University of Chicago Legal Forum

Volume 2018 Article 11

2019

Borrowing from the Old [Common Law] To Litigate the New [Beacon Surveillance Claims]

Courtney Albini

Borrowing from the Old [Common Law] To Litigate the New [Beacon Surveillance Claims]

Courtney Albini†

I. INTRODUCTION

Although new technologies are propelling modern society into an era of extraordinary connectivity, such advances simultaneously leave unaware citizens vulnerable to unprecedented personal invasions of privacy. Moreover, the speed at which technology advances within the areas of e-commerce, smartphones, social media, the cloud, and the internet of things, outpaces lawmakers' abilities to craft new regulations and electronic privacy laws. Consequently, beholden legal concepts, such as an individual's reasonable expectation of privacy, a defendant's engagement in highly offensive conduct, the voluntary disclosure of information to third parties, and unlawful intrusions into one's solitude, must be reevaluated as modern plaintiffs grow increasingly motivated to have their privacy concerns recognized by lawmakers. Unfortunately for plaintiffs, the legal infrastructure in America, unlike other nations, lacks a comprehensive data privacy statute that encompasses all sets of privacy concerns.[1] Instead, the American data privacy law landscape is "a mosaic of sector-specific laws,"[2] each of which "provides protection for certain specific types of information" and "un-

† A.B. 2013, University of Pennsylvania; M.Phil 2014, University of Cambridge; J.D. Candidate 2019, The University of Chicago Law School. I owe gratitude for the insight of Professors Laura Weinrib and Lior Strahilevitz, whose suggestions and edits helped me translate mere ideas into written form. Equally, I am thankful for the thoughtful recommendations of current and past *The University of Chicago Legal Forum* staff and board members that helped refined various versions of the Comment. And finally, I thank my parents, Rachelle and Ed Albini, for always encouraging me to follow my passions.

[1] James B. Rule, *When it comes to protecting its citizens' data, Europe is way ahead of the U.S.*, L.A. TIMES (May 12, 2014), *http://www.latimes.com/opinion/op-ed/la-oe-rule-nsa-privacy-european-union-20140513-story.html* [https://perma.cc/M7XF-BJ4H].

[2] Some prominent examples of "sector specific" privacy laws include: the Computer Fraud and Abuse Act, the Stored Communications Act (Title II of the ECPA), the Federal Wiretap Act (Title I of the ECPA), the CAN-SPAM Act, the Telephone Consumer Protection Act (TCPA), the Children's Online Privacy Protection Act, and the Video Privacy Protection Act.

derpins private rights of action for improper access to, or use of, that information" in a limited technical area.[3] When faced with this quandary, a critical inquiry to raise is: should lawmakers work more rapidly to craft legislation that addresses privacy concerns related to every new and niche technical platform? Or, because the rapid pace of technology growth would require constant amendments to the law, would it be more fruitful for technology users to bring their novel electronic privacy claims under battle-tested common law theories of privacy, specifically, the theory of "an unreasonable intrusion upon the seclusion of another"?[4]

I argue the latter situation, with the aim of showing why state common law privacy theories are better suited to protect plaintiffs' privacy rights related to unprecedented intrusions to privacy perpetrated by emerging technologies such as *audio beacon ultrasonic cross-device tracking* ("beacon technology"). Equally, I analyze common threads uniting beacon technology fact patterns in order to advance ideas of how plaintiffs' privacy rights can be more predictably protected under the law. Disadvantages of advancing privacy claims under seemingly obvious statutes like the Wiretap Act[5] will be noted in the presentation of early beacon-related litigation. I then highlight the advantages of advancing these same claims under an intrusion upon seclusion common law theory based on the success of related electronic privacy litigation. Although such cases will not specifically involve beacon technology, this Comment will argue that the electronic privacy and surveillance issues are factually similar enough, as to warrant an extension of the judicial framework.

