THE "RIGHT TO BE LET ALONE" SHOULD APPLY TO GEOLOCATION TRACKING WITHIN THE HOME

Eliza Smith-Driggs*

Cite as: Eliza Smith-Driggs, *The "Right to be Let Alone" Should Apply to Geolocation Tracking Within the Home*, 30 RICH. J.L. & TECH 495 (2024).

* 2025 J.D. Candidate, BYU Law School. The author would like to thank Professor Curtis Anderson for his guidance on this Note.

I. INTRODUCTION

[1] Lisa Magrin, a 46-year-old math teacher from New York, makes the 14-mile trip from her home to her middle school classroom multiple times a week.[1] On an innocuous day in 2018, she hiked with her dog, attended a Weight Watchers meeting, visited her dermatologist, and slept at her ex-boyfriend's home.[2] Little did she know that an app on her phone tracked her precise location as often as every two seconds.[3]

[2] Though Ms. Magrin knew apps could track geolocation data, she found it "disturbing" to know how often her precise location was tracked and then sold to advertisers.[4] Ms. Magrin's identity was not tied to the information sold to advertisers, but *The New York Times* reportedly connected the tracked geolocation dot to Ms. Magrin with ease, given that she was the only person during that time of day who regularly traveled the 14-mile commute to school.[5] With her permission, *The Times* reviewed four months of Ms. Magrin's geolocation data and determined that her location was recorded over 8,600 times—an average of once every 21 minutes.[6]

[3] Another cell phone user, Elise Lee, said she found it "very scary" having her precise geolocation data tracked: "It feels like someone is

---

[1] Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [perma.cc/3BDS-A7VQ].

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] Valentino-DeVries et al., *supra* note 1.

following me, personally."[7] Yet perhaps to Ms. Lee's dismay and surprise, geolocation tracking may intrude further than even a private investigator, who has the legal right to follow her in public places, as long as they are not shadowing her in "unreasonable and obtrusive" ways.[8] As soon as Ms. Lee enters her home, the investigator's right to follow her ceases.[9] They cannot record her movements within her own home; such an action would likely constitute trespass under property law[10] and an invasion of privacy under tort law.[11] If private investigators cannot lawfully record Ms. Lee's movements within her home, why should her phone be any different? This Note analyzes whether trespass and privacy tort standards could be reasonably applied to electronically tracking precise geolocation data within an individual's own home.

[4] Though no federal standard yet exists for geolocation data tracking, twelve states have enacted statutes that address data privacy practices in regard to consumers' geolocation data.[12] Many consider the Virginia Consumer Data Protection Act ("VCDPA"), which took effect on January

[7] *Id.*

[8] J. D. Emerich, *Investigations and Surveillance, Shadowing and Trailing, as Violation of Right of Privacy*, 13 A.L.R.3d 1025, § 2.

[9] *See id.*

[10] *See* Wellesley Hills Realty Tr. v. Mobil Oil Corp., 747 F. Supp. 93, 99 (D. Mass. 1990).

[11] *See* Souder v. Pendleton Detectives, Inc., 88 So. 2d 716, 718 (La. Ct. App. 1956).

[12] Zachary S. Schapiro, *Update: Processing Sensitive Personal Information under U.S. State Privacy Laws,* THE NAT'L L. REV. (Sept. 12, 2023), https://www.natlawreview.com/article/update-processing-sensitive-personal-information-under-us-state-privacy-laws [perma.cc/BM7S-ZWZJ]. Additionally, the list of state statutes are cited in footnotes 81–90 of this Note.

1, 2023,[13] as one of the leading state approaches on the topic.[14] The VCDPA requires controllers of data to obtain affirmative consent from Virginians to process and sell their sensitive data, including their precise geolocation data.[15] It also codifies the existing federal requirement under Section 5 of the Federal Trade Commission Act, which prohibits all "unfair or deceptive" practices.[16]

[5] However, the VCDPA does not require that consumers give their *informed* or *specific* consent to allow companies to track their every move even inside their own homes—conduct that the right to privacy would traditionally prevent private investigators from undertaking.[17] This Note argues that Virginia should require companies to obtain not just the consent, but the *informed* consent, of consumers so that they can make educated choices about the amount of precise geolocation data that they allow companies to access and sell.

[6] Part III.A of this Note details how the VCDPA approaches precise geolocation data protection as a proxy for the approach states are taking generally. Part III.B describes how tort law treats the right to privacy. Part III.C explains how precise geolocation tracking interacts with a privacy tort

[13] V.A. CODE. ANN. § 59.1-575 (West 2023).

[14] Theodore P. Augustinos & Alexander R. Cox, *U.S. State Privacy Laws in 2023: California, Colorado, Connecticut, Utah and Virginia*, LOCKE LORD (Dec. 2022), https://www.lockelord.com/newsandevents/publications/2022/12/us-state-privacy-laws-2023 [perma.cc/Z3QP-L5NZ].

[15] V.A. CODE. ANN. § 59.1-578 (West 2023).

[16] FED. RESERVE, FEDERAL TRADE COMMISSION ACT SECTION 5: UNFAIR OR DECEPTIVE ACTS OR PRACTICES, https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf [perma.cc/QBF3-ZSJU] (last visited Mar. 18, 2024).

[17] *See* VA. CODE ANN. § 59.1-575; *see also* Souder v. Pendleton Detectives, Inc., 88 So. 2d 716, 718 (La. Ct. App. 1956).

called "intrusion upon seclusion."[18] Part III.D discusses the challenges of implementing and enforcing informed consent requirements. Finally, Part III.E outlines recommendations for Virginia to encourage informed consent, including requiring a short warning pop-up disclaimer and a geofencing control that would allow homeowners to decide what type of data companies collect within the home.

II. BACKGROUND

A. Geolocation Overview

[7] If a customer enters a Nordstrom store today, security cameras could track her every move. If she spends 34 minutes in the maternity section and buys an item of clothing, it is legal for a Nordstrom employee or an automated tool to comb through the security footage and track her purchase patterns. The employee or automated tool might notice that she spent exactly 34 minutes in the maternity section, infer that either she or a loved one is expecting a baby, acquire her name from her time-stamped purchase receipt, and then customize her Nordstrom mailing advertisements to fit her current maternity needs. Nordstrom could even hire employees to follow customers around the store and note their interests in categories of items so that Nordstrom could better tailor its advertisements to fit each customer's needs.

[8] Though this method of targeted advertising is legal because the right to privacy does not protect public movement,[19] doing so would be extremely inefficient from both a cost and time perspective. Companies likely would not pay employees to comb through hours of footage and connect each customer to their purchase receipt just to tailor ads to the customers. But the invention of smartphones and precise geolocation-tracking technology shifts the cost-benefit analysis, making tracking a

[18] 3 BUS. TORTS § 33.02 (LexisNexis 2023).

[19] Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018) (citing United States v. Knotts, 460 U.S. 276 (1983)).

customer's shopping behavior neither costly nor inefficient and likely resulting in increased purchases from advertisements specifically tailored to meet individual customers' needs.

