection of data, the FTC also deemed their use of the data "to

---

[196] Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 640 (contending five categories of unfairness enforcement had emerged at time of article: "(1) retroactive policy changes, (2) deceitful data collection, (3) improper use of data, (4) unfair design, and (5) unfair information security practices").

[197] *Id.* at 641 ("The FTC has also developed a theory that it is an unfair act to collect personal information in a deceitful manner.").

[198] *Id.*; Complaint at 4, Aspen Way Enters., File No. 112-3151, No. C-4392, 155 F.T.C. 483 (Apr. 11, 2013) [hereinafter Aspen Way Complaint], https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415aspenwaycmpt.pdf [https://perma.cc/S95K-PY74] (alleging defendant's business practices constitute unfair gathering of consumers' personal information, unfair data collection, and deceptive gathering of consumers' personal information).

[199] Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 641.

[200] Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 642.

collect a debt, money, or property" improper and thus unfair.[201] Similarly, in *FTC v. Hill*, the FTC alleged that the use of consumer data to "pay for goods or services without the consumers' consent" was an unfair practice.[202] In *FTC v. ReverseAuction.com*, the FTC deemed the practice of collecting personal information and using that information to send spam emails unfair as well.[203] These unfair, improper uses of data are representative of the harm caused when data is used for an improper purpose, or a purpose not explicitly stated it would be used for.

The improper profiting off personal information that occurs when data brokers sell precise location data gathered from apps is an improper use in and of itself, but the intended uses of buyers are often even more improper. Even the reported uses of location data by its purchasers include targeted advertising to people in emergency rooms, the outing and firing of a priest, and the tracking of protestors by the government.[204] The FTC has found using personal information to send spam emails to be unfair, which lends support to the inference that the FTC can also consider unfair the use of precise location data to send antiabortion advertising to clinic patients or personal injury attorney advertising to emergency room visitors.[205]

In a similar yet expanded instance of improper use, the FTC recently alleged the public sharing of personal information of consumers who posted negative Yelp reviews to be unfair.[206] Mortgage Solutions disclosed the financial information and the details of the personal lives of Yelp reviewers in retribution.[207] Interestingly, the FTC explicitly stated that one of the injuries caused by this

[201] Aspen Way Complaint, *supra* note 198, at 4 (alleging unfair practices under Section 5 of FTCA); Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 642.

[202] Complaint for Permanent Injunction and Other Equitable Relief at 12, FTC v. Hill, No. H-03-5537 (S.D. Tex. filed Dec. 3, 2003) [hereinafter Hill Complaint], https://www.ftc.gov/sites/default/files/documents/cases/2004/03/040322cmp0323102.pdf [https://perma.cc/92YB-XDB6] ; Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 642.

[203] Complaint for Permanent Injunction and Other Equitable Relief, FTC v. ReverseAuction.com, No. 00-CV-00032 (D.D.C. filed Jan. 6, 2000) [hereinafter ReverseAuction.com Complaint], https://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversecmp.htm [https://perma.cc/7S8P-QD9R] (holding using eBay customers' email addresses and feedback ratings to target them via spam was improper use of their data); *see also* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 642.

[204] *See* Cox, *supra* note 84; Sherman, *supra* note 89; Allyn, *supra* note 93.

[205] *See* Cox, *Abortion Clinic Data*, *supra* note 84; Sherman, *supra* note 89; Allyn, *supra* note 93.

[206] Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 4-6, FTC v. Mortgage Sols. FCS, Inc., No. 4:20-cv-110 (N.D. Cal. filed Jan. 6, 2020) (asserting defendant improperly disclosed private financial information when posting replies to negative Yelp reviews).

[207] *Id.* at 10.

practice was that other users could read the sensitive data.[208] Thus, this recognition further highlights that harm can be caused when data is improperly used in a way that makes sensitive information available to the public—a practice nearly identical to that of data brokers when they make websites available with massive amounts of precise, sensitive location data.

