Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of

Request for Investigation of Alleged Violations of Section 5 of the FTC Act by Multiple Actors in the Location Data Industry

The Council on American-Islamic Relations

Laura M. Moy*
Communications & Technology Law Clinic
Georgetown University Law Center
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9547

Counsel for the Council on American-Islamic Relations

via electronic filing

April 12, 2022

* This request for investigation was drafted with considerable assistance from student attorneys Monty Roberson, Pariss Briggs, Philip Robbins, Luke Evans, and Quinten Stewart, and teaching fellow Victoria Tang in the Communications & Technology Law Clinic at Georgetown Law.

Table of Contents

BACKGROUND AND SUMMARY

The Council on American-Islamic Relations (CAIR), through its counsel, the Communications & Technology Law Clinic at Georgetown University Law Center, respectfully requests the Federal Trade Commission (FTC) investigate and enforce potential violations of Section 5 of the Federal Trade Commission Act across the location data industry.

Researchers and journalists have documented a pattern of deceptive practices aimed at monetizing the special value of location data that is specific to the Muslim community.[1] This location data has special value because it facilitates warrantless surveillance of individuals historically targeted by law enforcement, the intelligence community, and the military. In 2020, for example, the U.S. Special Operations Command admitted to purchasing the location data of users of a popular Muslim prayer app, Muslim Pro, and a Muslim dating app, Muslim Mingle.[2] And just last week, on April 6, 2022, researchers identified a defense contractor's "alternative monetization strategy" that appears to be premised on the special value governments assign to information about the religious beliefs and practices of Muslims.[3]

Location tracking has had a disproportionate harmful impact on American Muslims, limiting both their First Amendment activity and their consumer choice. Given hyper-surveillance concerns, deceptive practices that have been adopted by many apps used by American Muslims chill the practice of religion and freedom of assembly, rights so fundamental they are protected by the First Amendment. Revelations that some of the most popular apps among Muslims were sharing their location data with defense contractors and the military compounded a sense of constant surveillance inside the Muslim community, leading many American Muslims to either stop using apps or take other steps to avoid the deceptive practices.

Different actors and practices within the industry play a role in the unfettered collection and dissemination of location data, contributing to these harms. The industry includes the following actors: operating system developers ("operating systems"), app developers, software development kit (SDK) developers,[4] various participants

---

[1] Byron Tau & Robert McMillan, *Google Bans Apps With Hidden Data-Harvesting Software*, Wall St. J. (Apr. 6, 2022), https://www.wsj.com/articles/apps-with-hidden-data-harvesting-software-are-banned-by-google-11649261181 [https://perma.cc/43H3-9CCT].

[2] Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x [https://perma.cc/G98R-G6QS].

[3] Joel Reardon, *The Curious Case of Coulus Coelib*, AppCensus Blog (Apr. 6, 2022), https://blog.appcensus.io/2022/04/06/the-curious-case-of-coulus-coelib/ [https://perma.cc/26S4-TSAV].

[4] A software development kit (SDK) is a pre-made package of tools designed to enhance app functionality. Operating systems and third parties offer SDKs to help app developers build their

contributing to the real-time bidding (RTB) process,[5] and data brokers.[6] These actors often operate in secrecy, taking away consumers' control over their data. Operating systems and app developers often fail to provide adequate disclosure or obtain affirmative express consent for sharing location data. Worse, sometimes they share location data even when users opt out. SDK developers create location-tracking SDKs, which are pre-packaged bits of code that can be integrated into an app, without disclosing their full functionality to app developers. In turn, app developers create apps without full knowledge of their functionality, leaving consumers in the dark about their data being harvested and shared. The RTB process is confusing and allows nefarious participants, such as lurking data brokers, to acquire significant amounts of data without consumers knowing.

This request for investigation calls on the FTC to rein in the barrage of collection and dissemination of consumers' location data as it occurs through two practices. First, location data is often collected through apps, even when such data is unnecessary for the app to function. Then that data may be shared in two ways: the app provides the data directly to third parties, or a third party collects the data on its own through its location-tracking SDK already embedded in the app. Data collected in this manner frequently ends up in the hands of data brokers, who sell the data to additional parties. Second, location data is often collected by participants in the online advertising RTB process. Up to hundreds of times each day, a device's location data is paired with the device's unique advertising identifier and incorporated into a bid request shared with thousands of real-time bidders hoping to place an ad on a website or app being viewed on that device. Data brokers, who have no intention to win ad space, lurk among actual

---

apps and add certain features like maps, login portals, and more. *See* Kaveh Waddell, *Some Developers Don't Know What Their Apps Do with Your Data. Here's Why.*, Consumer Reports (Mar. 13, 2020), https://www.consumerreports.org/privacy/developers-dont-know-what-their-apps-do-with-your-data-a1055672912/ [https://perma.cc/Q5LJ-4KF6].

[5] The real-time bidding (RTB) process refers to the buying and selling of ad space in real-time, typically through an open auction. The entire process occurs in milliseconds: 1) the consumer opens a website (or app content); 2) as the website loads, the auction starts; 3) advertisers place bids for the available ad space on the website; 4) the highest bidder wins; 5) the winning advertiser gets to display their ad in the ad space. *See* Info. Comm'r's Office, Update Report into Adtech and Real Time Bidding 10–11 (June 20, 2019) ("RTB Report"), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

[6] In September 2021, The Markup identified 47 companies that harvest, sell, or trade in mobile phone location data, but this list only represents a sliver of the full pie. Jon Keegan & Alfred Ng, *There's a Multibillion-dollar Market for Your Phone's Location Data*, The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data [https://perma.cc/EU4C-24P3].

bidders to harvest location data to sell to additional parties.[7] Both of these troubling practices thrive because it is essentially impossible for consumers to entirely eliminate location tracking of their mobile devices.

Unless the FTC takes action, consumers will continually be subjected to harmful surreptitious collection and unconsented dissemination of their location data. Few state or federal laws adequately protect individuals' personal data, including information about their whereabouts.[8] Already valued at $12 billion, the location data industry market size is expected to grow to over $25.2 billion by 2027.[9] Without sufficient guardrails, the location data industry will chart its own path forward without regard to geographic privacy.

The FTC is the only federal agency with sufficient authority to rein in the troubling practices of numerous actors in the location data industry. The FTC should use its authorities, including by bringing enforcement actions and issuing warning letters, notices, and rules, to combat the unfair and deceptive practices of the data location industry. If necessary to better understand opaque areas of the industry, the FTC should conduct 6(b) investigations to determine which actors are harming consumers and release any information that would be beneficial to the public.