[9] Over 85% of the world's population owns a smartphone, and almost all smartphones contain a built-in geolocation tracker.[20] Most people have their smartphone on or close to their body a majority of the time; a recent study found the average American touches their cell phone 2,617 times per day, checking it once every ten to twelve minutes.[21] Cell phones track an individual's location across a variety of applications, from obtaining correct weather information to offering traffic-specific GPS navigation.[22] Knowing when to wear a jacket or how to route a road trip is useful for consumers, but they should know and understand that companies collect and use geolocation data to provide these services. Smartphones do far more than help you avoid traffic—they also track an individual's location to help create a customized user profile for which to best advertise various products and services.[23] Apple,[24] "free" app providers,[25] and even mobile carriers

[20] *See* Jack Flynn, *20 Vital Smartphone Usage Statistics [2023]: Facts, Data, and Trends on Mobile Use in the U.S.*, ZIPPIA (Apr. 3, 2023), https://www.zippia.com/advice/smartphone-usage-statistics/ [perma.cc/N4R2-VJWX]; *see also* Focal Point Insights, *How to Navigate Geolocation and Data Protection Laws*, FOCAL POINT DATA RISK (Mar. 18, 2021), https://blog.focal-point.com/how-to-navigate-geolocation-and-data-protection-laws [perma.cc/H3WH-2JPC].

[21] Flynn, *supra* note 20.

[22] Focal Point Insights, *supra* note 20.

[23] *Id.*

[24] *Apple Privacy Policy*, APPLE, https://www.apple.com/legal/privacy/en-ww/ [perma.cc/T9DT-HJVZ] (last updated Mar. 31, 2024).

[25] *See* Kalev Leetaru, *What Does It Mean For Social Media Platforms To "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=30c6e1002d6c [perma.cc/5NMA-ANM8].

such as T-Mobile, AT&T, and Verizon sell consumer information to advertisers without obtaining explicit consent from their consumers.[26]

[10] The location-based advertising market has grown exponentially every year.[27] In 2022, researchers estimated the market's value at $96 billion, projecting a compound annual growth rate of 15.1% from 2023 to 2030.[28] A March 2021 Focal Point Insights article noted that "[s]ince many . . . location services run discreetly in the background, data is potentially being captured without the individual's knowledge or consent."[29] And because geolocation data can reveal "detailed information about a tracked individual's behavior, patterns, and personal life (accurate to within a few yards and updated over 14,000 times a day), it raises the question of whether the location data being collected can be used to personally identify an individual, despite anonymizing the dataset."[30] A 2019 article ominously concluded that if an individual allows an app to access her location, "[she] should assume that data will be recorded for posterity, shared with other companies, and used in ways [she] didn't expect."[31]

---

[26] Mike Dano, *T-Mobile to ioin AT&T, Verizon in selling customers' data*, LIGHTREADING (Mar. 9, 2021), https://www.lightreading.com/security/t-mobile-to-join-at-t-verizon-in-selling-customers-data [perma.cc/5T3K-34QP].

[27] *Location-based Advertising Market Size, Share & Trends Analysis Report By Component (Geofencing, Geotargeting), By Advertisement Type, By Promotion Type, By Application, By Industrial Vertical, And Segment Forecasts, 2023–2030*, GRAND VIEW RSCH., https://www.grandviewresearch.com/industry-analysis/location-based-advertising-market [perma.cc/DB6E-GJCV] (last visited Mar. 18, 2024).

[28] *Id.*

[29] Focal Point Insights, *supra* note 20.

[30] *Id*.; Valentino-DeVries et al., *supra* note 1.

[31] Zachary M. Seward, *What to do when your iPhone says an app has been using your location in the background*, QUARTZ (Sept. 21, 2019), https://qz.com/1713581/what-to-do-when-an-iphone-app-is-using-your-location-in-the-background [perma.cc/TKA4-UWX4].

[11] In 2012, the United States Supreme Court found in *United States v. Jones* that GPS monitoring could generate a "wealth of detail" about an individual's personal life.[32] By simply reviewing an individual's location history, one can identify "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"—all of which constitute private information that businesses or governments can exploit.[33] Thus, by 2013, there was "strong public support" for banning the collection of geolocation data without a consumer's consent.[34]

[12] Compelled by this strong public support, Virginia legislators drafted the Consumer Data Protection Act, which will be explained in Part III.A. In 2022, Apple also responded to the public outcry and announced its new privacy consent framework, which required apps to display a pop-up asking new users for permission to track their data.[35] Perhaps unsurprisingly, 62% of users chose to opt out of sharing their data when they were given the option.[36] Among the apps affected by Apple's privacy change, Facebook parent Meta projected a $10 billion loss in revenue due to this opt-out option.[37] However, Apple's own 2022 revenue actually increased by eight

[32] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

[33] *Id.*

[34] Ryan Mura, *Geolocation and Targeted Advertising: Making the Case for Heightened Protections to Address Growing Privacy Concerns*, 9 BUFF. INTELL. PROP. L.J. 77, 87 (2013).

[35] Kif Leswing, *Facebook says Apple iOS privacy change will result in $10 billion revenue hit this year,* CNBC, https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html [perma.cc/8HEW-FJK3] (last updated Feb. 3, 2022, 11:06 AM).

[36] *Id.*

[37] *Id.*

percent.[38] This revenue increase is strong economic evidence of public support for Apple's bold step in the direction of vigorously protecting consumer data.

[13] The Federal Communications Commission ("FCC") recently disclosed to what extent mobile carriers access and use consumer data.[39] In July 2022, FCC Chairwoman Jessica Rosenworcel requested information from fifteen of the nation's largest mobile carriers regarding their data retention and data privacy policies and practices.[40] In the request, Rosenworcel stated that "the highly sensitive nature of this data—especially when location data is combined with other types of data—and the ways in which this data is stored and shared with third parties is of utmost importance to consumer safety and privacy."[41]

[14] A month later, in August 2022, Rosenworcel shared the carriers' responses with the public, adding this caution:

> Our mobile phones know a lot about us. That means carriers know who we are, who we call, and where we are at any given moment. This information and geolocation data is really sensitive. It's a record of where we've been and who

[38] *Apple Reports Fourth Quarter Results*, APPLE NEWSROOM (Oct. 27, 2022), https://www.apple.com/newsroom/2022/10/apple-reports-fourth-quarter-results/ [perma.cc/F3QG-EALQ].

[39] Chris Frascella, *Greater Legal Protections Needed for Phone Geolocation Data*, ELEC. PRIV. INFO. CTR. (Nov. 28, 2022), https://epic.org/greater-legal-protections-needed-for-phone-geolocation-data/ [perma.cc/84EE-HWDR].

[40] *Id.*

[41] Press Release, Federal Communications Commission, Chairwoman Rosenworcel Probes Top Mobile Carriers on Data Privacy Practices (July 19, 2022), https://docs.fcc.gov/public/attachments/DOC-385446A1.pdf [perma.cc/8SLL-552L].

> we are. That's why the FCC is taking steps to ensure this data is protected.[42]

Ominous statements like this—especially from prominent government officials—should raise concern. They raise red flags for consumers and invite cell phone users to give the ethical and practical ramifications of precise geolocation tracking a second thought. At the very least, the FCC's awareness of and action to protect the sensitive nature of consumer location data is an encouraging step toward more consumer privacy.