C. *Targeting Vulnerable Consumer Populations*

I contend that two additional categories of unfair trade practices exist beyond those discussed by Solove and Hartzog in *The FTC and the New Common Law of Privacy*: (1) targeting vulnerable consumers, and (2) distributing to risky third parties. The first of these categories is enforcement against practices that target consumer populations that may be in vulnerable situations. This practice leads to companies manipulating consumers to make decisions contrary to their own interests.

One instance of FTC enforcement against this practice was the FTC's allegation that EMP Media's solicitation and production of revenge porn was an unfair trade practice.[209] EMP Media allowed public access to a person's intimate images and personal information and made the person pay for the images and information to be removed.[210] The FTC outlined the financial harm to consumers, but then went on to outline the possible depression, anxiety, loss of reputation, and safety fears the practice could cause.[211] They also recognized a harm from potential harassment by strangers.[212]

Similarly, the FTC recently brought a complaint against BetterHelp, an app targeting people seeking mental health therapy and counseling, for unfairly failing to employ reasonable privacy practices, which resulted in the disclosure of sensitive health information to numerous third parties.[213] The FTC outlined the injury to consumers from disclosure of highly sensitive information—such as "whether Visitors and Users have previously been in therapy, the fact that they are seeking therapy or in therapy via the Service, and whether their LGBTQ status is affecting their mental health"—as "likely to cause them stigma, embarrassment, and/or emotional distress."[214] These practices and harms seem similar to those of data brokers who collect location data of emergency rooms or Planned Parenthood and then disclose that information. Thus, this category of

[208] *Id.* ("Defendants' actions deprived consumers of the ability to control whether and to whom they disclosed sensitive information.").

[209] Complaint for Permanent Injunction and Other Equitable Relief at 5-6, FTC v. EMP Media Inc., No. 2:18-cv-00035 (D. Nev. filed Jan. 9, 2018) [hereinafter EMP Media Complaint].

[210] *Id.* at 6-12.

[211] *Id.* at 16.

[212] *Id.* at 17.

[213] Complaint at 16, BetterHelp, Inc., No. 2023169 (F.T.C. filed Mar. 2, 2023) (explaining email addresses exchanged with third party allowed for inference person was seeking specific type of medical care).

[214] *Id.*

unfair trade practices seems particularly comparable to the practice of selling location data on certain demographics or certain sensitive locations.

D. *Distributing Monitoring Products and Data to Risky Third Parties*

Another new category of practices that the FTC has recognized as unfair is the distribution of monitoring products or data to risky third parties. This practice creates harm when potentially nefarious parties are granted access to sensitive or personal consumer information.

For example, the FTC brought an action against Support King, LLC (SpyFone.com) for their sale of monitoring products and services.[215] Specifically, the FTC outlined the consumer injury arising from the ability of stalkers and abusers to use their monitoring products to obtain sensitive personal information and monitor people's physical movements.[216] They claimed that monitoring by dangerous parties could lead to emotional abuse, financial and social harm, and physical harm.[217]

Similarly, the FTC deemed Retina-X Studios' sale of monitoring products, which could be installed on devices to monitor them remotely, unfair because the monitoring could be purchased for any purpose.[218] The monitoring products gave any purchaser access to sensitive personal information and the ability to monitor physical movements and online activities.[219] In *Retina-X Studios*, the FTC emphasized the potential for unauthorized parties to perpetuate "mental and emotional abuse, financial and social harm, and physical harm," which can result in depression, anxiety, and safety fears that endure long after the initial victimization.[220]

In *In re Designerware*, the FTC alleged the company's ability to install "Detective Mode" on their licensed computer rentals to gather data on users was unfair.[221] The FTC found that the data gathered was private, confidential, and personal; the software allowed access to the computer's webcam to take photographs; and the software also gathered the physical location of the device.[222] The system would then send that data to the email accounts of its licensees—not the users.[223] The FTC outlined the injury of this practice as the collection and disclosure of personal information to a third party which led to

[215] *See generally* Complaint, Support King, LLC, No. C-4756 (F.T.C. filed Dec. 20, 2021) [hereinafter Support King Complaint].

