JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOLUME 10 • ISSUE 1 • 2019

IS THE GRASS GREENER ON THE OTHER SIDE OF THE GEOFENCE? THE FIRST AMENDMENT AND PRIVACY IMPLICATIONS OF UNAUTHORIZED SMARTPHONE MESSAGES

Kearston L. Wesner[1]

ABSTRACT

Geofencing technology enables companies to obtain users' physical location and deliver customized communications, including political messages. But to accomplish this, some businesses transmit user data to third parties without consent. The privacy tort of intrusion and Federal Trade Commission actions target unfair or deceptive practices, but these avenues are inadequate. Users' privacy should be safeguarded by creating a federal privacy statute that requires opt-in notification and periodic reminders of data collection, usage, and transmission practices.

Keywords: Communications, data collection, data privacy, Federal Trade Commission, geofencing, technology, torts

[1] Assistant Professor of Media Studies, Quinnipiac University. B.A., 1996, Linguistics, University of Florida; M.A., 1998, Linguistics, University of Texas at Austin; J.D., 2001, Cornell Law School; Ph.D., 2012, Mass Communications, University of Florida.

CONTENTS

INTRODUCTION

"Pregnancy Help."

"You Have Choices."

"You're Not Alone."

In 2015 and 2016, young women in or near various medical facilities (including reproductive health clinics and methadone clinics) in five states received messages like these on their smartphones.[2] The messages ostensibly were designed to discourage "abortion-minded women"[3] from terminating pregnancies at the clinics. But the messages weren't invited, and they weren't welcome. They were thrust upon the smartphone users by a company called Copley Advertising. To accomplish this feat, Copley used a technology called geofencing.

Geofencing is a location-based tool targeting users of internet-enabled devices, such as smartphones, in a predefined area. Through Global Positioning

[2] These facilities were located in New York City; Columbus, Ohio; Richmond, Virginia; St. Louis, Missouri; and Pittsburgh, Pennsylvania. Assurance of Discontinuance Pursuant to G.L. 93A, §5, *In re* Copley Advertising, LLC (Apr. 4, 2017) [hereinafter *Assurance of Discontinuance*], at 3.
[3] AG Reaches Settlement with Advertising Company Prohibiting "Geofencing" Around Massachusetts Healthcare Facilities (Apr. 4, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html.

System (GPS) coordinates, individuals or companies can define geographic perimeters and build virtual fences (called "geofences") around these areas.[4] Identifying information from the users' smartphones—such as GPS information or wireless Internet access information[5]—can then be used to target users within, or exclude them from, that virtual boundary.[6]

Often, this technology is relatively benign. For example, the retail company Target uses geofencing technology to push advertisements to prospective shoppers within a certain radius of Target stores.[7] When potential customers enter that predefined radius, they receive messages regarding various deals at Target. To obtain these notifications, though, users must have the Target mobile application installed, have Bluetooth turned on, and opt in to receive these messages.[8] Because these users elect to receive such advertising, and can stop receiving the messages at will by disabling or removing the app or turning off Bluetooth, this use of geofencing technology typically poses few legal or ethical concerns—assuming that the users have been properly notified of how their data is being used.[9]

Copley's practices were detailed in an Assurance of Discontinuance ("Assurance") entered into between Copley and the Attorney General of Massachusetts in April 2017.[10] According to the Assurance, Copley's use of geofencing technology was arguably more nefarious because it identified, or "tagged," users' smartphones and caused third-party advertisements to display on mobile applications for up to 30 days. When users clicked on the messages, a webpage opened with abortion alternatives and access to a live "pregnancy support

[4] Thomas C. Gallagher, *The Virtual Bathroom Stall: Solving the Headache of Geo-Based Anonymous Message Applications*, 85 GEO. WASH. L. REV. 922, 935 (2017); Diana Graber, *Yik Yak App Makers Do the Right Thing*, HUFFINGTON POST: BLOG (Mar. 26, 2014, 6:10 PM ET), http://www.huffingtonpost.com/diana-graber/yik-yak-app-makers-do-the_b_5029679.html.
[5] The information transmitted by the smartphone that can be used to determine whether a user has entered or exited the designated area includes "latitude, longitude, GPS (Global Positioning System) information, IP (internet protocol) address, wireless Internet access information, so-called Bluetooth technology, Near-Field Communication ("NFC") information, or device identification information." Assurance of Discontinuance, *supra* note 1, at 2.
[6] Graber, *supra* note 4.
[7] Sarah Perez, Target Launches Beacon Test in 50 Stores, Will Expand Nationwide Later This Year, TECHCRUNCH (Aug. 5, 2015), https://techcrunch.com/2015/08/05/target-launches-beacon-test-in-50-stores-with-expanded-rollout-later-this-year/.
[8] *Id. See generally* Sophia Martin Schechner, *Beacon Technology and the Future/Present State of E-Commerce Retail Sales*, 26 ALB. L.J. SCI. & TECH. 172, 178-179 (2016) (explaining how retailers use Bluetooth Low Energy (BLE) beacon technology to reach consumers within predefined virtual borders).
[9] Schechner, *supra* note 8, at 181.
[10] Assurance of Discontinuance, *supra* note 2, at 1.

specialist."[11] Copley's sole employee, John Flynn, asserted that Copley could "set up a mobile geofence around an area—Planned Parenthood clinic[s], hospitals, [and] doctor's offices that perform abortions."[12] In fact, Flynn claimed that Copley could "tag all the smartphones entering and leaving the nearly 700 Planned Parenthood clinics in the U.S."[13] On Twitter, Flynn further noted that "Copley's advertising can drill down to age and gender."[14]

For example, Copley contracted with two companies: Bethany Christian Services, which provides pregnancy counseling, and RealOptions, which has California-based crisis pregnancy centers. Copley determined the geolocation of users near various medical facilities and disclosed that information to Bethany and RealOptions so the third parties' messages could be delivered to the targeted users. Users who received the messages were unaware that Copley had tagged their devices or disclosed their geolocation.[15]

The Assurance of Discontinuance states that after learning of Copley's practices in other states, Massachusetts Attorney General Maura Healey proactively sought to characterize them as "unfair or deceptive" under the Massachusetts Consumer Protection Act. Specifically, Healey said Copley's practices "intrude[ ] upon a consumer's private health or medical affairs or status and/or result[ ] in the gathering or dissemination of private health or medical facts about the consumer without his or her knowledge or consent."[16] Although admitting no fault in the Assurance, Copley promised to abstain from geofencing within "the Vicinity of any Medical Center located in the state of Massachusetts to infer the health status, medical condition, or medical treatment of any person."[17]