Furthermore, I will pay heightened attention to California's electronic privacy legal environment, given the likelihood that the majority of future beacon technology suits will be brought in the District Court for the Northern District of California, per rules of jurisdiction.[6] Within the context of California, I will focus on judicial opinions related to GPS mobile phone tracking, data content mining, and video surveillance. In addition, I will discuss how the strong privacy protections enshrined in California's state Constitution, in addition to California's statutory code, lend a powerful backdrop to judges' future analysis of

---

[3] ROBERT D. BROWNSTONE & TYLER G. NEWBY, DATA SECURITY AND PRIVACY LAW § 9:2 (2017).

[4] *Id.* § 9:123.

[5] 18 U.S. Code § 2511 (2012).

[6] The Northern District of California has featured a sizable number of cases relating to technology privacy questions. This rate is likely a function of the physical locations of many app developers in Silicon Valley, California, which is included in the Northern District of California. Consequently, a plaintiff bringing suit can most easily obtain personal jurisdiction over the defendants in this district.

common law electronic privacy claims. Lastly, I will provide some analysis of influential Supreme Court decisions, including *Riley v. California*[7] and *United States v. Jones*,[8] and how such decisions could have a significant impact on judges' future decision-making regarding the privacy of mobile phone content and the limits of surveillance.

II. ANOTHER TRACKING FEATURE INVADING AMERICANS' MOBILE PHONES

A. Understanding Beacon Technology

If any mobile device user has ever experienced the unsettling occurrence of speaking to a friend about an obscure subject, and then subsequently being greeted by an advertisement targeting that niche topic the next time she turns on her phone, then the user has been exposed to an early application of beacon technology.[9] About four years ago, companies like Samsung and LG admitted to the practice of capturing portions of phone users' private communications and then sending them to third-party speech and imaging recognition companies for the ultimate purpose of creating user-specific advertising.[10] Ever since these admissions, the capabilities of the underlying technology have evolved rapidly into the more comprehensive and sophisticated beacon technology, which has improved companies' abilities to track consumer preferences. Now, when mobile applications are downloaded onto users' smart devices, underlying beacon tracking microphones are activated and programmed to listen to inaudible messages broadcast via "audio beacons including."[11] These audio beacons can be activated independently on a daily basis, including while the user is watching movies, television and commercials; listening to music; shopping in stores; or attending sports games and concerts. Once the beacon signals have been "collected," third-party companies like the 2015 startups SilverPush, Shopkick and Signal360, can build detailed logs of the physical activities, retail purchases, and entertainment preferences of the user.[12]

---

[7] 134 S. Ct. 2473 (2014).

[8] 565 U.S. 400 (2012).

[9] *How Audio Beacons Monitor You via Smartphone*, NANALYZE (May 29, 2017), https://www.nanalyze.com/2017/05/audio-beacons-monitor-smartphone/ [https://perma.cc/BE58-W7VZ].

[10] *Id.* For example, Samsung admitted to capturing and sending private conversations to Nuance Communications, an American multinational computer software technology corporation headquartered in Burlington, Massachusetts.

[11] *Id.*

[12] Lily Hay Newman, *How to Block the Ultrasonic Signals You Didn't Know Were Tracking You*, WIRED (Nov. 3, 2016), https://www.wired.com/2016/11/block-ultrasonic-signals-didnt-know-tracking/ [https://perma.cc/A679-N3TE].

Despite its sophistication, beacon technology functions in a straightforward manner: (1) a user downloads a smartphone application from a mobile application store (e.g. Apple's App Store or Google Play); (2) upon download, the application requests permission to access the user's smartphone microphone; and, (3) if the user agrees, then the microphone can and will often remain activated whenever the phone is turned on. Importantly, while activated, the microphone has the capacity to listen for inaudible beacon frequencies that are emitted from retail stores, advertisements, and websites. Furthermore, because beacon technology combines "the best of two worlds"—namely audio tracking capabilities and GPS locating function—an increasing number of smartphone mobile application developers have incorporated it into their products. In turn, retail corporations, sports teams, and marketing firms pay for the developers to create an application promoting their organization, and work with the developers in the full-time operation of the application.[13]

Not surprisingly app developers[14] and their diverse range of clients[15] laud the "win-win" benefits of this technology for themselves and their users: while the app provides consumers a multidimensional, interactive experience based on consumers' specific personalities, the organizations are concomitantly able to track consumers' preferences. In so doing, the corporation can then "nudge" users into making a financial investment into a team, product, or service through the expertly targeted funneling of coupons, promotions, and advertisements directly to users' phones.[16] However, as more applica-