[216] *Id.* at 5-6.

[217] *Id.*

[218] Complaint at 7, Retina-X Studios, No. C-4711 (F.T.C. filed Oct. 22, 2019) [hereinafter Retina-X Complaint].

[219] *Id.* at 2-3.

[220] *Id.* at 3-4.

[221] Complaint at 6-7, Designerware, LLC, No. C-4390 (F.T.C. filed Apr. 11, 2013) [hereinafter Designerware Complaint].

[222] *Id.* at 2-4.

[223] *Id.* at 6.

the exposure of personal, financial, and medication information to strangers—an "unwarranted invasion into their homes and lives."[224]

The FTC also outlined a relevant harm in their complaint against Vizio for tracking highly specific television viewing behaviors and selling the information.[225] The FTC alleged the harm was that consumers would not expect to be tracked in that context, and Vizio collected and shared sensitive data without consent.[226]

The various mental and emotional harms recognized by the FTC from the distribution of surveillance to risky third parties are directly analogous to the harms caused by the sale of precise location data. The collection and sale of precise location data is a form of surveillance that could, and has been shown to, end up in the hands of parties with questionable or even dangerous intentions.[227] Instances of consumers' location data being acquired by strangers to reveal their sexual orientation, or by employers to reveal medical information, or by potential harassers and stalkers have already occurred.[228] And, as discussed, the chance that this information could now be used to prosecute people seeking medical care only exacerbates the harm.

The scope of precarious parties that could acquire precise location data when it is placed on the open market is vast and will cause the same harms recognized by the FTC here. Precise location data in the wrong hands can lead to awareness of people's presence at sensitive locations by dangerous parties, as outlined in the *Kochava* complaint, and enforcement against this unfair trade practice is justified based on past complaints raised by the FTC.

E. *The Sale of Location Data's Place in FTC Unfairness Enforcement*

As these four categories of FTC unfairness enforcement reflect, the FTC's theory of the unfairness of the sale of location data is not novel.[229] FTC enforcement, and other legal precedent, supports the theory that the sale of precise location data causes numerous harms and substantial injuries which the FTC has the ability to enforce against.[230] The commercialization of location data has resulted in data sets designed to track people to medical facilities, antiabortion messages sent to abortion clinic visitors, personal injury lawyer

[224] *Id.* at 5.

[225] Complaint at 7-9, FTC v. Vizio, Inc., No. 2:17-cv-00758 (D.N.J. filed Feb. 6, 2017) [hereinafter Vizio Complaint].

[226] *Id.* (noting consumers are unlikely to suspect their screen data would be recorded and stored).

[227] *See* Retina-X Complaint, *supra* note 218, at 2-3.

[228] *See* Cox, *supra* note 84; Sherman, *supra* note 89; Allyn, *supra* note 93; Cox, *Weaponization of App Data*, *supra* note 106; Cox, *Woman Stalked with Black Market Location Data*, *supra* note 115; Cox, *U.S. Military Buys Location Data*, *supra* note 126; Cagle, *supra* note 142; Tewari & Walter-Johnson, *supra* note 137.

[229] Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 640.

[230] *See, e.g.*, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 610 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

advertisements sent to emergency room patients, reveal of the location and layout of military bases, the public outing of a priest, harassment of families by strangers, targeted tracking of Muslims, monitoring of protestors by law enforcement, and surveillance of immigrants.[231] Notably, even this long list of harms caused by the sale of location data only includes harms uncovered and reported on by public interest or media organizations. It follows that there are inevitably even more harms that have already been caused by the sale of location data.

The FTC has recognized that invasive surveillance consumers cannot reasonably avoid is a substantial injury.[232] Similarly, the collection and distribution of a person's precise movements is therefore harmful and unfair because it is invasive surveillance a person cannot reasonably avoid so long as they use a cell phone.