The Assurance raises some questions, however. First, Copley claimed its First Amendment rights were violated because corporate political speech is protected by the First Amendment. And second, Copley argued that its "right to free speech should not be marginalized because government officials do not agree with the message of their advertisement."[18] If Healey, in fact, censured Copley based on its message *content*, then Copley's argument has weight. To add fuel to

[11] *Id*. at 2-4.
[12] *Id*. at 3.
[13] *Id*. at 4.
[14] Curt Woodward & Hiawatha Bray, *A Company Sent Anti-Abortion Ads by Phone. Massachusetts Wasn't Having It.*, BOSTON GLOBE (Apr. 4, 2017), https://www.bostonglobe.com/business/2017/04/04/healey-halts-digital-ads-targeted-women-reproductive- clinics/AoyPUG8u9hq9bJUAKC5gZN/story.html.
[15] *Assurance of Discontinuance*, *supra* note 2, at 3-4.
[16] *Id*. at 4-5.
[17] *Id*. at 7.
[18] Woodward & Bray, *supra* note 14.

this argument, numerous other companies use geofencing technology without attracting the attention of the Attorney General of Massachusetts.

This study explores the relationship between the First Amendment and regulating the use of geofencing technology to deliver targeted messages. The paper poses three questions: (1) can Copley's practices be curbed consistent with the First Amendment; (2) to what extent, if any, do Copley's practices violate individuals' privacy expectations; and (3) what would reasonable restrictions on the use of geofencing technology include?

To analyze these questions, this study employed traditional legal research methodology. A Westlaw search identified relevant law review articles for background information. Additionally, a Westlaw search for all federal and state cases involving the terms "geolocation" or geofencing" yielded 408 cases, which were filtered to exclude criminal cases (involving governmental use of geolocation technologies for surveillance purposes) and cases unrelated to privacy. The remaining 315 cases—mostly from the Northern District of California—were analyzed to determine how courts have viewed the privacy implications of electronic data collection and use, including geolocation technology. Finally, this paper also analyzed Federal Trade Commission ("FTC") reports to inform the analysis of the FTC's guiding principles regarding geolocation technology.

I. CORPORATE POLITICAL SPEECH AND THE FIRST AMENDMENT

Copley's speech has been characterized as "quite crass behavior" and even "predatory."[19] Yet Copley claimed Healey unfairly targeted the content of its speech in violation of the First Amendment.[20] This section argues that in light of Supreme Court decisions on abortion-related speech, Healey's actions in censuring Copley could be read as consistent with First Amendment principles. The key here is that if Healey's actions focused not on the content of Copley's speech, but on the "predatory" nature of Copley's practices—particularly the unauthorized use of geofencing technology to obtain and share users' sensitive information with third parties—then Healey's actions would pass muster. However, if Healey were to have targeted Copley based on the content or "crassness" of Copley's messages, this would violate the First Amendment.

Corporate political speech—which includes even crass corporate speech—is strongly protected under the First Amendment. In *Citizens United v. Federal Election Commission*, the Supreme Court held that the First Amendment protects

[19] *Id.*
[20] *Id.*

the core political speech of companies just as strongly as it does for individuals.[21] Citizens United, a nonprofit corporation, successfully argued in that case that corporations have a First Amendment-protected right to finance speech that expressly advocates the election or defeat of a candidate for federal office.[22] Until *Citizens United*, the Bipartisan Campaign Reform Act of 2002 ("BCRA") prohibited corporations from exercising their political voice in this manner.[23] However, in invalidating the BCRA's ban on corporate expenditures, the Court affirmed that First Amendment speech rights extend not just to individuals but to corporate entities.[24] Although *Citizens United* did not equate corporations with people, it did signal that speech will be treated equally, whether it comes from a corporation or a person. Perhaps the clearest pronouncement of the Court's intentions can be found in Justice Kennedy's *Citizens United* opinion, which stated, "[P]olitical speech does not lose First Amendment protection 'simply because its source is a corporation.'"[25]

The principle that political speech should be afforded the strongest protections has been stated numerous times by the Supreme Court.[26] For example, in *Buckley v. Valeo*, the Court said:

> Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution. The First Amendment affords the broadest protection to such political expression in order 'to assure

[21] Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 364 (2010).
[22] *See Id*. In January 2008, Citizens United released *Hillary: The Movie*, a documentary critical of Hillary Clinton, in theaters and DVD. Citizens United, however, wanted to broaden its reach by making the documentary available through video-on-demand in the 30-day window before the primary election. *Id.* at 320-21. Under the Bipartisan Campaign Reform Act of 2002, corporations could not use general treasury funds to make independent expenditures for any "electioneering communication." 2 U.S.C. § 441b (2005). Citizens United brought an action against the Federal Election Commission for declaratory and injunctive relief, asserting that the BCRA's ban on corporate-funded independent expenditures was unconstitutional. *Citizens United v. Fed. Election Comm'n.* 558 U.S. at 321.
[23] *Citizens United*, 558 U.S. at 320. The *Citizens United* Court overturned two cases that regulated these corporate expenditures: Austin v. Mich. Chamber of Commerce, 494 U.S. 652 (1990), and McConnell v. Fed. Election Comm'n, 540 U.S. 93 (2003).
[24] *Citizens United*, 558 U.S. at 364 (2010).
[25] *Id*. at 342 (quoting First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 784 (1978)).
[26] *See, e.g.*, Buckley v. Valeo, 424 U.S. 1, 25, 44-45 (1976); R.A.V. v. St. Paul, 505 U.S. 377, 422 (1992) (stating that "[c]ore political speech occupies the highest, most protected position; commercial speech and nonobscene, sexually explicit speech are regarded as a sort of second-class expression; obscenity and fighting words receive the least protection of all").