B. Current Data Privacy Regulations for Geolocation Data

[15] The United States does not currently have a federal law specifically governing the use, collection, or sharing of geolocation data.[43] It should, because companies will increasingly use geolocation tracking technology in the coming years. The government should establish clear rules and protocols to prevent further violations of consumers' privacy. But until the federal government acts, the use, collection, and sharing of geolocation data are generally regulated under one of two umbrellas: the Federal Trade Commission or the European Union's General Data Protection Regulation.[44] In addition to these federal and multinational regulations, states have increasingly regulated geolocation data.[45]

---

[42] Press Release, Federal Communications Commission, Chair Rosenworcel Shares Mobile Carrier Responses to Data Privacy Probe and Announces Next Steps (Aug. 25, 2022), https://docs.fcc.gov/public/attachments/DOC-386596A1.pdf [perma.cc/SY6E-2GWQ].

[43] Focal Point Insights, *supra* note 20; Caitriona Fitzgerald, *Full of Holes: Federal Law Leaves Americans' Personal Data Exposed*, ELEC. PRIV. INFO. CTR. (Apr. 27, 2023), https://epic.org/full-of-holes-federal-law-leaves-americans-personal-data-exposed/ [https://perma.cc/VV79-CQN8].

[44] Focal Point Insights, *supra* note 20.

[45] Schapiro, *supra* note 12.

1. The Federal Trade Commission

[16] The Federal Trade Commission ("FTC"), a government agency tasked with protecting competition and consumers,[46] has implemented protections for precise geolocation data because it considers such data to be sensitive.[47] Section 5 of the FTC Act prohibits "unfair and deceptive trade practices."[48] For example, the FTC targets companies that make false claims about "anonymizing" geolocation data before selling it to advertisers.[49] This is because anonymizing the data does not truly protect a consumer's identity and can be re-identified: "[I]n some instances, it [is] possible to uniquely identify 95% of a dataset of 1.5 million individuals using four location points with timestamps."[50] As noted in the Introduction of this Note, even though data controllers anonymized Ms. Magrin's identity when they tracked and sold her precise geolocation data, *The New York Times* still easily identified her based on her unique and routine movement patterns.[51]

[46] *What the FTC Does*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/what-ftc-does [https://perma.cc/L36A-CPPT] (last visited Apr. 3, 2024).

[47] Focal Point Insights, *supra* note 20.

[48] Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, FED. TRADE COMM'N: BUS. BLOG (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [perma.cc/GN7D-KPVZ].

[49] *Id.*

[50] *Id.*

[51] Valentino-DeVries et al., *supra* note 1.

2. The General Data Protection Regulation

[17] The European Union's General Data Protection Regulation ("GDPR") acts as Europe's data privacy regulatory scheme.[52] If a U.S. company has online customers from the European Union ("EU") or other parts of the European Economic Area ("EEA"), the GDPR governs.[53] Considered to be one of the world's most comprehensive privacy laws, the GDPR promotes consumers' knowledge of exactly what happens to their data, affirmative consent for data to be processed, stored, and used in certain ways, and withdrawal of consent at any time.[54]

C. Virginia is the Trendsetter

[18] Like the GDPR in many respects, the VCDPA gives Virginia consumers "the right to access their data and request that their personal information be deleted by businesses,"[55] among other rights. Virginia was the second state in the U.S. to pass comprehensive data privacy legislation.[56] The Virginia legislature passed the VCDPA in March 2021, just under three years after California became the first state to enact such legislation with the California Consumer Privacy Act ("CCPA").[57] But unlike the CCPA, the VCDPA garnered support from technology industry

[52] *See* Ben Wolford, *What is GDPR, the EU's new data protection law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ [perma.cc/U8ZR-DMQ6] (last visited Mar. 18, 2024).

[53] Josh Langeland, *GDPR in the US: Compliance Simplified for Businesses*, TERMLY (Aug. 14, 2023), https://termly.io/resources/articles/gdpr-in-the-us/ [perma.cc/8V9N-S5HJ].

[54] Focal Point Insights, *supra* note 20.

[55] *Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L.: PRIV. (Mar. 18, 2024), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/ [perma.cc/3QKD-S7UC]; *see* VA. CODE ANN. § 59.1-577 (West 2023).

[56] *Which States Have Consumer Data Privacy Laws?*, *supra* note 55.

[57] *Id.*

leaders like Amazon and Microsoft.[58] Such support presumably indicates that both consumers and companies consider the VCDPA's regulations as reasonable, beneficial, and fair.

[19] In addition to Virginia and California, ten other states have enacted comprehensive data privacy legislation.[59] Most reflect Virginia's model,[60] considering California's approach to data privacy protection as overly broad and ineffective at balancing privacy rights with legitimate business interests.[61] Accordingly, when Virginia enacted the VCDPA, advocates argued it would provide an alternative model to the CCPA:[62] "Virginia's recent action is relevant beyond its borders, becoming the model for proposed legislation in [states] and raising the profile of long-stalled congressional data privacy efforts."[63]

---

[58] *See* Christopher Escobedo Hart & Colin Zick, *Virginia's New Data Privacy Law: An Uncertain Next Step for State Data Protection*, JD SUPRA (July 7, 2021), https://www.jdsupra.com/legalnews/virginia-s-new-data-privacy-law-an-8812636 [https://perma.cc/S52A-7XBM]; *see also* Cat Zakrzewski, *Virginia Governor signs nation's second state consumer privacy bill*, WASH. POST (Mar. 2, 2021, 8:17 PM), https://www.washingtonpost.com/technology/2021/03/02/privacy-tech-data-virgina [https://perma.cc/YK65-LNFM].

[59] Schapiro, *supra* note 12.

[60] Augustinos & Cox, *supra* note 14.

[61] Tom Kulik, *Some Big Reasons Why The CCPA Is More Of A Problem Than You Think*, ABOVE THE L. (Oct. 28, 2019, 6:18 PM), https://abovethelaw.com/2019/10/some-big-reasons-why-the-ccpa-is-more-of-a-problem-than-you-think [https://perma.cc/336U-QVDS].

[62] Kirk J. Nahra & Ali A. Jessani, *Virginia's New Consumer Privacy Law Is Set for 2023—What's Next?*, BLOOMBERG L. (Mar. 2, 2021, 4:00 AM), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X9K768EC000000?bna_news_filter=privacy-and-data-security#jcite [https://perma.cc/7JVV-BCB7].

[63] Hart & Zick, *supra* note 58.

[20] Thus, this Note focuses on Virginia's data privacy policy as the trendsetter for many states' legislation. The VCDPA will likely also serve as a model for the national standard for data protection if Congress ever proposes such a policy for treatment of sensitive personal data.

D. Intrusion Upon Seclusion Overview

[21] As noted in the Introduction, this Note analyzes the relationship between the VCDPA and privacy under tort law. The following serves as a brief overview of how tort law treats privacy, with Part III.B exploring the specifics.