The FTC has recognized that using data for improper purposes, such as sending spam emails, causes substantial injury.[233] Similarly, the use of apps to collect precise location data and then sell it for profit—including to then send antiabortion or attorney advertising to people in sensitive locations—is thus harmful and unfair because of how it reveals such sensitive information for improper and often unknown purposes.

The FTC has recognized the substantial injuries of depression, anxiety, loss of reputation, and safety fears that result from trade practices that target vulnerable consumers to be unfair.[234] Similarly, the sale of location data of certain populations—such as immigrants, Muslims, or pregnant people—to law enforcement or employers is thus harmful and unfair because of the anxiety, safety fears, and potential harassment and discrimination that may result. Not to mention the fact that the harms caused by commercial surveillance disproportionately affect disadvantaged communities.[235]

The FTC has recognized the substantial injuries of emotional abuse, physical harm, social harm, anxiety and safety fears following stalking or abuse, and unwarranted invasions into a person's life that result from distributing

[231] *See* Cox, *Abortion Clinic Data*, *supra* note 84; Sherman, *supra* note 89; Allyn, *supra* note 93; Hern, *supra* note 96; Cox, *Inevitable Weaponization of App Data*, *supra* note 106; Cox, *Woman Stalked with Black Market Location Data*, *supra* note 115; Cox, *U.S. Military Buys Location Data*, *supra* note 126; Cagle, *supra* note 142; Tewari & Walter-Johnson, *supra* note 137.

[232] *See* Aspen Way Complaint, *supra* note 198, at 2 ("Consumers cannot reasonably avoid these injuries because Detective Mode is invisible to them.").

[233] *See, e.g.*, ReverseAuction.com Complaint, *supra* note 203.

[234] *See* Complaint for Permanent Injunction and Other Equitable Relief at 6, FTC v. GDP Network LLC, No. 6:20-cv-1192-78 (M.D. Fla. filed July 16, 2020) [hereinafter GDP Network Complaint]; EMP Media Complaint, *supra* note 209, at 5-6.

[235] Letter from Ctr. for Democracy and Tech., Ctr. on Priv. & Tech. at Georgetown L., Consumer Action, Consumer Reports, Demand Progress Educ. Fund, EPIC, Just Futures L., Mijente, Nat'l Consumer L. Ctr. & U.S. PIRG to Rohit Chopra, Director of CFPB (Feb. 8, 2023), https://epic.org/wp-content/uploads/2023/02/2023-02-08-Coalition-Letter-to-CFPB.pdf [https://perma.cc/7A7W-BVXK].

monitoring devices or data to precarious third parties.[236] Similarly, the sale of precise location data that can be used to track a person's every movement to any willing buyer is thus harmful and unfair because of the physical harm that could result from a stalker obtaining the precise location of a person, the emotional abuse that could result from receiving targeted antiabortion messages while in a clinic, or the unwarranted invasion of privacy that results every time a person's precise movements are purchased off the internet.

Notably, the FTC's complaint against X-Mode raised at least two of these categories of enforcement as reasons why X-Mode's location data sales injured consumers and were unfair.[237] The FTC stated that X-Mode "[t]argeted [c]onsumers [b]ased on [s]ensitive [c]haracteristics," and sold location data to third parties "who violated contractual restrictions limiting the resale of such data" with "little or no control over downstream uses" of the data.[238] The FTC's inclusion of targeting vulnerable parties and selling to risky third parties as unfair practices by a location data broker further affirms how FTC precedent can inform enforcement actions against the sale of location data.

As the FTC's history and other legal doctrines show, an expanded conceptualization of consumer harm for Section 5 enforcement is not without support. One of the FTC's strengths is its broad authority to interpret unfairness, and an expanded scope of injury interpretation by the FTC would afford broad privacy protections to consumers. Further, historical and legal support exist for the idea that the sale of location data is substantially likely to lead to injury. The substantial injury recognized from the sale of location data may not always include traditional physical or financial injury, but the emotional, mental, or privacy harms should be recognizable as unfair nonetheless. The sale of location data almost never causes financial harm to consumers, and thus some may argue that the FTC cannot enforce against the practice without a recognizable substantial injury. However, an expanded recognition of the intangible harms resulting from the sale of location data and comparison to legal doctrines and previous FTC enforcement actions demonstrate that the FTC can enforce against such harms because they do cause substantial injury.