> (the) unfettered interchange of ideas for the bringing about of political and social changes desired by the people.'[27]

Protecting the robust discussion of political issues is central to the First Amendment. Therefore, using consumer protection laws to stifle or silence political discourse should, as one scholar said, "give people pause."[28]

Despite the limitations implied by its name, "core political speech" is not reserved for speaking out about candidates running for office in governmental elections.[29] It encompasses a diverse array of activities, from speech about income tax referendums to the anonymous distribution of leaflets about a ballot issue.[30] In this vein, abortion-related speech has been characterized as political. Thus, the Supreme Court has on multiple occasions protected the rights of protestors who gather near abortion clinics.[31] Copley's speech is also not just commercial, but political, and should realize the same heightened First Amendment protections.[32] Content-based regulations aimed at curbing Copley's speech would therefore be subject to strict scrutiny.

Even if Copley's speech is political, though, the analysis would not cease here. The question would morph into whether Copley's speech could (or should) still be regulated consistent with First Amendment principles. Supreme Court decisions on abortion-related speech, particularly with respect to reasonable buffer zones, provide an avenue to curb Copley's practices without stifling corporate speech rights.

In *Hill v. Colorado*, the Supreme Court found constitutional a Colorado statute requiring a 100-foot buffer around abortion clinics, designed to protect women from "sidewalk counseling," including "efforts 'to educate, counsel, persuade, or inform passersby about abortion and abortion alternatives by means of verbal or written speech.'"[33] The *Hill* Court was particularly concerned about protecting women from "strong and abusive language in face-to-face encounters."[34] The Court focused on the *behaviors* targeted by the statute: "the harassment, the nuisance, the persistent importuning, the following, the dogging, and the implied

[27] *Buckley*, 424 U.S. at 14.
[28] Woodward, *supra* note 14, at 4.
[29] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 347 (1995).
[30] First Nat'l Bank of Bos. v. Bellotti, 435 U.S. 765, 776 (1978); *McIntyre*, 514 U.S. at 347.
[31] *See* McCullen v. Coakley, 134 S. Ct. 2518, 2537 (2014); Madsen v. Women's Health Ctr., Inc., 512 U.S. 753, 776 (1994).
[32] *See, e.g.*, Citizens United v. FEC, 558 U.S. 310, 340 (2010); R.A.V. v. St. Paul, 505 U.S. 377, 422 (1992).
[33] Hill v. Colorado, 503 U.S. 703, 708 (2000).
[34] *Id*. at 710.

thread of physical touching."[35] The Colorado statute did not target a particular viewpoint; it just "establishe[d] a minor place restriction on an extremely broad category of communications with unwilling listeners."[36] Similarly, it would be possible to craft a law regulating Copley's nefarious behavior—the use of geofencing technology to target vulnerable women without obtaining user permission in advance.

On the other side of the coin, in *Madsen v. Women's Health Center, Inc.*,[37] the Supreme Court considered an injunction that curbed speech by pro-life protesters. The injunction included a 36-foot buffer around an abortion clinic as well as other provisions including a ban on all "images observable" from the clinic, and a restriction on approaching women within 300 feet of the clinic.[38] The 36-foot buffer zone was upheld because it was a simple content-neutral time, place, or manner restriction that facilitated entering and exiting the clinic and shielded the clinic from overly loud speech.[39] But the other three restrictions unconstitutionally burdened speech. Patients who were made uncomfortable by the "images observable" from within the clinic could easily shield themselves from the images by engaging in simple behaviors such as closing their curtains.[40] The 300-foot ban on picketing was similarly overbroad:

> [I]t is difficult, indeed, to justify a prohibition on *all* uninvited approaches of persons seeking the services of the clinic, regardless of how peaceful the contact may be, without burdening more speech than necessary to prevent intimidation and to ensure access to the clinic.[41]

Central to *Madsen* is the idea that individuals should be protected from harassment and threats while alternatives that support speech should be provided.

Although *Hill* and *Madsen* initially seem at odds, when evaluated in light of Copley's behavior, they are, in fact, consistent. Together, they stand for the proposition that speech can be reasonably restricted. The restrictions, however, must be neutral and not burden more speech than necessary. Under this umbrella is

[35] *Id*. at 724.
[36] *Id*. at 723.
[37] Madsen v. Women's Health Center, Inc., 512 U.S. 753, 754 (1994).
[38] *Id*. at 759-61.
[39] *Id*. at 769.
[40] *Id*. at 773 (stating that this provision violates the First Amendment because "it is much easier for the clinic to pull its curtains than for a patient to stop up her ears, and no more is required to avoid seeing placards through the windows of a clinic").
[41] *Id*. at 774.

ample room to regulate the use of geolocation technology. If a restriction neutrally targets the unauthorized use of geofencing technology, and does not impose a viewpoint restriction on speech, then it could pass constitutional muster. Thus, there is room here to regulate Copley's activities without infringing its First Amendment rights.

Another point to consider here is the *Hill* Court's focus on "unwilling listeners."[42] This issue is critical because it raises another First Amendment concern with respect to Copley's messaging. Just as people have a First Amendment-protected right to *distribute* information, they also have a right to *receive* it.[43] According to the Court, "Freedom of speech presupposes a willing speaker. But where a speaker exists, as is the case here, the protection afforded is to the communication, to its source and to its recipients both."[44] The problem here, however, is that the Assurance prevents the public from receiving Copley's political messages. Again, though, there is a meaningful distinction between protecting one's right to receive information and penalizing a company's unauthorized commandeering of a smartphone as a tool to deliver that information. The content-neutral focus on the unauthorized use of technology alleviates the First Amendment concerns.

In the end, Copley's First Amendment-focused response to the Massachusetts action is a bit of a smokescreen. The response focused on Copley's role in delivering (or being a conduit for the delivery of) political speech. But the key problem was not the content of Copley's speech; it was the shady business practices Copley used to deliver its message. Copley's unauthorized collection and transmission of user data falls outside the purview of the First Amendment. Geolocation data is not "speech." It "is not collected, used, or sold for its expressive content at all; it is a tool for processing people, not a vehicle for injecting communication into the 'marketplace of ideas.'"[45] Copley is still free to share political messages, but it must comply with strict privacy protection practices that safeguard how users' sensitive information is collected, used, and transmitted.

---

[42] *Hill*, 503 U.S. at 716-719.
[43] Virginia State Pharmacy Board v. Virginia Citizens Consumer Council, 425 U.S. 748, 756-757 (1976) (discussing consumers' right to receive information about drug prices in the commercial speech context); Red Lion Broadcasting v. FCC, 395 U.S. 367, 390 (1969) (discussing listeners' First Amendment rights).
[44] Virginia State Pharmacy Board. v. Virginia Citizens Consumer Council, 425 U.S. 748, 756 (1976).
[45] Joseph Tomain, *Online Privacy & The First Amendment: An Opt-In Approach to Data Processing*, 83 U. CIN. L. REV. 1, 39-40 (2014).