INTEREST OF COMPLAINANT

Established in 1994, the Council on American-Islamic Relations is a nonprofit organization dedicated to protecting American Muslims' civil rights through advocacy, education, and media relations. CAIR is America's largest Muslim civil liberties organization with offices throughout the country and a national headquarters in Washington, D.C. Since its founding, CAIR has worked to promote a positive image of Islam and Muslims in American. Through media relations, lobbying, education, and

---

[7] *See* James Hercher, *Everything You Need to Know About the Bidstream*, AdExchanger (Mar. 7, 2019), https://www.adexchanger.com/online-advertising/everything-you-need-to-know-about-the-bidstream/ [https://perma.cc/64KC-BF2T]. Data brokers tout their ability to conduct remarkably specific profiling of consumers into groups like "Rural and Barely Making It" or "Ethnic Second-City Strugglers." Justin Sherman, *Data Brokers Are a Threat to Democracy*, Wired (Apr. 13, 2021), https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/ [https://perma.cc/32ZJ-PN4K].

[8] For example, only four states have enacted comprehensive consumer privacy legislation, and there is no comprehensive federal law. *See* Taylor Kay Lively, *US State Privacy Legislation Tracker*, IAPP (Mar. 31, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/6332-S8VH].

[9] Grand View Research, Location Intelligence Market Size, Share & Trends Analysis Report By Application (Sales & Marketing Optimization, Remote Monitoring), By Service (Consulting, System Integration), By Vertical, And Segment Forecasts, 2020 - 2027 (Feb. 2020), https://www.grandviewresearch.com/industry-analysis/location-intelligence-market [https://perma.cc/DR4D-BY8J].

advocacy, CAIR defends the rights of American Muslims. In the fight for those rights, CAIR recognizes the history of harm and oppression of the American Muslim community. Since 9/11, one major harm to American Muslims is unwarranted surveillance by law enforcement, which has been facilitated by individuals' location data. Given the detrimental and prejudicial nature of this practice, CAIR is concerned about the unchecked location data industry.

ARGUMENT

I. The location data industry is rife with deception.

There is widespread consumer deception in location data industry. Under Section 5 of the FTC Act, a deceptive practice is (A) a representation, omission, or practice that is likely to mislead (B) a consumer acting reasonably in the circumstances and (C) is material.[10] The collection and dissemination of individuals' location data without proper notice and consent satisfies all of these elements and thus violates Section 5.

A. The location data industry thrives by engaging in practices likely to mislead consumers, including making misrepresentations and omissions.

The first part of a Section 5 deception analysis examines whether there is a representation, omission, or practice that is likely to mislead the consumer. Outright misrepresentations and omissions in location data disclosures mislead consumers, particularly in the case of advertising identifiers. Hidden or confusing disclosures are deceiving too. And even when disclosures appear to be satisfactory, another type of misrepresentation occurs when actors falsely claim that they only collect or maintain anonymous location data, when in fact the data they maintain can easily be linked to an individual. With these specious practices, consumers are often unaware of the rampant collection and dissemination of their location data; but upon discovery, their shock and outrage illustrate that they were misled.

Misrepresentations and omissions in location data disclosures mislead consumers. The FTC has stated that because precise location data is sensitive, it can be collected and disseminated only if those practices are disclosed to consumers who provide affirmative express consent.[11] Disclosure must be clear and prominent for it to

---

[10] 15 U.S.C. § 45; *FTC Statement on Deception*, 103 F.T.C. 174, 175 (1984) ("*Deception Policy Statement*").

[11] FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change 47 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/

be adequate.[12] Affirmative express consent requires "a clear and conspicuous mechanism" for the consumer to indicate their assent.[13] But these requirements are frequently disregarded. One prominent example of how misleading disclosures tricked consumers was Google's use of advertising identifiers, each tied to a specific Android device to make it easy for companies to track users.[14] Google had claimed that users could opt out of tracking and personalized advertising when using apps, but companies still received the advertising identifiers, allowing them to obtain more information about users to build profiles for targeting.[15]

Location data disclosures often are hidden, misleading consumers. When there is disclosure, it is often buried in a lengthy, complex, or vague privacy policy that is difficult to find. For instance, only 0.55% to 6.7% of subscribers to large Internet Service Providers (ISPs), which collect and sell location data,[16] visit their ISPs' privacy pages.[17] This is likely because these pages are hidden beneath multiple sub-pages and labeled ambiguously. A recent FTC investigation found that one ISP forced users seeking to change privacy settings to click through four different pages before taking them to a page with six different settings categories, none of which explicitly referenced privacy.[18]

120326privacyreport.pdf [https://perma.cc/X4YR-TG6V]; FTC Staff Report, Mobile Privacy Disclosures: Building Trust Through Transparency 15 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [https://perma.cc/B5GC-8H58].

[12] *See* FTC Staff Report, .com Disclosures: How to Make Effective Disclosures in Digital Advertising iii (Mar. 2013), https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf [https://perma.cc/D5YD-4Y92].

[13] *Lenovo, Inc.*, No. C-4636 F.T.C. 3 (Sept. 13, 2017), https://www.ftc.gov/system/files/documents/cases/152_3134_c4636_lenovo_united_states_decision_and_order.pdf [https://perma.cc/C32Y-VZES].

[14] Megan Graham, *Google Follows Apple's Lead and Makes It Harder for Advertisers to Track Users On Android*, CNBC (June 3, 2021), https://www.cnbc.com/2021/06/03/google-will-restrict-use-of-android-advertising-id-to-opted-in-users-.html [https://perma.cc/X93D-THCH].

[15] James Hercher, *Google Tightens 'Limit Ad Tracking' Policies for Android Ad ID*, AdExchanger (June 2, 2021), https://www.adexchanger.com/mobile/google-tightens-limit-ad-tracking-policies-for-android-ad-id/ [https://perma.cc/5D53-GMYU]. Google changed this practice only last year; and although Google now allows Android users to actually opt out of location-targeted personalized ads, it does not prompt users to take advantage of this option. *Id.*

[16] *See* FTC Staff Report, A Look at What ISPs Know About You 25, 36–37 (Oct. 21, 2021), https://www.ftc.gov/news-events/blogs/business-blog/2021/10/look-what-isps-know-about-you-must-read-report-ftc [https://perma.cc/DA3Z-R8UA].

[17] *Id.* at 27.

[18] *Id.* at 30.

Location data disclosures also mislead consumers with confusing language. To be adequate, disclosure must be in understandable language and syntax.[19] A persistent consumer may be able to find a privacy policy, but it often will be lengthy, confusing, or vague. For example, one family location-tracking app's policy is over 11,000 words with meandering, complicated sentences.[20] At the other end of the spectrum, Muslim Mingle has only a cursory and vague explanation of its use of location data: "We may use your location to show you tips when you're in participating location venues, and we may share this information with our trusted partners."[21] This policy neither describes the concept of "participating location venues" nor lists any "trusted partners."[22]

Another type of misrepresentation occurs when promises of anonymous location data turn out to be false, especially in this age of big data where an individual's identity can be easily discerned through cross-referencing with just a few additional datapoints. For example, in one recent analysis of the location data industry, 75 companies claimed to have received "anonymous" location data from users had who enabled location services on their phones only to get geographically-relevant information.[23] But the "anonymous" location data was easily linked to specific individuals. For example, researchers were able to discover the identity of one user, a teacher named Lisa Magrin, because she was the only person who made the trip from a specific house to the middle

---

[19] .com Disclosures, *supra* note 12.