[22] The "intrusion upon seclusion" tort falls under the broader umbrella of "invasion of privacy" torts.[64] The purpose of the invasion of privacy tort is to protect an individual's "right to be let alone."[65] One violates the intrusion upon seclusion tort if they "intentionally intrude[], physically or otherwise, upon the solitude or seclusion of another or his [or her] private affairs or concerns[.]"[66] The intrusion must be "highly offensive to a reasonable person."[67] Examples of highly offensive intrusions include opening someone's private mail, searching through a safe or wallet, using binoculars to look into someone else's windows, tapping telephone wires, examining another's bank account without permission, or fraudulently compelling someone to submit to a court order permitting inspection of personal documents.[68]

---

[64] Nahra & Jessani, *supra* note 62; RESTATEMENT (SECOND) OF TORTS §§ 652A–652B (1997).

[65] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

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

[67] *Id.*

[68] *See id.*

[23] Though the Introduction already established that private investigators have no right to track an individual's location within her home because that would constitute trespass and a tortious violation of privacy, this Note analyzes whether a *company* tracking an individual's precise location within her home is "highly offensive to a reasonable person" and therefore a violation of the intrusion upon seclusion tort.

III. ANALYSIS

A. The VCDPA's Approach to Geolocation Data Protection

[24] The VCDPA is a step in the right direction in the effort to protect consumers' sensitive data. To describe it simply, the VCDPA requires certain businesses to provide consumers choice, access, and control over the collection, processing, use, and storage of their personal data.[69] It also requires companies to obtain consent from consumers before using their personal data for capital gain.[70] Under the VCDPA, Virginians have the right to "submit a request to access, correct inaccuracies within, and delete personal data they have provided or that has been obtained about them."[71] This is new. Rather than simply following the disclosure and consent requirements under existing federal law,[72] the VCDPA grants rights beyond consent; it gives consumers control over how companies use their data even after collection with their consent.[73] A 2009 study found 92% of American adults agreed there should be a law that requires "websites and advertising companies to delete all stored information about an individual[] if requested

[69] *See* Hart & Zick, *supra* note 58.

[70] *Id.*

[71] *Id.*

[72] *See* FED. RESERVE, FEDERAL TRADE COMMISSION ACT SECTION 5: UNFAIR OR DECEPTIVE ACTS OR PRACTICES, https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf [perma.cc/QBF3-ZSJU] (last visited Mar. 18, 2024).

[73] Hart & Zick, *supra* note 58.

to do so[,]" and 69% of American adults felt a law should "give[] people the right to know everything that a website knows about them."[74]

[25] Before describing the VCDPA in more detail, it is important to first identify key terminology. The VCDPA relevantly defines the following terms:

> "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information.
>
> "Precise geolocation data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.
>
> "Sensitive data" means a category of personal data that includes: (1) [p]ersonal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (2) [t]he processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (3) [t]he personal data collected from a known child; or (4) [p]recise geolocation data.[75]

---

[74] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities That Enable It*, SSRN (Sept. 29, 2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 [https://perma.cc/A2M8-Y38L].

[75] VA. CODE ANN. § 59.1-575 (2023).

Note that "sensitive data" includes precise geolocation data, unlike the European Union's GDPR definition, which includes racial or ethnic origin, political opinions, biometric data, and health data but not precise geolocation data.[76] Also note that because the VCDPA's definition of "precise geolocation data" includes an individual's movements within a radius of 1,750 feet, such data often reveals information about an individual's location in her home, information that even private investigators cannot access.[77]

[26] With those definitions in mind, the rule for Virginia data controllers states:

> Controllers shall "[n]ot process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.)."[78]

Essentially, consumers must give their affirmative consent (i.e., they must opt-in) before controllers can process or sell sensitive data.[79] Controllers generally obtain consent by requiring consumers to "agree" to a company's privacy policy when downloading an app or setting up an account.[80] Once

[76] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 561 (2019) (analyzing the General Data Protection Act's (GDPR) definition of sensitive data); VA. CODE ANN. § 59.1-575 (2023).

[77] Souder v. Pendleton Detectives, Inc., 88 So. 2d 716, 718 (La. Ct. App. 1956); VA. CODE ANN. § 59.1-575 (2023).

[78] VA. CODE. ANN. § 59.1-578(5) (2023).

[79] Hart & Zick, *supra* note 58.

[80] *Id.*

a consumer consents to the privacy policy, consent is rarely addressed again. Given this "agreement," consumers may not understand that (1) they have certain privacy rights within their own home, (2) they have the right to withdraw their consent, and (3) controllers processing their precise geolocation data perhaps violate those privacy rights. In short, controllers do not collect sensitive data with *informed* consent. This Note expands on the concept of informed consent in Part III.D.

[27] All but one of the states that recently implemented comprehensive data privacy laws include precise geolocation data in their definition of "sensitive data": California,[81] Connecticut,[82] Delaware,[83] Indiana,[84] Iowa,[85] Montana,[86] Oregon,[87] Tennessee,[88] Texas,[89] and Utah (Utah calls "precise" geolocation "specific," but the definition of "specific" mirrors Virginia's definition of "precise").[90] Of those states, California is the only state which does not include the 1,750-foot radius requirement in its definition of sensitive data; instead, it extends the radius to 1,850 feet.[91] To date, Colorado is the only state that does not consider precise geolocation data to

[81] CAL. CODE REGS. tit. 1.81.5 § 1798.140 (2018).

[82] S.B. 6, Pub. Act No. 22-15 § 1 (Conn. 2023).

[83] H.B. 154, 152nd Gen. Assemb. § 12D-102 (Del. 2023).

[84] S.B. 5, 123rd Gen. Assemb., Reg. Sess. § 28 (Ind. 2023).

[85] S.F. 262, Gen. Assemb. § 1 (Iowa 2023).

[86] S.B. 0384, 68th Leg. § 2 (Mont. 2023).

[87] S.B. 619, 82nd Leg. Assemb., Reg. Sess. § 1 (Or. 2023).

[88] H.B. 1181, 113th Gen. Assemb. § 2 (Tenn. 2023).

[89] H.B. 4 § 541.001 (Tex. 2023).

[90] S.B. 227, Gen. Sess. § 13-61-101 (Utah 2023).

[91] CAL. CODE REGS. tit. 1.81.5 § 1798.140 (2018).

be sensitive data.[92] Colorado also does not include the 1,750-foot radius requirement, nor any radius requirement, in its description of location data.[93]

B. Tort Law's Approach to Privacy

[28] Invasion of privacy torts are designed to protect an individual's "right to be let alone"[94] and "the right to respite from observation and judgment so that, when we do participate socially, we can be more engaged and ethical participants."[95] Interestingly, the tort bases liability not on the content of the information discovered but on the *behavior* that resulted in the discovery of such data.[96]

[29] Privacy torts include four basic causes of action: (1) intrusion upon seclusion, (2) appropriation of name or likeness, (3) public disclosure of private facts, and (4) placing a person in a false light.[97] The only cause of action that applies when geolocation data could be compromised without a consumer's informed consent is intrusion upon seclusion. The other three causes of action involve "publicizing private facts about someone else for personal benefit."[98] This is not typically an issue when selling a consumer's precise geolocation data because it would not usually benefit a company to

[92] S.B. 21-190, Gen. Assemb. § 6-1-1303 (Colo. 2023).