II. THE PRIVACY OF MEDICAL INFORMATION

Privacy defies simple definition. A few constructions, though, have a more expansive reach. Arguably the most common definition was articulated by Samuel Warren and Louis Brandeis, who characterized privacy as the "right to be let alone."[46] A more detailed version of this definition describes privacy as follows:

> The right to privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communication and our freedom to associate with the people we choose.[47]

This definition focuses on autonomy—the right to moderate your behaviors as suits you and shield yourself from scrutiny.

Yet another variation enumerates five "species" of privacy rights folded into the definition of a "right to be let alone": the Warren and Brandeis right grounded in unauthorized information collection and use; the First Amendment right to be free from others' speech; the Fourth Amendment right to be free from unreasonable searches and seizures; the Fourteenth Amendment right of individual decision-making; and the broad privacy protections granted by state constitutions.[48]

There are countless other examples of scholars attempting to explain what privacy *is*. Although the definitions may be numerous and vague, two common threads emerge. The first theme is decisional privacy, or the right to make decisions about personal issues such as "marriage, procreation, contraception, family relationships, and child rearing and education."[49] The second is informational privacy, grounded in the idea that people should be able to shield certain information about themselves from the public.[50] Copley's practices involve significant informational privacy violations.

Certain types of information trigger unique privacy concerns. The heightened expectation of privacy in medical information can be seen in the proliferation of laws like the Health Insurance Portability and Accountability Act

[46] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890).
[47] Hill v. National Collegiate Athletic Association, 7 Cal. 4th 633, 644 (Cal. 1994).
[48] Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1434 (1992).
[49] Roe v. Wade, 410 U.S. 113, 152-153 (1973) (internal citations omitted); Paul v. Davis 424 U.S. 693, 714 (1976).
[50] Whalen v. Roe, 429 U.S. 589, 599-600 (1977) (recognizing the right to informational privacy, but rejecting plaintiffs' claims that New York statute mandating disclosure of prescription information to the state threatened privacy).

("HIPAA").[51] HIPAA's Standards for Privacy of Individually Identifiable Health Information, commonly known as the "Privacy Rules," articulate an individual's right to limit who can obtain and use his/her private medical information.[52] Health care providers must provide notice of how they use and share private medical data.[53] Users must also give permission before their health records can be shared.[54]

Copley's practices trigger unique informational privacy concerns because they accessed and used individuals' sensitive medical information to deliver targeted messages. The users' physical proximity to certain healthcare providers enabled Copley to discern pertinent information about their medical situation. This is why users received focused messages outlining abortion alternatives and live-chat options with pregnancy counselors. As one article noted:

> '[Copley was not] sending them ads for free gasoline or discounts at Macy's[.]' . . . 'They were sending them messages that related directly to their health and medical status, which, by definition, meant that they were improperly accessing somebody's private medical health data in a way that we feel is exploitive.'[55]

In other words, Copley was using physical location data to extrapolate sensitive medical information which, then, could be used to turn a profit.

Using geolocation data is an example of "frictionless sharing." This refers to the practice of businesses collecting users' data automatically without seeking permission for each disclosure. This type of sharing is especially appealing to businesses because it removes "friction," which is defined as those "forces which prevent individuals from disclosing personal information to online services."[56] The less overt a business's data collection practices are, the less individual friction there is. Obviously, this makes it easier for businesses to profit from their consumers. A huge problem occurs, however, when "frictionless sharing" includes uniquely sensitive information. While companies may characterize unobtrusive data collection practices as "frictionless sharing," these practices render users unable to

[51] *See generally* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).
[52] 45 C.F.R. § 164.500-164.534 (2014); s*ee also* U.S. DEP'T OF HEALTH & HUMAN SERVS., OCR PRIVACY BRIEF: SUMMARY OF THE HIPAA PRIVACY RULE (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/FN6K-P6HH].
[53] OCR Privacy Brief, *supra* note 53, at 11-12.
[54] *Id*. at 5-6.
[55] Woodward & Bray, *supra* note 14 (quoting Massachusetts Attorney General Maura Healey).
[56] Schechner, *supra* note 8, at 180.

engage in fully informed decision-making. The success of "frictionless sharing" is firmly grounded in an informational imbalance between businesses and consumers.

Even if, however, there is a deeply held belief that companies should not trade on medical information without first obtaining permission, it is functionally difficult to impose strong privacy protections for a couple of reasons.

First, businesses have come to rely on robust data collection practices. The ability to aggregate users' personal information and derive detailed information from that—and as Copley noted, being able to "drill down to age and gender"[57]—is immensely valuable "not only to marketers and advertisers but also to insurers, lenders and employers."[58] Being able to identify consumers with such specificity increases the likelihood that a business's messages will reach a uniquely receptive audience. And because collecting users' data has become cheap, easy, and lucrative, commercialized collection has become ubiquitous.[59]

Additionally, users are becoming increasingly willing to share personal information. To take full advantage of the Internet of Things—the world in which our Internet-enabled devices facilitate the exchange of information—people must divulge information about themselves.[60] The result is that data commoditization is relatively unrestrained and, predictably, consumers have reduced their privacy expectations.[61]

To illustrate these problems, one need only consider Google, which came under international fire in 2013 for its questionable data collection practices. For years, specially outfitted Google cars have photographed buildings and streets to provide data that strengthens Google Maps. Problems began to arise, however, when Google also began collecting data about Wi-Fi hotspots, which it ultimately used to learn shockingly specific real-time information about its users' locations. Google also obtained sensitive data—including sensitive medical information—from unencrypted routers. Even though Google was sanctioned in numerous countries for its shady practices, its position in the geolocation services market was

[57] Woodward & Bray, *supra* note 14.
[58] Lisa Madelon Campbell, *Internet Intermediaries, Cloud Computing and Geospatial Data: How Competition and Privacy Converge in the Mobile Environment*, 7 NO. 2 COMPETITION L. INT'L 60, 62 (2011).
[59] *Id*.
[60] Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U. L. REV. 1183, 1197 (2017).
[61] Madelon Campbell, *supra* note 58, at 62 (noting that "the plummeting cost of collecting, sharing and using personal data, and the utility of personal data as a financial underlay for many online services, are fundamentally transforming traditional notions of privacy").