[20] *See Full Privacy Policy*, Life360 (last visited Feb. 18, 2022), https://support.life360.com/hc/en-us/articles/ 360043228154. One section reads: "We may share information about your use of our Services over time, including location information, with third party ad networks, social media companies and other third parties so that they may play or display ads that may be relevant to your interests on our Service as well as on other websites, apps or services, or on other devices or advertising channels . . . . These third party ad partners collect and use information such as click stream information, timestamp, hashed email address, device ID or AdID, your use of third party applications and/or precise geolocation data and other information, and may combine this information with information they collect directly through tracking technologies or that they receive other partners, both online and offline, so that they may recognize you across other browsers or devices you use, including computers, mobile devices and Smart TVs." After public reports exposing its relationships with up to a dozen data brokers, Life360 recently announced that it will "phase out" of selling precise location data. Jon Keegan & Alfred Ng, *Life360 Says It Will Stop Selling Precise Location Data*, The Markup (Jan. 27, 2022), https://themarkup.org/privacy/2022/01/27/life360-says-it-will-stop-selling-precise-location-data [https://perma.cc/C7N7-EN8R]. However, it still sells aggregated location data to data brokers, and still sells precise location information to a company affiliated with Allstate that measures traffic patterns. *Id.*

[21] *Privacy Policy*, Muslim Mingle (last visited Feb. 18, 2022), https://muslim.mingle.com/privacy/#data-collection [https://perma.cc/F76H-SJNK].

[22] *See id.*

[23] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 18, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/72LB-FFMQ].

school where she worked each weekday.[24] Indeed, it has long been known to researchers that the majority of individuals can be identified from just a few datapoints indicating both location and time.[25]

The shock and outrage expressed by consumers once they learn their location data has been provided to third parties confirms they have been misled by the disclosures. When shown the analysis above, the teacher was shocked that her location data was recorded and shared so frequently without her knowledge. She voiced concern over the "thought of people finding out those intimate details you don't want people to know."[26] Furthermore, news reports of unexpected collection and dissemination of location data seem to come out almost every week, and each time consumers themselves state that they were confused and duped about their lack of location privacy. Following the revelation that prayer app Muslim Pro was sharing users' location data to third parties, San Francisco CAIR Executive Director Zahra Billoo called it a betrayal: "People feel that they should have been able to trust a [Muslim-centric] company . . . to keep that data private, to be incredibly diligent about who they were selling it to, if they would sell it at all." Lawsuits brought by consumers, cities, and states regarding location practices further demonstrate how people widely feel misled due to the lack of adequate disclosure and consent.[27]

B. Consumers acting reasonably to safeguard their location data are misled when industry actors conceal their inner-workings and ignore consumers' decisions to opt out.

The second part of a deception analysis considers a practice from the perspective of a consumer acting reasonably in the circumstances. The FTC should consider that mobile device users lack deep technical understanding of the location data ecosystem,

---

[24] *Id.*

[25] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 Scientific Reports 1376 (Mar. 25, 2013), https://www.nature.com/articles/srep01376 [https://perma.cc/TN6A-YHVT] (finding that "in a dataset where the location of an individual is specified hourly and with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals").

[26] Valentino-DeVries et al., *supra* note 23.

[27] Los Angeles settled a lawsuit with The Weather Channel and IBM after the city alleged that the weather app deceived consumers about their data collection and sharing practices. The Weather Channel and IBM agreed to revise their disclosures and ensure transparency for and to obtain informed consent of their users. Taylor Lyles, *Los Angeles Settles Weather Channel Lawsuit, Lets It Keep Selling Location Data to Advertisers*, The Verge (Aug. 19, 2020), https://www.theverge.com/2020/8/19/21376217/los-angeles-the-weather-channel-app-lawsuit-settlement-location-data-selling. *See also* Joseph Cox, *Google Faces Class Action for Allegedly "Selling Users' Data*," Vice (Mar. 29, 2021), https://www.vice.com/en/article/93we9z/google-class-action-lawsuit-real-time-bidding-selling-data [https://perma.cc/9H7E-AKUU].

pseudonymous location data can easily be reidentified, and actors in the ecosystem may disregard consumers' express choices.

The average mobile device user may be aware that some type of location data collection occurs but have no knowledge of exactly where, why, and how that data is disseminated because the location information ecosystem is technically complex and, as discussed above, privacy policies frequently are hidden, misleading, or confusing. For example, RTB affects every mobile device user, but its lack of transparency makes it difficult for the average consumer to understand how the current RTB infrastructure allows their location data to be harvested.[28] Yet consumers view location data as sensitive information, so they would not expect it to be disseminated widely without their express permission.[29]

Even when consumers are aware that they have shared their location data in some context, they typically are not able to understand how invasive the collection and use of that data can be. As the Supreme Court noted in the landmark location privacy case *Carpenter v. United States*, time-stamped location data "provides an intimate window into a person's life, revealing not only [their] particular movements, but through them [their] familial, political, professional, religious, and sexual associations. These location records hold for many Americans the 'privacies of life.'"[30] It is, in fact, relatively easy for a sophisticated data analyst to reidentify individual users and mine valuable details of their private lives from location data.[31] And as discussed above, this is often the case even in location data misleadingly claimed to be "anonymous."[32]

In addition, consumers acting reasonably under the circumstances may believe they have taken steps to protect their location data, and have no way of knowing that their expressed preferences will be disregarded. Some location data industry actors mislead consumers into believing they can opt out of tracking, but then fail to respect the consumer's decision.[33] For example, Google permits Android users to opt out of personalized ads. But until recently, even after users selected this option, their advertising identifiers remained accessible, which allowed developers to measure app

---

[28] *See* RTB Report, *supra* note 5, at 23.
[29] Lee Rainie & Maeve Duggan, Pew, Privacy and Information Sharing 5 (Jan. 14, 2016), https://www.pewresearch.org/wp-content/uploads/sites/9/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf [https://perma.cc/PD5W-K9NN].
[30] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (internal quotations omitted).
[31] *See, e.g.*, de Montjoye et al., *supra* note 25.
[32] *See* Sara Harrison, *When Is Anonymous Not Really Anonymous?*, The Markup (Mar. 24, 2020), https://themarkup.org/ask-the-markup/2020/03/24/when-is-anonymous-not-really-anonymous [https://perma.cc/6Z9M-NAED].
[33] Joseph Cox, *Location Data Firm Got GPS Data from Apps Even When People Opted Out*, Vice (Oct. 25, 2021), https://www.vice.com/en/article/5dgmqz/huq-location-data-opt-out-no-consent [https://perma.cc/7UVT-WDCT].

usage and advertisers to detect invalid traffic.[34] Consumers acting reasonably in choosing to opt out were misled because that choice was actually ignored.

C. The representations, omissions, and practices of the location data industry are material because consumers would otherwise make different choices to avoid the detrimental effects from the collection and dissemination of location data.