[93] *Id.*

[94] Warren & Brandeis, *supra* note 65, at 193.

[95] Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 206 (2012).

[96] *Id.* at 206–07.

[97] *The Torts of Invasion of Privacy*, LAWSHELF, https://lawshelf.com/shortvideoscontentview/the-torts-of-invasion-of-privacy [https://perma.cc/CA65-NGWL] (last visited Mar. 19, 2024).

[98] *Id.*

publish a consumer's precise location. Selling such specific information would signify to an otherwise ignorant consumer that companies track information about their whereabouts.

[30] "The intrusion tort penalizes conduct—offensive observations—not revelations."[99] Proponents of using the intrusion upon seclusion tort to enforce ethical geolocation tracking practices "point to the fact that it 'reinforces norms by tracking social consensus, which means that most people will recognize what is and is not seclusion, even in new contexts.'"[100]

[31] Section 652B of the Second Restatement of Torts defines intrusion upon seclusion as follows:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[101]

Though litigation on this issue is ongoing, courts throughout the country have weighed in on what conduct constitutes a highly offensive intrusion.

[32] First, the Court of Appeals of Florida held in *Jackman v. Cebrink-Swartz* that conducting constant video surveillance of a neighbor's backyard represents an intrusion of privacy.[102] The court held that "there is a material difference between occasionally viewing the activities within a neighbor's backyard that are observable without peering over a privacy fence and erecting a camera to see over a privacy fence to thereafter surveil

[99] Bambauer, *supra* note 95, at 207.

[100] Mura, *supra* note 34, at 87.

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

[102] Jackman v. Cebrink-Swartz, 334 So. 3d 653, 657–58 (Fla. Dist. Ct. App. 2021).

and record those activities on a consistent basis."[103] However, when data controllers access a consumer's precise geolocation data through her cell phone, they do not collect video footage.[104] It would thus be difficult to argue that access and sale of location data violated a consumer's right to not be physically or virtually "seen." Therefore, *Jackman* could stand for the proposition that tracking and selling precise geolocation data is *not* highly offensive to a reasonable person.

[33] Second, the Georgia Court of Appeals held in *Anderson v. Mergenhagen* that, while following a car and taking pictures of its driver does not represent a tortious invasion of privacy itself, doing so *repeatedly* violates the individual's right to privacy because the repetition crosses the line into harassment.[105] Applying this case to the geolocation tracking discussion, data controllers track a consumer's precise location as often as every two seconds, certainly a repetitious act.[106] Even still, since most consumers do not know that companies track and sell their data as often as they do, such repetitious offenses would likely not constitute harassment because virtual tracking does not threaten or invade an individual's daily life in the same way. *Anderson* is thus another case that could distinguish geolocation tracking from conduct a reasonable person would consider highly offensive. That said, as will be explained in Part III.C, current evidence points to consumers indeed viewing geolocation tracking as a "highly offensive" practice.

[34] Though the purpose of the intrusion upon seclusion tort is to "be let alone,"[107] consumers often do not realize how frequently companies track and sell precise geolocation information. The consumers are likely still

[103] *Id.* at 656–57.

[104] *Id.* at 656.

[105] Anderson v. Mergenhagen, 642 S.E.2d 105, 110 (Ga. Ct. App. 2007).

[106] Valentino-DeVries et al., *supra* note 1.

[107] *See* Warren & Brandeis, *supra* note 65, at 193, 195–96.

being "let alone" because of their ignorance with regard to how much of their personal information is being sold. As Part III.C explains, ignorance is not necessarily bliss in knowing how often companies track and sell precise geolocation data.

C. How Precise Geolocation Tracking and Tort Law Interact

[35] Though some consumers err on the side of allowing precise geolocation tracking to enhance and personalize their online experiences, most find it surprising and even offensive to discover how often their geolocation is tracked and sold.[108] A "reasonable person" would more likely than not consider precise geolocation tracking "highly offensive"[109] and, therefore, a violation of the intrusion upon seclusion tort. However, even if the practice violates tort law, consumers waive that protection by consenting to companies' tracking practices without understanding the full implications of that waiver.

1. Arguments for Why Geolocation Tracking is Unreasonable

[36] Most Americans consider precise geolocation tracking to be unreasonable and offensive.[110] A 2010 survey showed that a majority of Americans fear losing their privacy as a result of geolocation tracking on their phones.[111] Of those surveyed, 46% of women were "highly concerned"

[108] *See infra* Part III.C.1–2.

[109] *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see also infra* Part III.C.1–2.

[110] *See generally* Timothy J. Van Hal, *Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection*, 15 VAND. J. ENT. & TECH. L. 713, 728–29 (2013); Kaja J. Fietkiewicz & Aylin Ilhan, *Fitness Tracking Technologies: Data Privacy Doesn't Matter? The (Un)Concerns of Users, Former Users, and Non-Users*, 53RD HAW. INT'L CONF. ON SYS. SCIS., 3446–47 (2020).

[111] Van Hal, *supra* note 110, at 728.

stalkers would get their information, and 45% of all participants were "highly concerned" about letting a potential burglar know when they were not home.[112] In another study of users and non-users of fitness-tracking applications, the researchers found that current users, former users, and non-users of such apps all agreed GPS data is highly sensitive information.[113]

[37] An individual's precise geolocation can, on the other hand, assist in emergency situations.[114] For example, parents may check their child's location if she is not home by curfew, parole officers may check a parolee's location to know if she has been in a restricted area, and caregivers may check a dementia patient's location to ensure she is not wandering.[115] Viewing this behavior with a more discerning eye, these same authority figures check an individual's location with the intent of identifying misbehavior to later discipline.

[38] Though that conduct may have its benefits, as described later in this section, individuals should at least be properly informed of the existence and sophistication of the data tracking. The individual should know that authority figures track their precise latitude and longitude, not just their general vicinity.[116] Put another way, "[i]t is ethical for the person being

[112] *Id.* at 728–29.

[113] Fietkiewicz & Ilhan, *supra* note 110, at 3447.

[114] Andrew Mcnamee, *Ethical Issues Arising from the Real Time Tracking and Monitoring of People Using GPS-based Location Services* (Oct. 25, 2005) (Information and Communication Honours Thesis, University of Wollongong) (available at: https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1003&context=thesesinfo) [https://perma.cc/T97N-JEN4].