ultimately strengthened.[62] What could possibly incentivize a business to safeguard its users' privacy when there is no effective deterrent to unfettered data collection, especially when these businesses can experience significant financial windfall from their unauthorized data collection practices? As one scholar explained, "[T]here is little incentive for the design of systems which restrict collection of personal data."[63]

Even given businesses' preferred practices and users' concomitant limited expectations, users still recognize that they have some expectations of privacy, which must be protected. Users who rely on smartphones understand that their reliance comes with privacy tradeoffs. A Pew Research Center survey of 2,254 adults revealed that because of privacy concerns, 19% of cell phone users disabled their phone's tracking abilities.[64] Furthermore, the survey indicated that 54% of the respondents declined to install at least one app, and 30% of users uninstalled an app, due to concerns about data collection practices.[65] These numbers were consistent among both Android and iPhone users. So, clearly, privacy remains a concern to users despite their general recognition that they have less overall expectation of privacy.

Despite users' obvious concern, little has been done to protect their privacy, leading to the lament of some scholars.[66] A few statutes, such as HIPAA and the Stored Communications Act (SCA)[67], protect consumers from the unauthorized use of their data. However, these statutes do not address Copley's business practices. Under the SCA, smartphones are not "facilities through which an electronic communication is provided," and geolocation is not covered "content."[68] HIPAA, on the other hand, only governs the disclosure of information by certain healthcare providers, an umbrella listing that would not apply to Copley.[69] Furthermore, no

[62] Nathan Newman, *Search, Antitrust, and the Economics of the Control of User Data*. 31 YALE J. ON REG. 401, 435-437 (2014).
[63] Madelon Campbell, *supra* note 58, at 62.
[64] Jan Boyles, Aaron Smith, and Mary Madden, Privacy and Data Management on Mobile Devices, PEW RESEARCH CENTER, (Sept. 5, 2012), http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/ [https://perma.cc/7HY6-VNB9].
[65] *Id*. at 2.
[66] *See, e.g.*, Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 Alb. L.J. Sci. & Tech. 61, 115 (2011); Matthew Whitten, *Attacking Analogies: The Need for Independent Standards for Mobile Privacy*, 19 U.C.L.A. J.L. & Tech. 1, 2 (2015).
[67] 18 U.S.C. § 2701 *et seq.* (2017).
[68] In re iPhone Application Litigation, 844 F. Supp. 2d 1040 (N.D. Cal. 2012).
[69] 45 C.F.R. § 160.102(a) (2013) (HIPAA applies to the following entities: a health plan, a health care clearinghouse, or a health care provider "who transmits any health information in connection with a transaction covered by this subchapter.").

current federal laws specifically regulate businesses' use of geolocation technology. Several laws have been proposed to alleviate privacy concerns, including the Commercial Privacy Bill of Rights Act of 2011,[70] the Application, Privacy, Protection and Security Act of 2013,[71] and Illinois' Geolocation Privacy Protection Act of 2017.[72] Each one of these proposals has failed to become law.

Two possible relevant avenues still provide protections for users' privacy: FTC actions under section 5 of the Federal Trade Commission Act, and the privacy tort of intrusion. What follows is an evaluation of the applicability of each avenue, including the relative strengths and weaknesses of each potential remedy.

A. Section 5 of the Federal Trade Commission Act

Copley's practices were arguably "unfair and deceptive," in violation of the Massachusetts Consumer Protection Act (MCPA).[73] This act was intended to be "guided by the interpretations given by the Federal Trade Commission and the Federal Courts to section 5(a)(1) of the Federal Trade Commission Act…"[74] Section 5 of the Federal Trade Commission Act (FTCA) uses similar language; it empowers the FTC to regulate a company's "unfair or deceptive acts or practices."[75] Enforcement actions under section 5 provide guidance regarding the legality of Copley's practices.[76] These actions aim to protect consumers by ensuring that a business's practices are honest and transparent.[77] To this end, the FTC has repeatedly focused on promoting practices which protect users' personally

[70] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (proposed April 12, 2011), https://www.congress.gov/bill/112th-congress/senate-bill/799 [https://perma.cc/9GVW-U5MS].
[71] Application, Privacy, Protection and Security Act of 2013, H.R. 1913, 113th Cong. (proposed May 9, 2013) (providing privacy guidelines for personal data collection, use and storage by mobile phone application developers) https://www.congress.gov/bill/113th-congress/house-bill/1913 [https://perma.cc/3PXV-7ES4].
[72] Illinois Geolocation Privacy Protection Act, H.B. 3449, 100th Gen. Assembly (proposed Feb. 10, 2017), http://www.ilga.gov/legislation/BillStatus.asp?DocNum=3449&GAID=14&DocTypeID=HB&SessionID=91&GA=100 [https://perma.cc/46ME-2SV7].
[73] M.G.L.A. 93A §2(a) (2017).
[74] M.G.L.A. 93A §2(b) (2017).
[75] 15 U.S.C. §45 (2006); 15 U.S.C. § 52 (1994)
[76] The MCPA directs courts to look to the FTC and federal courts for guidance. M.G.L.A. 93A §2(b) (2017).
[77] *See, e.g.*, Electronic Privacy Information Center, *In re: Snapchat*, EPIC.ORG (discussing a consent decree in which Snapchat admitted to storing messages on its servers despite leading users to believe that these messages were being deleted) http://epic.org/privacy/internet/ftc/snapchat/#response (last visited July 27, 2018).

identifiable information (PII), including information that directly identifies an individual, such as driver's license information or social security numbers.[78]

According to the FTC, geolocation information qualifies as protectable PII.[79] Even though location information may not seem to be PII at first glance, it has the potential to be used in ways that violate a consumer's expectations of privacy. Geolocation data can be used in a whole host of nefarious ways. It could "help build profiles about consumers without their knowledge or consent, or it could be accessed by cybercriminals, hackers or through surreptitious means such as 'stalking apps.'"[80] Recognizing the dangers posed by these technologies, the FTC has used its section 5 enforcement authority in other relevant actions. For example, the FTC targeted an Android app provider that collected and transmitted users' geolocation data to third-party advertisers without first obtaining the users' consent[81] and a software development kit provider that accessed and improperly used users' geolocation information to deliver advertisements.[82]

Under section 5, the FTC has typically required businesses that collect and use PII to give users sufficient notice of their data collection and usage activities, obtain users' informed consent, and properly safeguard the privacy of collected information.[83] The FTC's notice requirements tend to be specific because absent adequate notice, a consumer cannot make informed decisions about whether to disclose certain information. In one case, for example, the FTC ordered an Android app provider to "prominently display[ ]" notice of the following on users' phones:

> (1) That such application collects, transmits, or allows the

[78] FEDERAL TRADE COMMISSION, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, 20 n. 47 (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [https://perma.cc/Q7V4-Q34S].