The widespread deceptive practices by multiple actors in the location data industry are material because consumers care deeply about the privacy of their location data and rely on their understanding of location privacy to make choices about whether and how to use apps and services.

Studies and surveys have consistently shown that consumers place a high value on their location privacy. For example, research conducted by an online security company found that the majority of mobile device users who are on social media with geolocation enabled are concerned about their privacy.[35] A 2014 Pew Research Center survey found that 82%of respondents considered details of their physical location to be sensitive information.[36] Based on another survey and focus groups, Pew reported in 2016, "[l]ocation data seems especially precious in the age of the smartphone. Some of the most strongly negative reactions [from respondents] came in response to scenarios involving the sharing of personal location data."[37]

In addition, consumers have repeatedly demonstrated that they would make deliberate choices in their use of mobile devices and apps to avoid the harms stemming from location tracking. For example, after a news story revealed that the U.S. military purchased location data of Muslim Pro users, thousands condemned the app across social media, with many deleting the app in protest and promoting alternatives.[38] In

---

[34] Graham, *supra* note 14. In contrast, Apple's App Tracking Transparency (ATT) gives users the opportunity to opt out when first downloading the app, replacing the advertising identifier with a non-unique string of all zeros to prevent targeted ads. *Id.*

[35] *Webroot Survey Finds Geolocation Apps Prevalent Amongst Mobile Device Users, but 55% Concerned About Loss of Privacy*, PR Newswire (July 13, 2010), https://www.prnewswire.com/news-releases/webroot-survey-finds-geolocation-apps-prevalent-amongst-mobile-device-users-but-55-concerned-about-loss-of-privacy-98300449.html [https://perma.cc/8QHW-RT35].

[36] Mary Madden, Pew, Americans Consider Certain Kinds of Data to be More Sensitive than Others (Nov. 12, 2014), https://www.pewresearch.org/internet/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/ [https://perma.cc/Q39D-CFQV] (50% described as "very sensitive" and 32% described as "somewhat sensitive.").

[37] Rainie & Duggan, *supra* note 29.

[38] Johana Bhuyian, *Muslims Reel Over a Prayer App that Sold User Data: 'A Betrayal from Within Our Own Community'*, L.A. Times (Nov. 23, 2020), https://www.latimes.com/business/technology/story/2020-11-23/muslim-pro-data-location-sales-military-contractors [https://perma.cc/5AAR-EGXV]. One tweet read, "This is horrifying, violent and traumatic for so many reasons. This should concern EVERYONE, not just Muslims." Dr. Mama Kam

fact, a leadership council representing 90 New York State mosques sent a notification urging its constituents to delete the app.[39] If American Muslims had this information upfront, many would have decided not to download the app in the first place. Generally, consumers value having control over their own data, feeling particularly strongly that location data privacy is important.[40] A common reason users cite for their preference of Apple devices over Google devices is the former's enhanced privacy protections, including for location information.[41] Such deliberate consumer action to select less harmful alternatives underscores materiality.

II. The location data industry is rife with unfairness.

In addition to widespread deception, the location data industry is rife with unfairness. Under Section 5 of the FTC Act, a practice is unfair if it (A) causes or is likely to cause substantial injury to consumers that is (B) not reasonably avoidable by consumers themselves, and (C) not outweighed by countervailing benefits to consumers or to competition.[42] The current practices of the location data industry satisfy all of these elements and thus violate Section 5.

A. Location data industry practices cause substantial injury to consumers, with a disproportionately harmful impact on historically hyper-surveilled communities.

The first part of a Section 5 unfairness analysis looks at whether a practice causes or is likely to cause substantial injury to consumers.[43] Location data contains sensitive details of individuals' lives that can cause various harms when revealed. It also facilitates harmful discriminatory advertising. Furthermore, unchecked collection and dissemination of location data has had a disproportionate impact on communities already subjected to hyper-surveillance by law enforcement. One affected community is American Muslims, who have also suffered substantial injuries related to limitations on both their First Amendment rights and consumer choices.

(@KameelahRashad), Twitter (Nov. 19, 2020, 7:46 PM), https://twitter.com/KameelahRashad/status/1329586947849932800 [https://perma.cc/2WK7-7RY8].

[39] Bhuyian, *supra* note 38.

[40] Rainie & Duggan, *supra* note 29.

[41] *See* Abhin Mahipal, *Report: Brand Loyalty at an All-Time High of 92% for Apple as Android Brands Take a Dive*, SellCell (Mar. 16, 2021), https://www.sellcell.com/blog/cell-phone-brand-loyalty-2021/ [https://perma.cc/4Z79-Q88K].

[42] 15 U.S.C. § 45(n); *FTC Policy Statement on Unfairness*, 104 F.T.C. 949, 1070 (1984) ("*Unfairness Policy Statement*").

[43] *Id.*

Because location data reveals sensitive details of people's lives, its unfettered collection and use are likely to lead to substantial injury.[44] As Senator Wyden has observed, an individual's whereabouts "can reveal some of the most intimate details of a person's life—whether you've visited a psychiatrist, whether you went to an A.A. meeting, who you might date."[45] Moreover, the FCC noted that information about a wireless customer's location is "highly personal and sensitive,"[46] and the NSA concluded that "location data can be extremely valuable and must be protected."[47] This means that misuse of location data is sought after by numerous bad actors who can cause a range of harms. For example, a few years ago it was revealed that stalkers and debt collectors exploit leaks in the location data ecosystem to track their targets.[48] More recently, "anonymous" location data from a gay dating app was sold and linked to a Catholic priest who was forced to resign because he was outed.[49] Without the use of location data, this injury likely would not have happened.

Even when it is not accessed by malicious actors, location data frequently facilitates harmful and discriminatory targeted pricing and advertising—harms that fall disproportionately on historically disadvantaged communities like American Muslims. For example, for years it has been known that sites adjust their prices based on users' location data.[50] Sometimes location-based targeting appears to be racially discriminatory, such as the Princeton Review practice, exposed by a ProPublica investigation, of charging higher prices for SAT test prep to consumers in ZIP codes

---

[44] *See* FTC Press Release, FTC Testifies on Geolocation Privacy, (June 4, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/06/ftc-testifies-geolocation-privacy [https://perma.cc/4R6F-EXKB].

[45] Valentino-DeVries, et. al, *supra* note 23.

[46] *T-Mobile USA, Inc.*, 35 FCCR 1785 (2020), https://www.fcc.gov/document/fcc-proposes-916m-fine-against-t-mobile-location-information-case [https://perma.cc/6SR9-WCRL].

[47] NSA, Limiting Location Data Exposure 1 (Aug. 2020), https://media.defense.gov/2021/Sep/16/2002855924/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF [https://perma.cc/V5V3-UHVE].

[48] *See* Joseph Cox, *Stalkers and Debt Collectors Impersonate Cops to Trick Big Telecom into Giving Them Cell Phone Location Data*, Vice (Mar. 6, 2019), https://www.vice.com/en/article/panvkz/stalkers-debt-collectors-bounty-hunters-impersonate-cops-phone-location-data [https://perma.cc/RG3W-FAG7].