While this Note focuses on the expansion of FTC substantial injury to include the harms caused by the sale of location data, the expansion of substantial injury can be applied to encourage the FTC's recognition of a wide array of privacy violations and harms that are often hard to conceptualize in traditional terms. As the number of privacy invasions grow, agencies equipped to protect consumers against them cannot shrink or even stay stagnant. The expansion of substantial consumer injury interpretation is supported, and it is necessary.

[236] *See* Support King Complaint, *supra* note 215, at 5; Retina-X Complaint, *supra* note 218, at 2-3; Designerware Complaint, *supra* note 221, at 2-4; Vizio Complaint, *supra* note 225, at 4-6.

[237] *See* X-Mode Social Complaint, *supra* note 60, at 7-8.

[238] *Id.*

CONCLUSION

The FTC has the ability to protect consumers from a wide array of privacy violations through its Section 5 powers, and it has signaled its intention to do so on numerous occasions.[239] The recent FTC complaint against Kochava signaled a significant expansion of the Agency's Section 5 powers, and the subsequent consent agreement with X-Mode demonstrated the FTC's interest in continuing that progress.[240] Yet, this expansion is not significant because it is novel or outrageous, but rather because it aims to break through the gatekeeping of privacy violations to recognize them for the true harm they cause to consumers. Rather than find a way to fit the substantial injuries caused by privacy violations into physical or financial boxes, the FTC is attempting to recognize the mental, emotional, and other intangible injuries caused by the violation of consumers' privacies. And legal doctrine and prior FTC enforcement support this choice.

The privacy violation of the sale of location data has already created vast real-world consequences, as exemplified above. These consequences can be linked to various legal doctrines' recognitions of similar incorporeal or nonfinancial harms. Further, past FTC unfairness enforcements show that an expanded conceptualization of substantial injury should not be a surprise, as many actions have been signaling this shift. The FTC has previously alleged that practices resulting in invasive surveillance, risky third-party use of personal information, or targeting of vulnerable populations are unfair because of various nontraditional harms.[241] The sale of location data has already been shown to result in those same harms, so to explicitly state those harms as sufficient to create an unfair trade practice even without financial harm is not outside the realm of the FTC's power.[242]

Further, the FTC's recognition of the harms from the sale of location data will have a protective effect far beyond just *Kochava* or its Section 5 powers.[243] An expanded enforcement scheme for the FTC also takes on an expressive character, in that it can work to reshape for-profit companies' privacy practices.[244] The FTC's addition of new privacy harms to its common law of enforcement will have rippling effects on the privacy practices of any company that considers invading consumers privacy in a way that will result in these harms. More importantly, what message would it send to continue to say that

[239] Hartzog & Solove, *The Scope and Potential of FTC Data Protection*, *supra* note 30, at 2232.

[240] *See* Kochava Complaint, *supra* note 5, at 1.

[241] Hartzog & Solove, *The Scope and Potential of FTC Data Protection*, *supra* note 30, at 2232; GDP Network Complaint, *supra* note 234, at 6.

[242] Hartzog & Solove, *The Scope and Potential of FTC Data Protection*, *supra* note 30, at 2280.

[243] Solove & Hartzog, *New Common Law of Privacy*, *supra* note 8, at 622-23 (highlighting how common law nature of FTC enforcement actions leads to FTC's publicized orders being relied upon by community of practitioners).

[244] Citron & Solove, *Privacy Harms*, *supra* note 12, at 828; *see* Solove & Hartzog, *FTC and the New Common Law of Privacy*, *supra* note 8, at 621-22.

these privacy violations do no recognizable harm? If we were to continue to ignore the harm done by privacy violations or reframe the harm to say that financial impact is the only real, important interest, then privacy harms will continue to go unrecognized and thus unchecked.