[79] FEDERAL TRADE COMMISSION, FTC STAFF REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf .

[80] Schechner, *supra* note 8, at 188.

[81] Complaint at 2, Goldenshores Technologies (FTC 2013) (No. C-4446), https://www.ftc.gov/sites/default/files/documents/cases/131205goldenshorescmpt.pdf (noting that users were informed that their data would be collected for updates and support, but not told that the data would be transmitted to third parties).

[82] Complaint at 3-6, United States v. InMobi Pte Ltd., (N.D. Cal. 2016) (No. 3:16-cv-3474).

[83] *See generally* Tomain, *supra* note 47, at 27-31 (discussing the FTC's preference for opt-in policies). The Federal Communications Commission also issued a report discussing the importance of notice and transparency for companies using beacon technology. FEDERAL COMMC'NS COMM'N – WIRELESS TELECOMMS. BUREAU, LOCATION-BASED SERVICES: AN OVERVIEW OF OPPORTUNITIES AND OTHER CONSIDERATIONS, at 19 (May 2012), https://apps.fcc.gov/edocs_public/attachmatch/ DOC-314283A1.pdf.

> transmission of geolocation information; (2) How geolocation information may be used; (3) Why such application is accessing geolocation information; and (4) The identity or specific categories of third parties that receive geolocation information directly or indirectly from such application."[84]

This notice adequately informs users about what type of data will be collected and how that data will be used and distributed. Requiring strong notice provisions helps cure the informational imbalance presented by the collection of information.

Some companies have pushed back against stringent notice requirements, but transparency arguably benefits even them. Straightforward practices help eliminate "friction" in users' decision-making because consumers are more likely to divulge personal information when they are assured that their data will be safeguarded.[85] These practices not only safeguard users from informational imbalance; they promote an ethically sustainable way of reducing friction, which is key to the business practices outlined above. Thus, strong privacy protection practices can even be good for business.

Some questions will inevitably arise with respect to privacy policies: At what point should notice be given? Should notice be opt-out or opt-in? And if notice is opt-in, would this yield any unique legal concerns? According to the FTC, companies should ideally provide users with notice just before collecting their geolocation data.[86] This notice should also be opt-in; while opt-out policies may be preferred by companies, they tend to be ineffective in practice.[87] Users frequently fail to exercise their rights and "opt-out" for a variety of reasons: they are given insufficient information about the policies; the policies are vague and broad; and/or the opt-out may be too limited and/or functionally inaccessible.[88] And while opt-in policies may arguably compel corporate speech, they satisfy First Amendment principles if they are "reasonably related to the State's interest in preventing deception of consumers."[89]

---

[84] Decision and Order at 4, Goldenshores Technologies (FTC 2014) (No. C-4446), https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf.
[85] Schechner, *supra* note 8, at 181.
[86] FEDERAL TRADE COMMISSION, FTC STAFF REPORT: MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY, at 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.
[87] *See, e.g.*, Decision and Order at 2, Nomi Techs., Inc., (FTC 2015) (No. C-4538) (finding online opt-out policy was insufficient in part because it was unlikely that customers could easily access policy).
[88] Tomain, *supra* note 47, at 24-25.
[89] *Id*. at 52; Zauderer v. Office of Disciplinary Counsel, 475 U.S. 626, 651 (1985).

In any event, FTC enforcement actions are useful because they provide administrative oversight of business practices. These actions ultimately help protect users because businesses will theoretically be compelled to incorporate stronger privacy protections into their policies. However, enforcement actions are inadequate because they do not help users realize immediate, individualized relief for the damages they have suffered due to a business's unfair or deceptive practices.

B. The Privacy Tort of Intrusion Upon Seclusion

When users are damaged by a business's intrusive practices, they can pursue relief through four different privacy torts: intrusion upon seclusion ("intrusion"), public disclosure of private facts, false light, and appropriation.[90] Of these, intrusion is most directly applicable to the present issue because it involves how private information is obtained and used. The privacy tort of intrusion is defined 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 the invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[91]

The central issue here is whether using geolocation information to deliver targeted messages constitutes actionable intrusion. The answer, as evidenced in the "intrusion" definition above, requires the resolution of two questions: (1) does the individual have a reasonable expectation of privacy, and (2) was the intrusion "highly offensive to a reasonable person"?[92]

The first question requires finding that the individual had an objectively reasonable expectation of privacy in his geolocation data. As noted above in the discussion of FTC actions, there is reasonable ground to treat geolocation data as private given the sensitive nature of the information that can be extrapolated from it. The pertinent case law, however, is unsettled.

In *In re Vizio, Inc., Consumer Privacy Litigation*,[93] for example, the Central District of California held that the plaintiffs' privacy claims were sufficient to survive a motion to dismiss.[94] In that case, the plaintiffs successfully argued that Vizio improperly disclosed information about their "digital identities."[95] The information included the individuals' MAC addresses, which uniquely identifies

[90] William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).
[91] RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).
[92] *Id*. at cmt. a.
[93] In re Vizio, Inc., 238 F. Supp. 3d 1204 (C.D. Cal. 2017).
[94] *Id*. at 1211.
[95] *Id*. at 1225.

users' electronic devices and "can be used to acquire highly specific geolocation data."[96] However, the court was also motivated by the plaintiffs' assertion that MAC addresses could "allegedly identify a person when combined with Vizio's disclosure of consumers' IP addresses, zip codes, product model numbers, hardware and software versions, chipset IDs, and region and language settings."[97] It is, therefore, difficult to judge how much the court's analysis hinged on the privacy concerns of geolocation data.