[49] Sara Morrison, *This Outed Priest's Story As a Warning for Everyone About the Need for Data Privacy Laws*, Vox (July 21, 2021), https://www.vox.com/recode/22587248/grindr-app-location-data-outed-priest-jeffrey-burrill-pillar-data-harvesting [https://perma.cc/KPZ8-C8XX].

[50] Jennifer Valentino-DeVries, Jeremy Singer-Vine & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, Wall St. J. (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534 [https://perma.cc/Y8Y6-97RS]; Bob Sullivan, *How Target Snooped on Shoppers, Changed Prices Based on Location*, MoneyTalksNews (Feb. 16, 2019), https://www.moneytalksnews.com/how-target-snooped-on-shoppers-changed-prices-based-on-location/ [https://perma.cc/V7LT-XUZ2].

with higher percentages of Asian Americans.[51] Advertisers also have been known to use location data to target users based on their religion, such as when marketers used geofencing techniques around sites of worship to target particular political ads at Catholics.[52]

Commercial location tracking also facilitates government surveillance, which is particularly harmful to communities subject to hyper-surveillance. Law enforcement has historically targeted Black and brown communities for patrolling, and location data facilitates this prejudicial practice. Post-9/11, American Muslims are one hyper-surveilled community injured by location-based surveillance. As a prominent Muslim scholar stated, the sale of their personal data by Muslim Pro "is part of a wrong pattern of crackdowns and all sorts of violations of our civil liberties that have preyed on our most basic functions as Muslims."[53]

Because it augments government surveillance powers, sharing location data from apps designed to assist with the practice of Islam could also chill American Muslims' First Amendment rights to freedom of religion, speech, and assembly. If an app shares a user's precise location information whenever it is opened during prayer time, the user may impose self-restrictions on their religious practice out of surveillance concerns. Indeed, as Johana Bhuiyan of the *L.A. Times* pointed out, "the sale of personal information by an app that helps [American Muslims] interact with their faith in the privacy of their own homes feels like a greater personal violation."[54] Similarly, when American Muslims face heightened surveillance, including having their location data sold to the government, they may be compelled to self-censor minority viewpoints, which affects their freedom of speech.[55] Lastly, American Muslims' right to assembly

---

[51] Julia Angwin, Surya Mattu & Jeff Larson, *The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get Higher Price from Princeton Review*, ProPublica: Machine Bias (Sept. 1, 2015), https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review [https://perma.cc/U6PH-BAQP].

[52] Audie Cornish, *How Political Campaigns Are Using 'Geofencing' Technology to Target Catholics at Mass*, NPR (Feb. 6, 2020), https://www.npr.org/2020/02/06/803508851/how-political-campaigns-are-using-geofencing-technology-to-target-catholics-at-m [https://perma.cc/6BVS-97PG].

[53] Johana Bhuiyan, *Muslims Reel over a Prayer App that Sold User Data: 'A Betrayal from Within Our Own Community'*, The Los Angeles Times (Nov. 23, 2020), https://www.latimes.com/business/technology/story/2020-11-23/muslim-pro-data-location-sales-military-contractors.

[54] *Id.*

[55] *See* Elizabeth Stoycheff, *Mass Surveillance Chills Online Speech Even When People Have "Nothing to Hide"*, Slate (May 3, 2016), https://slate.com/technology/2016/05/mass-surveillance-chills-online-speech-even-when-people-have-nothing-to-hide.html [https://perma.cc/G5T7-XER7] (summarizing research finding that subjects made aware of the possibility of interception and surveillance were less willing to express or support political views online that they felt differed from those of most Americans, an effect that disproportionately affected racial and ethnic minorities).

could be chilled due to the targeted nature of location tracking. If American Muslims' location data is constantly being shared, they would likely be wary of gathering in groups that could draw more attention from law enforcement. Therefore, due to privacy concerns, American Muslims would likely refrain from freely exercising their First Amendment rights.

Additionally, the practices of the location data industry have decreased technology options for American Muslims—a substantial injury to their consumer choice. Upon learning that U.S. Special Operations Command purchased location data from apps tailored to Muslims, users stated that they now have a generally heightened distrust of technology and limit their use of certain apps.[56] To be safe, CAIR Executive Director Nihad Awad encouraged "American Muslims to stop using these applications unless and until the companies thoroughly explain and fully end use of their data by government agencies."[57] Recognizing the potential for severe harms from the sharing of location data, American Muslim have been forced to be extra cautious about technology adoption.

B. Consumers cannot reasonably avoid the injuries associated with location tracking because unknown harms are occurring or known harms are irremediable.

The second part of an unfairness analysis examines whether consumers can reasonably avoid the injuries.[58] With the lack of transparency in the location data industry, consumers may not know that they are being harmed and thus cannot avoid unknown injuries. Even when consumers are aware of a harm and attempt to avoid known injuries, the actions they take can turn out to be futile.

Because the opaque location data ecosystem obscures harms, consumers cannot reasonably avoid injuries because they cannot see them. As noted in Section I.A. above, misrepresentations and omissions in location data disclosures keep consumers in the dark about how their data is sold and shared.[59] Reasonable consumers cannot consent to the collection and sharing of their location data when they receive inadequate disclosure—something the FTC has regulated in recent years.[60] Without the details of

---

[56] Bhuiyan, *supra* note 53.
[57] *Rights Group Warns US Muslims Against Using Apps Targeted by Military*, The New Arab (Nov. 17, 2020), https://english.alaraby.co.uk/news/rights-group-warns-us-muslims-against-using-targeted-apps [https://perma.cc/WM2D-LD5F].
[58] *Unfairness Policy Statement*, *supra* note 42.
[59] Section I.A. *supra* p. 4 *et. seq.*; Valentino-DeVries et al., *supra* note 23.
[60] *FTC Approves Final Order Settling Charges Against Flashlight App Creator*, Federal Trade Commission (Apr. 9, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app-creator [https://perma.cc/WQU3-NVTS].

how location data is collected and disseminated, consumers cannot reasonably make a real, informed choice to avoid harmful practices.

Even when consumers are provided with a real, informed choice to avoid injuries, sometimes that decision is ignored, either unintentionally or intentionally, by location data industry actors. Despite opting out, consumers' location data can continue to be collected and disseminated, and they are, in the words of Senator Wyden, "unable to do anything about it."[61] For example, Huq, a data vendor that obtains information from mobile apps and then sells it, continuously received GPS coordinates even when people had explicitly opted out.[62] Huq claimed that it was unaware of the issue and noted that "the app developer is responsible for the implementation of their own consent management system."[63] Meanwhile, the FTC settled with InMobi after alleging that its SDK purposefully sidestepped consumer's choice.[64] The SDK collected information from users' devices about nearby Wi-Fi networks, then used that information to reverse-engineer location data. These examples emphasize consumers' legitimate concerns that their location data sharing preferences are not respected. Even informed consumers acting reasonably by opting out cannot avoid injuries related to location tracking.