[115] *Id.*

[116] *Id.*

tracked to be given clear information about the consequences [of such tracking]."[117]

[39] A federal district court in 2012 agreed that individuals have a reasonable expectation of privacy when it decided the case of *Goodman v. HTC America, Inc*. In *Goodman*, the plaintiffs alleged a cell phone manufacturer and application developer "installed a local weather application ostensibly to provide convenient weather reports," but the developer actually used the app "to transmit the plaintiffs' locations for other purposes, including for 'fine' geographic location data," which is another word for precise geolocation data.[118] The court held that collecting precise geolocation data violated the plaintiffs' right to privacy under the California Constitution because the plaintiffs had a "reasonable expectation of privacy under the circumstances."[119] The court noted that collection of precise geolocation data is "more sensitive" than collecting addresses or phone numbers because "people often carry their smartphones with them wherever they go."[120]

[40] The average person does not understand how few privacy laws there are to protect them.[121] A study revealed that "Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them."[122] This suggests American consumers have insufficient notice of how companies will use their geolocation data when consenting

---

[117] *Id.*

[118] Theodore F. Claypoole & Richard C. Balough, *Developments in the Law Concerning Geolocational Privacy*, 68 BUS. L. 197, 202 (2012), https://www.jstor.org/stable/pdf/23527084.pdf [https://perma.cc/QYQ3-8R6Q].

[119] Goodman v. HTC Am., Inc., No. C11-1793MJP, 2012 U.S. Dist. LEXIS 88496, at *37, *41 (W.D. Wash. June 26, 2012).

[120] *Id.* at 43.

[121] Mura, *supra* note 34, at 81.

[122] Turow et al., *supra* note 74, at 4.

to a company's privacy policy.[123] And, speaking of privacy policies, "[m]ost [consumers] choose not to read them . . . and those that do find them unclear and excessively long."[124] In a 2009 study, a majority of American adults believed that a law should give them the right to access all information a website has about them.[125] Luckily, state governments heeded studies like that and began enacting privacy laws, such as the VCDPA.

2. Arguments for Why Geolocation Tracking is Reasonable

[41] For some, precise geolocation tracking provides advantages, the most obvious of which is to provide law enforcement with the enhanced ability to catch criminals.[126] Though still controversial in its Fourth Amendment warrant requirement implications, tracking criminals' cell phone location data certainly assists law enforcement.[127] In one case, law enforcement tracked a cocaine dealer's location to find evidence to convict him of drug trafficking.[128] In less extreme examples, tracking and storing

[123] Mura, *supra* note 34, at 81.

[124] M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1032 (2013).

[125] Turow et al., *supra* note 74, at 3.

[126] *How GPS Tracking Helps Police Catch Criminals*, GPS TECHNOLOGIES (Feb. 7, 2019), https://gpstechnologies.com/2019/02/how-gps-tracking-helps-police-catch-criminals/ [https://perma.cc/THL4-7PWL].

[127] *See Why It Matters*, LOCATION PRIV., https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/PrivacyAndGPS/why-it-matters/index.html [https://perma.cc/K66G-GBVB] (last visited Mar. 18, 2024).

[128] *Id.*

location data critically informs city planning, supply chain monitoring, and disaster planning.[129]

[42] Some consumers prefer tracking because they find the resulting app customization to be useful and convenient.[130] For example, Ms. Magrin, the teacher mentioned in the Introduction, likes that her tracking technology records and saves her jogging routes.[131] Additionally, a 2022 survey found that 81% of Generation Z and 57% of Millennial respondents liked personalized ads[132]—which could not be personalized without access to respondents' sensitive data. Consumers often benefit monetarily from sharing their personal data,[133] such as receiving 15% off a clothing purchase if they provide the company with their email address. Thus, receiving discounts and rewards for sharing personal data often incentivizes consumers to forfeit their privacy rights.[134] One chief executive of a mobile advertising firm described it this way: "You are receiving [online] services for free because advertisers are helping monetize and pay for it [by profiting off your data]. . . . You would have to be pretty oblivious if you are not aware that this is going on."[135]

---

[129] Jason Sarfati, *Making the case for a new geolocation data privacy paradigm*, IAPP (Aug. 25, 2022), https://iapp.org/news/a/making-the-case-for-a-new-geolocation-data-privacy-paradigm/ [https://perma.cc/Z6QG-ZGZT].

[130] Valentino-DeVries et al., *supra* note 1.

[131] *Id.*

[132] *Share of consumers who liked personalized ads in the United States as of March 2022, by generation*, STATISTA (Aug. 17, 2023), https://www.statista.com/statistics/796167/us-internet-users-primary-attitude-personalized-video-ads/ [https://perma.cc/F52V-XCBT].

[133] Valentino-DeVries et al., *supra* note 1.

[134] *Id.*

[135] *Id.*

[43] At the same time, most mobile applications do not explicitly alert consumers that their information is used for targeted advertising.[136] In 2018, *The New York Times* tested 20 applications to analyze their uses of consumer geolocation data.[137] In total, 17 of the 20 apps sent exact latitude and longitude coordinates to roughly 70 businesses.[138] Of the 17, only three on iOS and one on Android informed the consumer that their data could be used for advertising.[139]

[44] This is concerning because, in a legal system that traditionally values informed consent, the data privacy world takes a dangerously relaxed approach. One chief executive even admitted that "[m]ost people don't know what's going on," so the duty to comply with data-gathering regulations falls squarely on the companies themselves.[140] But another executive noted that "[t]here are really no consequences" for companies that do not protect location data "other than bad press that gets forgotten about."[141] In other words, companies looking to exploit consumer data can easily do so without obtaining a consumer's informed consent.

[45] App developers and other companies could argue that, if a consumer opens an app in their home, they invite the app developer's intellectual property into their home. In other words, the consumer technically accesses the *company's* property and enters *its* space, not the other way around. But the law does not consider intellectual property and physical property

[136] *Id.*

[137] *Id.*

[138] Valentino-DeVries et al., *supra* note 1.

[139] *Id.*

[140] *Id.*

[141] *Id.*

equally.[142] There is a vital difference between expectations of privacy in public and within one's home; the VCDPA makes no distinction, but tort law does.[143]

[46] Overall, precise geolocation tracking "can potentially save lives but at the expense of a person's right to privacy."[144] The reality is that most consumers do not know that a company can observe how long they stay in each room of their house and learn about their activities within each room. Therefore, since most Americans oppose the supposed "benefits" of geolocation tracking once they realize the privacy cost,[145] the scale tips toward precise geolocation tracking constituting something highly offensive to a reasonable person, thus violating the intrusion upon seclusion tort. If a consumer does not like the idea of being tracked in public, which she has no control over, tracking in her own home should naturally cause even more concern.

D. Challenges of Implementing and Enforcing Informed Consent

[47] Even if precise geolocation tracking would highly offend a reasonable person, often a consumer gives a company her express consent to track her location, thereby relieving the company of any civil liability for invading her privacy. "Arguably the biggest privacy concern related to geolocation is that users give consent presumably without fully

[142] *Property and Intellectual Property*, BUS. ETHICS, https://philosophia.uncg.edu/phi361-matteson/module-6-privacy-property-and-technology/property-and-intellectual-property/ [https://perma.cc/TL6P-W46M] (last visited Mar. 18, 2024).

[143] *See* 3 BUS. TORTS § 33.02 (LexisNexis 2023). This Note does not address the data that smart fridges, smart TV's, smart speakers like Alexa, and other smart devices collect in a person's home.

[144] Mcnamee, *supra* note 114.