Other case law in California (mostly unpublished decisions in the Northern District of California) provides ammunition to argue that geolocation data should not be deemed private. In *In re Google, Inc. Privacy Policy Litigation*,[98] the court considered the privacy implications where Google aggregated user data among its products and divulged this information to third parties.[99] In *dicta*, the court said, "Courts in this district have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms."[100] Similarly, the court declined to find an actionable privacy invasion under the California Constitution where users' browsing histories were disclosed without authorization to third-party advertisers.[101] The disclosure, which included users' LinkedIn IDs and URLs they visited, did not constitute a "highly offensive disclosure of information" as required by California law.[102]

While the privacy status of geolocation data is, at best, open to question, language in one unpublished California decision provides some guidance for what behaviors could be construed as actionable. In *Yunker v. Pandora Media, Inc.*,[103] the court said that more egregious electronic tracking could support an invasion of privacy claim.[104] The court referred to *Goodman v. HTC* in support of its decision.[105] In that case, HTC allegedly installed codes on users' phones that could "track their movements, including where they live, work, dine and shop."[106] This information

[96] *Id*.
[97] *Id*.
[98] In re Google, Inc. Privacy Policy Litig., 58 F. Supp. 3d 968 (N.D. Cal. 2014).
[99] *Id*. at 974.
[100] *Id*. at 985.
[101] Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012).
[102] *Id*.
[103] Yunker v. Pandora Media, Inc., No. 11-CV-02113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013).
[104] *Id*. at *14-15.
[105] *Id*.
[106] Goodman v. HTC Am., Inc., No. C11-1793MJP, 2012 WL 2412070, *1 (W.D. Wash. June 26, 2012).

was compiled into a dossier and sold without authorization.[107] This suggests that behavior, if egregious enough, could violate privacy expectations.

Unfortunately, the most factually similar case provides scant guidance for the Copley issue because it was resolved on technical standing grounds. *In re iPhone Application Litigation*[108] involved claims that Apple wrongly exchanged geolocation information with its servers even when users turned off location services on their iPhones.[109] The plaintiffs sued under two California statutes: the Consumer Legal Remedies Act (CLRA) and the Unfair Competition Law (UCL).[110] To prevail on these claims, the plaintiffs were required to demonstrate that they detrimentally relied on Apple's misrepresentation(s), but they failed to show any actual reliance.[111] Although the plaintiffs clicked to consent to Apple's privacy policies, this action alone could not satisfy the reliance element. To prove reliance, the plaintiffs would have to show some affirmative action, such as actually reading the relevant policy.[112] The "click" alone was insufficient; because there was no reliance, the plaintiffs' claims failed.

Because scant law exists, and what exists is contradictory, it is unfortunately unclear whether geolocation data would be deemed private. The second question—whether using geolocation data to deliver targeted messages would be "highly offensive to a reasonable person"—is even trickier to predict. In *Opperman v. Path, Inc.*,[113] the court said that whether an invasion was "highly offensive" would depend on such things as "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[114] The offensiveness inquiry hinges on the facts of each case.[115] Attempting to apply this nebulous standard to Copley's situation is difficult. What makes Copley's case more persuasive, however, is that even if a court determined that the use of geolocation technology itself presents no actionable intrusion, Copley traded on users' sensitive medical information. The unique privacy concerns attached to the unauthorized use of that information may very well be deemed "highly offensive," and therefore actionable.

---

[107] *Id*.
[108] In re iPhone Application Litigation, 6 F. Supp. 2d 1004 (N.D. Cal. 2013).
[109] *Id*. at 1008-1009.
[110] *Id*. at 1007.
[111] *Id*. at 1012.
[112] *Id*. at 1025.
[113] Opperman v. Path, Inc., 205 F. Supp. 3d 1064 (N.D. Cal. 2016).
[114] *Id*. at 1077.
[115] *Id*. at 1078.

There is, indeed, something off-putting about the idea of Copley using geofencing technology to obtain users' sensitive information and target their smartphones with judgmental messages. These messages were intended for a vulnerable population—women seeking medical guidance regarding the termination of pregnancy—at their most vulnerable time: when they were in close proximity to their medical providers. Such behavior arguably violates "community norms of privacy," which would strongly suggest that the actions are "highly offensive."[116] This question ultimately cannot be resolved, however, unless it is determined that the transmission of user data effectuated something more than *de minimis* injury.

The problem with relying on the privacy tort of intrusion is that relief is inconsistent and case law is contradictory. It is unclear how any particular court would evaluate the intrusiveness of business practices like Copley's. This makes it difficult to determine what reasonable privacy expectations should look like and how the law should operate to protect them.

III. PROTECTING USERS' PRIVACY THROUGH A NEW FEDERAL STATUTE

As discussed above, both FTC actions and the intrusion tort are insufficient to safeguard users' privacy expectations fully. Ideally, a federal privacy statute that clearly delineated the practices for collecting, using and transmitting geolocation information would also protect users. With respect to the concerns of mobile privacy issues, one scholar argued, "A strong legislative response is necessary to help combat the threats to privacy that exist, and legislation at the national level would be the most effective means of enacting such reform."[117]

A. Proposed Laws and Industry Guidelines

A proposed Illinois law, the Geolocation Privacy Protection Act (GLPA),[118] actually created clear guidelines for geolocation data that could be adapted for a federal statute. The GLPA said that businesses could not:

> collect, use, store, or disclose geolocation information from a location-based application on a person's device unless the private

[116] *Id*. at 1079.
[117] Whitten, *supra* note 66, at 24.
[118] H.B. 3449, 100th Gen. Assemb., Reg. Sess. (Ill., 2017), http://www.ilga.gov/legislation/BillStatus.asp?DocNum=3449&GAID=14&DocTypeID=HB&SessionID=91&GA=100.

> entity first receives the person's affirmative express consent after complying with the specified notice requirements.[119]

The GLPA also would have provided impacted users the greater of liquidated or actual damages, as well as attorney's costs and injunctive relief.[120] This bill, however, was vetoed by Illinois Governor Bruce Rauner, who said it "would result in job loss across the state without materially improving privacy protections for Illinoisans or making devices and their apps safer for children."[121] Privacy advocates and trade associations decried the veto, noting that the bill actually reflected existing FTC guidelines.