C. The substantial and unavoidable injuries to consumers that result from revealing sensitive information about their location are not outweighed by countervailing benefits.

The last part of an unfairness analysis requires assessing whether the substantial and unavoidable injuries to consumers are outweighed by countervailing benefits.[65] The main benefit of location tracking is personalization—but personalization that is beneficial to consumers can plainly be accomplished without location data. For instance, advertising can be tailored based consumers' specific traits, interests and preferences through contextual advertising.

Additionally, it is noteworthy that the U.S. intelligence community has already determined that the possible harms stemming from targeted advertisements outweigh any benefits. In fact, the NSA and CIA have internally implemented and externally

---

[61] Valentino-DeVries et al., *supra* note 23.
[62] Cox, *supra* note 33.
[63] *Id.*
[64] Lesley Fair, *Track or Treat? InMobi's Location Tracking Ignored Consumers' Privacy Settings*, Fed. Trade Comm'n: Bus. Blog (June 22, 2016), https://www.ftc.gov/business-guidance/blog/2016/06/track-or-treat-inmobis-location-tracking-ignored-consumers-privacy-settings [https://perma.cc/SAT3-U7PY].
[65] *Unfairness Policy Statement*, *supra* note 42.

encouraged ad blockers to stay safe online.[66] Therefore, the substantial and unavoidable injuries caused by location tracking are not outweighed by countervailing benefits.

III. The FTC is uniquely positioned to effectively protect consumers from deceptive and unfair location-tracking practices.

Previous FTC investigations into some location data industry actors are a good start,[67] but harms will continue to proliferate without stronger guardrails. Due to the complexity and opacity of the location data ecosystem, neither market forces nor mobile device users can adequately address these problems. The FTC must use its multiple authorities to bring enforcement actions, develop guidance or rules, and further investigate the location data industry.

A. FTC intervention is necessary because no other entity wields the power to prevent deceptive and unfair location tracking practices.

Given the immense profits generated by the collection and dissemination of location data, industry actors have no incentive to stop without regulatory intervention. Market forces will not compel change because consumers do not know enough to collectively vote with their dollars. When transparency is lacking, regulation is direly needed—and the location data industry is cloaked in secrecy. Recognizing this need, Congress has twice urged the FTC to investigate the location data industry, as the FCC plus European regulators have already taken action.[68] The FTC must act immediately to end certain location data industry practices.

---

[66] Joseph Cox, *The NSA and CIA Use Ad Blockers Because Online Advertising Is So Dangerous*, Vice (Sept. 23, 2021), https://www.vice.com/en/article/93ypke/the-nsa-and-cia-use-ad-blockers-because-online-advertising-is-so-dangerous [https://perma.cc/48N7-3PRQ].

[67] *See* Press Release, Fed. Trade Comm'n, FTC Recommends Congress Require the Data Broker Industry to Be More Transparent and Give Consumers Greater Control Over Their Personal Information (May 27, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more-transparent-give-consumers-greater [https://perma.cc/8JSE-5V4K] (The FTC has previously conducted investigations against data brokers and internet service providers. The investigations against data brokers and ISPs were more broadly focused on data collection, use, and dissemination practices but each investigation did discuss the implications of these practices as related to location data.).

[68] *See* Press Release, Fed. Commc'ns Comm'n, FCC Proposes Over $200M in Fines for Wireless Location Data Violations (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations [https://perma.cc/QJC9-BH7Z]; Simon McDougall, *Adtech Investigation Resumes*, Info. Comm'r's Office (Jan. 22, 2021), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/01/adtech-investigation-resumes/.

1. Market incentives alone will not bring about meaningful change to existing location data practices.

Market incentives cannot protect consumers from the injurious location data industry so long as widespread deception is permitted to continue, rendering it impossible for consumers to know which actors respect location privacy, and which violate it. Rather than being forthright, numerous industry actors have misled consumers into a false sense of security, lulling them into believing they have control over their location data. Eighty-one percent of smartphone users think they know how to adjust their location settings, but these attempts to block tracking are actually ineffective.[69] For example, Google services, such as Google Maps and Android's weather updates,[70] automatically stored device location data without asking, even after users followed instructions on the company's support page to change privacy settings to ostensibly prevent this.[71] And although some consumers know their data is being collected, many are unaware of the risks associated with such collection or think potential harms are too attenuated to be of concern.[72] Without full knowledge of what happens with their location data, consumers cannot make informed purchasing decisions, limiting their market power to force companies to curtail existing location data practices.

2. The lack of transparency surrounding location data practices prevents consumers from catalyzing change.

Even in circumstances lacking clear intentional deception, impenetrable opacity prevents consumers from catalyzing change. The location data industry is shrouded in secrecy, and according to a cyber policy fellow at the Duke Tech Policy Lab, "operate[s] on the fact that the general public and people in Washington and other regulatory centers aren't paying attention to what they're doing."[73] This opacity can be attributed to the lack of a relationship between consumers and many of the actors and consumers, the unknown contracts and non-disclosure agreements between parties, and the complexity of the technology.

---

[69] Emily Clark, *Do People Trust Apps that Track Their Location?,* Manifest (Jan. 23, 2019), https://themanifest.com/app-development/blog/do-people-trust-apps-that-track-location [https://perma.cc/HQ3U-8W3C].
[70] Associated Press, *Google Records Your Location Even When You Tell It Not To*, The Guardian (Aug. 13, 2018), https://www.theguardian.com/technology/2018/aug/13/google-location-tracking-android-iphone-mobile [https://perma.cc/MV2N-5MRX].
[71] *Id.*
[72] *What's the Worst that Could Happen with My Phone Data? Our Journalists Answer Your Questions*, N.Y. Times (Aug. 19, 2020), https://www.nytimes.com/2019/12/26/reader-center/location-tracking-phones-questions.html [https://perma.cc/BB5V-KYGG].
[73] Keegan & Ng, *supra* note 6.

Consumers cannot exercise choice based on their preferences because they have no direct relationship with many actors that have access to their location data. Outside of operating systems and app developers, actors in the location data industry rarely, if ever, interact with consumers. Because consumers are oblivious to the existence of SDK developers, many RTB participants, and data brokers, consumers have no idea about their practices.[74] In a bipartisan letter urging the FTC to investigate the adtech industry, lawmakers noted that "few Americans realize that companies are siphoning off and storing . . . 'bidstream' data to compile exhaustive dossiers about them."[75] Without understanding the extent to which their location data may spread, consumers cannot assert their preferences through marketplace choices. Even if these hidden actors provide choices for data settings, consumers may not know how to exercise them.[76] An FTC investigation would yield findings to educate consumers about the actors they do not interact with directly.