[145] Mura, *supra* note 34, at 81–82.

understanding the consequences."[146] Thus, since most consumers give their express consent for companies to access, process, and sell their precise geolocation data, they likely have no claim or recourse under the intrusion upon seclusion tort.[147]

[48] Virginia tried to address the consent problem by forcing companies to obtain "affirmative" consent before processing their sensitive data, meaning Virginia consumers must expressly opt-in to companies accessing and processing their geolocation data.[148] This was a significant step above what the European Union's GDPR traditionally required of companies, which did not require obtaining any consumer consent before collecting their geolocation data.[149] In fact, some do not believe geolocation data merits a consent or opt-in standard at all because "one's location does not relate to an inherently personal characteristic of an individual—namely because one's location is always changing."[150] Even still, requiring affirmative consent to access home-roaming data provides greater individual protection than not requiring consent at all. Having educated consumers means companies cannot exploit consumers' sensitive data and violate their protected right to privacy within their own home. Since tort law treats public tracking and tracking within the home differently, privacy laws should also treat the two differently.

[49] Even requiring affirmative consent does not result in companies getting punished for violating consumer privacy. For example, in the 2014 case of *Cousineau v. Microsoft Corporation*, the plaintiff sued Microsoft for allegedly obtaining unauthorized access to her geolocation data through her cell phone's camera application after the plaintiff had *explicitly* selected

[146] *Id.* at 85.

[147] *Id.* at 86–87.

[148] V.A. CODE. ANN. § 59.1-575 (2023).

[149] Sarfati, *supra* note 129.

[150] *Id.*

"cancel" when the prompt "Allow the camera to use your location?" came up after she opened the camera application.[151] The court defined "exceeding authorized access" as occurring "when a party accesses information that the party has no authority to see, or information that is stored in a place where the party has no authority to be."[152]

[50] In that case, the plaintiff allowed other applications on her cell phone to access her location when necessary, and no evidence in the record indicated that the camera application accessed her location in additional ways.[153] The court found:

> No setting gave [the plaintiff] control over the precise times that her phone's location framework would access the RAM-stored data. It is thus inaccurate to say that she denied Microsoft access to location information at any particular point in place or time. At most, she could simply have expected that her location information would not be used by the camera application.[154]

Accordingly, though Microsoft's practices may have been "deceptive," it ultimately got off the hook.[155] In this case, it seemingly made no difference to the court whether Microsoft tracked the plaintiff's location within her home or in public. But this distinction should be an important factor in a court's analysis of geolocation tracking violations because tort law treats public tracking differently than in-home tracking.

---

[151] Cousineau v. Microsoft Corp., 6 F. Supp. 3d 1167, 1170 (W.D. Wash. 2014).

[152] *Id.* at 1171.

[153] *Id.* at 1172.

[154] *Id.* at 1174.

[155] *Id.*

[51] In another case, *In re iPhone/iPad Application Consumer Privacy Litigation*, the plaintiffs alleged that Apple "collected precise home and workplace locations and 'current whereabouts' of the plaintiffs by using certain features of iPhone and iPad operating systems and applications" without the plaintiffs' knowledge.[156] Ultimately, the plaintiffs' allegations failed.[157] Again, if Apple tracked the plaintiffs within their own homes, that fact should have mattered to the court.

[52] Thus, the question of whether *informed* consent, not just consent, should be required in geolocation tracking cases is an ongoing debate. It is unethical and arguably unconscionable to exploit consumer data for capital gain, particularly where the consumer did not realize she consented to a provision that constitutes a tortious violation of her privacy.

1. Arguments For and Against Providing Notice to Consumers

[53] While the following explanations apply to privacy laws affecting consumers when they step outside of their homes, there is little known about what it would look like to provide notice for *in-home* tracking. Particularly for the purposes of notifying consumers, in-home geolocation tracking should be treated differently than public geolocation tracking.

[54] There are drawbacks to requiring companies to provide notice to their consumers regarding tracking inside and outside the home. For example, the growing burden on companies to provide proper notice may impede innovation and result in less useful and personalized services for consumers.[158] Especially considering that extensive evidence shows most consumers do not read the privacy notices, even when they are forced to

[156] Claypoole & Balough, *supra* note 118, at 202.

[157] In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1040 (N.D. Cal. 2012).

[158] Calo, *supra* note 124, at 1049.

"click through" them on the way to content or services,[159] companies may view writing the policies as a waste of time and money. Even the sitting Chief Justice of the United States Supreme Court admits he does not read terms of service.[160]

[55] But an average American may be more likely to read geolocation-related terms because geolocation privacy notices are already treated differently than other privacy notices. At least on iPhones, an entirely separate pop-up window appears and asks for a consumer's geolocation tracking preference when they first download an app.[161]

[56] One example of a privacy notice that most consumers clearly did *not* read is a provision in a video game company's terms of service that, unless the user opted out, "the company would retain rights to the user's eternal soul."[162] Examples like this are alarming. Even still, bizarre examples likely would not cause consumers to read companies' privacy policies or other terms of service. Even if they did, reading every privacy policy might not make economic sense. Researchers at Carnegie Mellon once calculated that "it would cost $781 billion in worker productivity if everyone were to read all of the privacy policies they encountered online in one year."[163]

[57] Another reason providing notice may not provide the best solution for consumer protection relates to the notices' readability. Companies typically write notices at a college reading comprehension level, but the

[159] *Id.* at 1051–52.

[160] *Id.* at 1052.

[161] APPLE SUPPORT, *About privacy and Location Services in iOS, iPadOS, and watchOS,* https://support.apple.com/en-us/102515 [https://perma.cc/2J5E-JPYC] (last updated Mar. 27, 2024).

[162] Calo, *supra* note 124, at 1052.

[163] *Id.*

average American reads at an eighth or ninth grade level.[164] Also, companies almost always write the policies in English and do not provide translations for consumers whose first language may not be English.[165] For both of these reasons, even if consumers read the policies, an average consumer might not comprehend what rights they forfeit to the company by accepting the policies' terms.

[58] That said, notice is a popular solution for many companies.[166] Privacy notices can "furnish[] consumers with information they would not otherwise have so they can protect themselves and police the market."[167] Giving consumers proper notice theoretically arms them with all the information needed to make the best choice for themselves regarding how much privacy to waive.[168] "The hope is that informed consumers create a market that rewards companies for good privacy practices and penalizes them for bad ones."[169]

[59] Companies shield themselves from liability by including a privacy policy or other type of privacy notice; courts often consider the existence or absence of notice as evidence of how much a consumer understood the product or service.[170] Requiring notice is also an inexpensive way for regulators to protect consumers.[171] Lastly, mandated notice may be more

[164] *Id.* at 1053.

[165] *Id.*

[166] *Id.* at 1050.

[167] Calo, *supra* note 124, at 1044.

[168] *Id.* at 1049.

[169] *Id.*

[170] *Id.* at 1046.

[171] *Id.* at 1048.

politically "palatable" than federal regulations.[172] "Regulators, eager to do something to help consumers, but lacking the political capital or will to limit or curtail the activities of a given industry, may opt for notice as a means at least to improve the context of online privacy for some consumers."[173]

[60] Again, the above explanations and arguments for providing—or not providing—notice to consumers apply mainly to *public* geolocation tracking contexts. This Note's recommendations apply to in-home tracking instead of public tracking, but one must fully understand both landscapes before considering policy action.