Despite Rauner's veto, the Illinois law nevertheless provides a reasonable starting point to craft a federal statute. In addition, guidance for constructing a statute can be derived from the best practices adopted by various trade associations, including CTIA, a trade association representing the wireless communications industry, and the Digital Advertising Alliance (DAA), which establishes privacy practices for digital advertising.

The CTIA established guidelines to "promote and protect user privacy as new and exciting Location-Based Services ("LBS") are developed and deployed."[122] They also suggest protecting users' information through seven other safeguards, including compliance with "applicable laws" and retention limitations.[123] Similarly, the DAA established privacy guidelines that "apply to certain types of data in the Mobile web site and application development."[124] These policies are particularly relevant because they acknowledge the more modern privacy concerns of the mobile environment. The DAA's policies, similar to those put forth by the CTIA, also focus on notice and consent, though it includes stronger guidance for data transmitted to third parties. It also has specific guidelines for safeguarding sensitive information, including health data.

B. What Elements Should a Federal Statute Include?

[119] *Id*. at para 1.
[120] *Id*.
[121] Robert Channick, *Rauner Vetoes Geolocation Privacy Bill Aimed at Protecting Smartphone Users*, CHICAGO TRIBUNE (Sept. 22, 2017), http://www.chicagotribune.com/business/ct-biz-geolocation-privacy-rauner-veto-20170922-story.html.
[122] CTIA, BEST PRACTICES AND GUIDELINES FOR LOCATION BASED SERVICES (2010), https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services.
[123] *Id*.
[124] Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment,* 1 (July 2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf.

This section of the article draws upon the GLPA, as well as CTIA and DAA guidelines, to highlight key elements that should be incorporated into a federal geolocation privacy statute. The bulk of this information can be broken down into six broad elements that must be included in order to adequately protect users' privacy. These provisions help maximize the potential for users to be fully informed before consenting to a business's data practices. They are also simple so businesses can easily adhere to them. Ideally, businesses will also realize increased user confidence due to the transparency of their privacy practices.

1. Businesses must provide adequate notice to consumers regarding how their data is collected, used, and transmitted to third parties.

The utility of a geolocation privacy statute turns on adequate consumer notice. Primarily, the privacy statute must direct businesses to provide ample notice to users about how their information will be obtained, used, and shared. The purpose of notice is to provide users with sufficient information to make informed decisions about whether to consent to a business's data practices. Requiring sufficient notice will serve to correct the informational imbalance and enable users to control whether and how their information can be manipulated.

The notice must indicate exactly what information will be collected, whether that data includes any PII, how the data will be used, with whom the information will be shared, how the information will be stored, and for how long the information will be retained.

2. Businesses must give adequate notice to consumers regarding how third parties will use their data.

Business policies regarding the transmission of data to third parties must be specifically outlined for the user. Here, the informational imbalance is most pronounced. The user has entered into an agreement with a business; however, this user's data is now being transmitted to third parties with whom the user never communicated directly. Therefore, users must be notified of (1) the identities of the third parties collecting and using their information, and (2) how these third parties are using that information.

Including information about third-party data use in a generalized notice policy is insufficient to give users the opportunity to meaningfully consent to the use of their data. This information should be conveyed in a way that is meaningful to consumers.

Another element important here is that businesses should be required to obtain individualized consent for each third party to whom data will be transmitted. Obtaining blanket consent is insufficient here.

3. Businesses must give adequate notice to consumers regarding data retention policies.

Businesses must inform users of how their data is being stored and safeguarded. Data should only be retained as long as necessary, depending on business needs. If a business intends to store information for any significant length of time, it must anonymize the data to the extent practicable. When the information is no longer central to the business's needs, it must be destroyed.

4. Businesses must provide periodic updates reiterating their data policies and convey information about any policy changes to consumers promptly.

Businesses should periodically provide users updates reiterating their data policies. If a business alters its data practices, it must convey these changes to the user promptly.

These requirements together enable the user to evaluate the business's practices and determine whether to provide consent. The provisions both correct informational imbalance and empower the user to determine whether and how his information is used.

5. Businesses must provide periodic updates reiterating their data policies.

Users should also be given periodic updates that reiterate the business's data policies. This enables users to reassess their consent and encourages mutually beneficial practices to be sustained.

6. All notice must be "clear, meaningful, and prominent."

The various guidelines set forth in the trade publications do not indicate a preference for format. CTIA simply says that "[p]roviders may use written, electronic or oral notice so long as users have an opportunity to be fully informed of … information practices."[125] Similarly, the DAA directs businesses to provide

[125] CTIA, *supra* note 122, at section 4.

notice in a form "where such notice is clear, meaningful, and prominent."[126] Again, although the notice formatting requirements are deliberately left up to a broad interpretation, it seems clear that the most "clear, meaningful, and prominent" form of notice when a business is using geolocation data would be delivered electronically to the user. This notice does not need to be a push notification—although that would maximize the clarity, meaningfulness and prominence of the notice—but it should at least be a prominent piece of the user agreement. Notice, however, cannot be buried in the terms of service agreement. As part of the agreement, users should be given a separate prompt covering data use and transmission.

CONCLUSION

Copley's messages were, on their face, protected political speech under the First Amendment. However, reasonable content-neutral restrictions can still apply to regulate Copley's speech, even considering Supreme Court case law protecting speech near abortion clinics. Healey's actions, as evidenced in the Assurance of Discontinuance,[127] focused on neutral concerns, specifically Copley's unauthorized use of geolocation data to customize messages to reach a particular group of consumers: vulnerable "abortion-minded" women near medical providers.

Existing mechanisms that arguably target Copley's behavior are FTC section 5 enforcement actions and the common-law privacy tort of intrusion. The former is robust, but aggrieved users will not realize immediate, individualized relief, and it is unclear whether the unauthorized collection and/or transmission of geolocation data alone can support a cause of action under the latter.

This study ultimately suggests that users' privacy expectations would be best protected by delineating clear business practices regarding the collection, use, and transmission of geolocation information. The policy should include: strong, clear notice provisions with periodic updates provided to users; statements regarding the transmission of data to, and use by, third parties; revocable opt-in consent for the use of individuals' information; provision regarding changes to data use; a statement about the collection, use or distribution of sensitive (non-geolocation) data, including medical information; and a strong data retention and destruction policy.

[126] Digital Advertising Alliance, *supra* note 124, at 13.
[127] Assurance of Discontinuance, *supra* note 2, at 3.