Even if they were aware of the many actors in the location data industry, consumers would not be able to exert market influence on the industry because they would not be able to discover how those parties share data with one another. Nearly every type of location data industry actor interacts with another type of actor,[77] but these relationships are dictated by secret agreements. Entities rarely, if ever, reveal their data sources or data recipients. For example, Safegraph, which offers a location-tracking SDK, refused to disclose from which smartphone apps, data brokers, and government agencies it acquires location data.[78] Similarly, X-Mode cited non-disclosure agreements when asked which defense contractors and government agencies purchased their data.[79] Even the industry actors themselves are sometimes left in the dark. Following

---

[74] Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability at i (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/J55K-YW5M] ("Because these companies generally never interact with consumers, consumers are often unaware of their existence, much less the variety of practices in which they engage.").

[75] Letter from Senator Ron Wyden et al. to Joseph J. Simons, Chairman, Fed. Trade Comm'n (Jul. 31, 2020), https://www.wyden.senate.gov/download/073120-wyden-cassidy-led-ftc-investigation-letter.

[76] Fed. Trade Comm'n, *supra* note 74 at vi.

[77] Keegan & Ng, *supra* note 6.

[78] Bennett Cyphers & Jason Kelley, *Illinois Bought Invasive Phone Location Data from Banned Broker Safegraph*, Elec. Frontier Found. (Aug. 19, 2021), https://www.eff.org/deeplinks/2021/08/illinois-bought-invasive-phone-location-data-banned-broker-safegraph [https://perma.cc/6N8V-T5C3] Google recently announced a ban against any apps working with SafeGraph because the company sells location data on the open market to essentially anyone. Joseph Cox, *Google Bans Location Data Firm Funded by Former Saudi Intelligence Head*, Vice (Aug. 12, 2021), https://www.vice.com/en/article/5db4ad/google-bans-safegraph-former-saudi-intelligence.

[79] Cox, *supra* note 2.

revelations about X-Mode, multiple app developers, including Muslim Pro, noted they did not know that their users' location data was being sent to defense contractors, facilitating many harms stemming from the hyper-surveillance of the American Muslim community.[80] Only an enforcement agency like the FTC can get to the bottom of these non-public agreements and exert its authority to prevent such hyper-surveillance of historically targeted communities.[81]

Natural market forces in the location data industry are further thwarted by the complexity of the technology underlying the collection and dissemination of location data, which is too complex for the average consumer to comprehend. For example, SDKs with unknown functions make it more risky to use apps, as the app ecosystem has reached a point where "a lot of developers are pulling in code that they couldn't even explain how it works."[82] Similarly, the two main RTB protocols are so "long, detailed, and technical in nature" that it is unclear whether RTB participants understand how personal data gets processed.[83] When even the actors in the location data industry are stumped, it is unrealistic to expect consumers to understand these technical practices. An FTC investigation into the confusing and concealed technology used in the location data trade would be valuable for the public to regain control of their information.

3. Congress and other agencies recognize that regulatory intervention is key to changing the location data industry.

The FTC has ample and bipartisan support from Congress to rein in harmful practices in the location data industry. In January 2019, Congress urged both the FCC and FTC to broadly investigate "the sale of American's location data by wireless carriers, location aggregators, and other third parties."[84] The FCC investigated wireless carriers and determined they did sell location data without consumers' consent, leading to fines totaling more than $200 million.[85] But the FCC noted that with respect to any

---

[80] *Id.*
[81] Fed. Trade Comm'n, Patent Assertion Entity Activity: An FTC Study 38 (2016), https://www.ftc.gov/system/files/documents/reports/patent-assertion-entity-activity-ftc-study/p131203_patent_assertion_entity_activity_an_ftc_study_0.pdf [https://perma.cc/7222-33KR].
[82] Waddell, *supra* note 4.
[83] RTB Report, *supra* note 5, at 19.
[84] Letter from Senator Ron Wyden et al. to Joseph J. Simons & Ajit Pai (Jan. 24, 2019), https://www.wyden.senate.gov/imo/media/doc/15-senators-location-aggregator-letter-to-fcc-ftc-final.pdf [https://perma.cc/MH5D-RXQT].
[85] Chris Welch, *FCC Confirms Carriers 'Apparently' Broke the Law by Selling Real-time Customer Locations*, The Verge (Jan. 31, 2020), https://www.theverge.com/2020/1/31/21117264/fcc-carriers-broke-law-selling-location-verizon-att-tmobile-sprint [https://perma.cc/UU4E-6GNL]; FCC Press Release, *supra* note 68.

other entities involved, that authority rests with the FTC.[86] In July 2020, Congress asked the FTC to investigate "widespread privacy violations by companies in the advertising technology (adtech) industry that are selling private data" about Americans without their consent.[87] As additional justification for FTC action, Congress highlighted ongoing European investigations into RTB to "enabl[e] transparency and [protect] vulnerable citizens."[88] But given the lack of FTC action, in April 2021, members of Congress themselves attempted to seek information on the RTB practices of six companies, including Google.[89] Considering Congress's eagerness to tackle the location data industry, any FTC assistance would be welcomed.

B. The FTC has the authority to curb practices that are deceptive and unfair and shed much-needed light on the location tracking industry.

The FTC should use its ample authority to rein in multiple location data actors and practices. The FTC should take immediate enforcement action against app developers, SDK developers, operating systems, actors in the RTB process, and location aggregators engaging in unfair and deceptive practices. The FTC can further make a long-lasting impact on the availability of mobile location data by regulating operating systems' and advertising exchanges' collection and mediation of location data. The FTC can also use its investigative powers to shed light on unknown or poorly understood actors or practices in the location data industry. Taking even some of these actions would drastically change the industry to the benefit of all consumers, but especially historically disadvantaged communities.

As explained above, the location data industry is rife with ongoing deceptive and unfair practices. If the FTC does not do more now, actors will not be deterred from continuing to deceive consumers and maintaining harmful practices.[90]

---

[86] *T-Mobile USA, Inc.*, *supra* note 46, at 6.
[87] Wyden et al., *supra* note 75.
[88] McDougall, *supra* note 68.
[89] Letter from Senator Ron Wyden et al. to Sundar Pichai, CEO, Google (Apr. 1, 2021), https://www.wyden.senate.gov/imo/media/doc/040121%20Wyden%20led%20Bidstream%20Letter%20to%20Google.pdf [https://perma.cc/S8FX-BJRN] (The letter requested information about the "specific data elements about users, their devices, the websites . . . and apps they are using that you provide to auction participants," foreign and domestic companies that have been provided bidstream data, contractual restrictions on the "sharing, sale, or use, or secondary use of bidstream data," and " each foreign headquartered or foreign-majority owned company to whom bidstream has been provided.").
[90] *See* Cox, *supra* note 33; Geoffrey Fowler & Tatum Hunter, *When You 'Ask App Not to Track,' Some iPhone Apps Keep Snooping Anyway*, Wash. Post (Sept. 23, 2021), https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/ [https://perma.cc/493R-GMJ7].