E. Recommendations for Virginia

[61] Virginia lawmakers should explicitly identify what consumers consent to when they allow companies to track, process, and sell their precise geolocation data so that they knowingly waive their right to privacy within their homes. They should also implement an additional geofencing control for smart homes to allow homeowners to manage the tracking of their data within their own home.

1. Recommendation #1: Require a Warning Pop-Up Window

[62] Despite its flaws, most companies currently follow the notice model as explained above. Therefore, this Note's first recommendation to Virginia follows that model. The recommendation requires companies to add a short warning pop-up window every time a consumer gives the company's app constant access to her precise geolocation data.

[63] On most current smartphones, when a consumer first downloads or uses an app, the app asks the consumer to select a preference of how often the company can track her location. The consumer may click "always

[172] Calo, *supra* note 124, at 1050.

[173] *Id.*

allow," "allow while using the app," or "never allow."[174] Those are the only options a consumer has when first providing her consent. As discussed earlier, companies do not always respect consumers' express wishes when tracking their geolocation data, even if they click "never allow."[175] Nevertheless, this is the current system and method by which many companies are "requesting" consent from their consumers to track geolocation data.

[64] Using this Note's recommendation, if the consumer clicks, "always allow," companies should then be required to display a short warning pop-up that informs the consumer that she is allowing the company to violate her privacy beyond what tort law typically allows. The warning language should be written to the average eighth or ninth grade American reading level.[176] Here is a possible example of the warning pop-up language:

> *Please note that this app will take, process, and sell your precise GPS coordinates as often as every two seconds. You generally have a right to privacy within your home, which you may be waiving by allowing [X company] to track your movements within your home. Once you've consented to this, the app is legally permitted to track you everywhere.*

Even if consumers only read or glance over this pop-up the first time they see it, that alone represents a leap in the right direction in encouraging informed consent in Virginia. Unlike terms and conditions, which take an average of 30 minutes to read,[177] the short example paragraph only takes at most 15 seconds to read. Additionally, if a consumer must forcibly click

[174] Cousineau v. Microsoft Corp., 6 F. Supp. 3d 1167, 1170 (W.D. Wash. 2014).

[175] *Id.*

[176] Calo, *supra* note 124, at 1053.

[177] Matt Gaedke, *How Long Does It Take to Read the Terms of Service of Popular Online Services?*, DAILY INFOGRAPHIC (Oct. 18, 2021), https://dailyinfographic.com/how-long-does-it-take-to-read-the-terms-of-service [https://perma.cc/Y75A-TMQD].

through yet an additional waiver of consent, it would presumably provide an additional signal to her brain that she should read the notice.

2. Recommendation #2: Add a Geofencing Control

[65] This Note also recommends that Virginia legislators require companies to enable a geofence around a consumer's home so the consumer can choose when she wants her data collected. A geofence is an invisible radius that smart homeowners draw around their home to enable smart devices "to automatically activate when [they] leave home or return—an event that is (usually) determined by the location of [their] smartphone."[178] For example, once a homeowner sets up a geofence around her property and drives away from the smart home, the home can lock the doors and turn off the air conditioning on its own.[179] It can also detect when the homeowner nears the home and will automatically open up the garage door and turn on the house lights so the homeowner can enter her home seamlessly.[180]

[66] Geofencing gives homeowners a sense of control over their home because they pre-select each specific setting. To encourage even more control and home privacy, smart devices could ask homeowners whether they want their geolocation data tracking services turned off once they enter their home. As this Note has established, tort law treats privacy differently inside and outside one's home. Thus, it would be ethical and beneficial to add a control onto a smart home geofence that allows homeowners to control how they are tracked.

[67] The geofencing tool's default could—and should—be that geolocation tracking services automatically turn off once a homeowner

---

[178] Eric Chiu, *Geofences Make Your Home Work Better. Here's How.*, N.Y. TIMES WIRECUTTER (June 10, 2022), https://www.nytimes.com/wirecutter/blog/geofencing-smart-home-devices/ [https://perma.cc/ER5A-8VDZ].

[179] *Id.*

[180] *Id.*

enters the geofence radius and automatically turn on when she leaves the radius, unless the homeowner explicitly turns off the geofence control. The smart device could periodically ask the homeowner whether she still wants her geolocation tracking services turned off. Alternatively, the default could be that geolocation tracking services stay on even within the home, and the homeowner must manually turn the tracking off. In either event, an additional geofence control would rightly treat a person's home differently than public areas.

[68] In addition, a homeowner could potentially decide which data trackers could access her data. The default should be that the geofence blocks *all* trackers. But, for example, if one of the trackers is the homeowner's mobile carrier needing location data to send a cell signal, the homeowner should be able to manually allow her carrier into the geofence to receive cell service. Even so, not having a cell signal within one's home these days could prove to be problematic if the Wi-Fi stops working. So, whether mobile carriers should even have the power to withhold cell service from inside a geofence unless given access to the homeowner's sensitive data is an important consideration.

3. Other Recommendations

[69] Other recommendations for Virginia lawmakers and companies include making a company's privacy policy easier for consumers to understand by converting the "legalese" into plain language, placing the policies in a table format, or otherwise standardizing disclosure.[181] But studies show only marginal improvement in consumer understanding with improved company privacy policies.[182] Some argue getting rid of the consent requirement altogether would fare better because, if consent is required for every use of precise geolocation tracking, then presumably

[181] Calo, *supra* note 124, at 1033.

[182] *Id.*

positive uses of geolocation tracking such as catching criminals and disaster planning could become obsolete tools.[183]

[70] Regardless, it is time for the federal government to establish a comprehensive data privacy law nationwide. As the trendsetter, the VCDPA is a great place to start since it considers precise geolocation data to be sensitive and requires companies to obtain consent from consumers before processing and selling their data.[184] Though, as this Note discusses, consent alone may not be enough to make such processing ethical; informed consent is a much better standard to implement.

IV. CONCLUSION

[71] The Virginia Consumer Data Protection Act is a step in the right direction in the data privacy protection landscape because it protects consumers from companies tracking, processing, and selling their data without consent. Yet studies show consumers do not actually know what they consent to when they "accept" privacy policy conditions. Virginia could better encourage Virginian consumers to make data privacy decisions with informed consent. One way to do that is to require companies to add a short warning pop-up window when consumers allow their apps to have constant access to their location data. Another way is to require a geofencing control on smart homes that allows homeowners to control how much data is processed and sold to third parties. With such protections in place for consumers, companies will better respect the "right to be let alone" within one's home.

[183] *See* Sarfati, *supra* note 129.

[184] Amy C. Pimentel, *Virginia Consumer Data Protection Act: A Growing Wave of Comprehensive State Privacy Laws*, MCDERMOTT WILL & EMERY (Feb. 23, 2021), https://www.mwe.com/insights/virginia-consumer-data-protection-act-a-growing-wave-of-comprehensive-state-privacy-laws/ [https://perma.cc/ZX5B-7AFE].