The FTC should take immediate enforcement action to curb these practices and reemphasize that actors in the location data industry share a joint responsibility for ensuring that consumers have clear and conspicuous information about how their location information will be collected and used, protecting location information by default, and giving consumers choices that are meaningful. The FTC should begin by bringing Section 5 enforcement actions against:

- App developers that include location-tracking SDKs in their apps without fully understanding and/or disclosing their data-distribution capabilities, leading to users' sensitive data being unknowingly shared with third parties.[91] For example, the Muslim Pro and Muslim Mingle apps incorporated a location-tracking SDK that sent users' location data to the firm X-Mode, which collected users' location data without their knowledge.[92] This data was then sold to third parties, including law enforcement and possibly foreign actors.[93]
- SDKs that fail to inform apps about their location-tracking behaviors or that do not take reasonable measures to ensure that apps in which they are embedded properly notify consumers about their location-tracking behaviors and obtain affirmative prior consent.
- Mobile operating systems that fail to adequately protect location information by default, or that misleadingly collect or share location information for purposes other than to facilitate operation of the device without ensuring that users receive clear notice of location tracking practices and are protected from location tracking unless they provide affirmative prior consent.
- Actors in the RTB process that collect and retain consumer data from the information shared on advertising exchanges regarding available impressions, when such data is used for any purpose other than to offer good faith bids for impressions or is retained beyond the amount of time necessary to inform good faith bids for impressions.
- Location aggregators that receive or purchase location data, aggregate location data, or resell location data without taking reasonable measures to ensure that such activities are consistent with the disclosures made to and affirmative prior consent received from consumers.
- Any and all of the above that sell or share location data with other parties without taking measures to ensure that downstream parties do not aggregate

[91] Waddell, *supra* note 4.
[92] Cox, *supra* note 2.
[93] *Id.*

that data with other datasets, reidentify it, or use it in manners inconsistent with the disclosures made to and affirmative prior consent received from consumers.

- Any and all of the above that fail to adequately disclose their practices, that do so in a misleading way, or that falsely claim location data as "anonymous" when it is reidentifiable.

The FTC should build on enforcement actions by simultaneously issuing guidance to parties in the location data industry on the affirmative steps they can take to help avoid deceiving their users. For example, the FTC has already provided some guidance to app developers for addressing security vulnerabilities when it comes to SDKs,[94] and could amend such guidance to additionally instruct SDK developers on best practices for explaining the functionality of their SDKs to app developers and the public. FTC guidance could further help app developers identify what questions to ask about the functionality of any kit used in their app, and what details to disclose about their SDKs to consumers.

In the longer term, the FTC should initiate a rulemaking proceeding to regulate mobile operating systems' and advertising exchanges' management and use of location data. This is the most effective way to rein in the location data industry because the location data industry is permeated by prevalent unfair and deceptive practices, and these entities are the primary gatekeepers of users' location data with the greatest power to effect change. Where mobile operating systems are concerned, FTC rules could improve practices related to unique advertising identifiers and mediation of location data. Mobile operating systems provided by both Apple and Android recently have adopted more privacy-protective practices regarding users' unique identifiers.[95] These are positive changes, but the FTC can and should adopt prospective rules that

---

[94] *App Developers: Start with Security*, Fed. Trade Comm'n (May 2017), https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security [https://perma.cc/8JWS-834P].

[95] Apple recently required apps to ask users to opt in upfront and otherwise shares only a zeroed-out advertising identifier, which prohibits apps from re-identifying a user who opts out. *See* Brian Chen, *To Be Tracked or Not? Apple Is Now Giving Us the Choice.*, N.Y. Times (Sept. 29, 2021), https://www.nytimes.com/2021/04/26/technology/personaltech/apple-app-tracking-transparency.html [https://perma.cc/3FPP-D85R]. Older Android operating systems offer no choice for opting out, but Google recently announced that the advertising identifiers of users who opt out will now be zeroed out rather than still shared. Prior to the announcement, the advertising id was still shared with app developers even when the user opted out. The effectiveness of the opt-out was in part reliant on app developers complying with Google's order not to use the advertising ID for advertising purposes. Tim Anderson, *Upcoming Android Privacy Changes Include Ability to Blank Advertising ID, and 'Safety Section' in Play Store*, The Register (July 29, 2021), https://www.theregister.com/2021/07/29/android_privacy_changes/ [https://perma.cc/BV8C-BPB2].

mandate opt-in consent for enabling advertising identifiers; an easily-accessible reset mechanism that prevents linking a new advertising identifier with the previous one; and technical, rather than contractual, solutions to prevent the use of an advertising identifier when a user does not consent.

Where advertising exchanges are concerned, the FTC could adopt rules that limit the amount of information made vulnerable to bidstream siphoning in the RTB process.[96] More specifically, the FTC should implement a "minimum necessary" rule to govern the level of detail permitted for data included in a bid request—at the very least, generalized enough to prevent identification of individuals.[97] This could be accompanied by outright prohibitions against the sharing of sensitive data, such as latitude and longitude, with available ad impressions offered up for prospective buyers—some of which may be data brokers siphoning data—to evaluate and bid on. Furthermore, the FTC should require ad exchanges to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information within the RTB process. Lastly, the FTC should take steps to ensure that auction participants cannot use the bidstream data for derivative products or to undermine publishers.

Finally, in circumstances where the FTC finds insufficient information exists even to initiate investigation and enforcement or issue a request for comments on the feasibility of rulemaking, the FTC should consider using its investigative powers to probe further into the location data industry and shed much-needed light on the many troubling practices detailed in this request. For example, the FTC could host a workshop or hearing seeking public comments and discussion regarding various actors in the location data industry. The FTC has also, in the past, relied on its 6(b) authority to seek detailed information from companies about their business practices, and could do so here to learn more and to inform a public report regarding these practices.

---

[96] *See* Cox, supra note 27.

[97] An example of such a requirement can be found in HIPAA. Under HIPAA's minimum necessary rule, covered entities are required to make reasonable efforts to ensure that access to protected health information is limited to the minimum amount of information necessary to fulfill or satisfy the intended purpose of the disclosure. *Minimum Necessary Requirement*, U.S. Dept. of Health & Hum. Servs. (Apr. 4, 2003), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html [https://perma.cc/F6SR-2PT9].

CONCLUSION

The location data industry is harming all consumers, but especially communities subject to hyper-surveillance like American Muslims. The FTC should take immediate action to catalyze change across the industry, stopping current harms and preventing future harms. Where the practices are known to be deceptive and unfair, the FTC should immediately bring enforcement action. The FTC should further issue guidance and rulemaking to clarify what are unfair and deceptive practices or investigate the actors and practices to learn more about the opaque location data industry.

By:

/s/ _____
Laura M. Moy*
Communications & Technology Law Clinic at Georgetown Law
600 New Jersey Ave, NW
Washington, DC 20001

Counsel for the Council on American-Islamic Relations

Respectfully submitted,

The Council on American-Islamic Relations

April 12, 2022

* This request for investigation was drafted with considerable assistance from student attorneys Monty Roberson, Pariss Briggs, Philip Robbins, Luke Evans, and Quinten Stewart, and teaching fellow Victoria Tang in the Communications & Technology Law Clinic at Georgetown Law.