---

[13] *Id.*

[14] The largest app developers that utilize Beacon technology include: iMOBDEV Technologies, Clearbridge Mobile, Multidots Solutions, K2B Solutions, and Guarana Technologies. *See Top Beacon App Development Companies*, RECOVENDOR https://recovendor.com/beacon-app-development-companies/ [https://perma.cc/G4D3-AW57]; *See also* Neha Mallik, *5 Best iBeacon Apps That Are Leading the Pack*, BEACONSTAC (Feb. 19, 2015), https://blog.beaconstac.com/2015/02/5-best-ibeacon-apps-that-are-leading-the-pack/ [https://perma.cc/52D7-8WPL].

[15] The range of corporations that contract with Beacon technology app developers include: the Golden State Warriors basketball team, the Indianapolis Colts football team, Rite Aid, Target, Macy's, American Eagle Outfitters, Oscar Mayer, McDonald's, Lord & Taylor, Walgreens, Neiman Marcus, Walmart, Tesco, Nordstrom, and MLB.com.; Shubhi Mittal, *25 Retailers Nailing It with Their Proximity Marketing Campaigns*, BEACONSTAC (Feb. 11, 2016), https://blog.beaconstac.com/2016/02/25-retailers-nailing-it-with-their-proximity-marketing-campaigns/ [https://perma.cc/VP88-RUQZ]; *Qualcomm to Provide iBeacon Hardware to Work with the 'MLB.com At the Ballpark" App*, QUALCOMM (Mar. 6, 2014), *https://www.qualcomm.com/news/releases/2014/03/06/qualcomm-provide-ibeacon-hardware-work-mlbcom-ballpark-app* [https://perma.cc/VES8-7PVA]; *See* Michael J. Stortz et al., *Plaintiffs Face Challenges in Cellular Phone Application Privacy Litigation*, DRINKERBIDDLE PUBL'NS, (Feb. 16, 2017), https://www.drinkerbiddle.com/insights/publications/2017/02/plaintiffs-face-challenges-in-cellular-phone (last visited Apr. 30, 2018).

[16] Lily Hay Newman, *Hundreds of Apps Can Listen to Marketing 'Beacons' You Can't Hear,* WIRED (May 2, 2017), https://www.wired.com/2017/05/hundreds-apps-can-listen-beacons-cant-hear/ [https://perma.cc/B9N7-944E].

tions are deploying beacon with or without a specific retail or promotional purpose, users are less cognizant of its presence within applications. Thus, they are not aware that when they are granting access to the microphone upon download it will remain activated during significant periods when the users' phones are on, even if the phones are disconnected from the internet.[17] Ultimately, these enormous periods of activation contribute to the building of a biographical snapshot of the user, of which she has not explicitly consented.[18]

B. The Current Legal Landscape of Beacon Technology

1. Legal problems presented by "hybrid" tracking features

Inevitably, the newness of beacon technology, coupled with the unprecedented security issues posed by the all-access audio and physical location tracking features, have led to rancorous clashes in district courts. Angered by the "surreptitious" surveillance perpetrated by their phones, plaintiffs have generally advanced their grievances under various titles of the Electronic Communications Privacy Act (ECPA),[19] particularly Sections 2511(1)(a) and 2511(1)(d) of Title I, otherwise known as the Wiretap Act.[20]

Under the Wiretap Act, in particular, plaintiffs have experienced mixed success. This is especially true in the District Court for the Northern District of California, the jurisdiction where many of the app developers are based.[21] An analysis of these related judicial opinions shows that the Wiretap Act is an unpredictable legal vehicle for these types of claims for two reasons: (1) because under § 2511(1)(a), a prima facie "interception" claim requires plaintiffs to show the "acquisition" of a deliberately spoken "oral communication;" and, (2) because under § 2511 (1)(d), an unlawful "use" claim requires plaintiffs to allege facts to show defendants' targeted advertisements were based distinctly on the content of the allegedly "intercepted" communications made by users' during the microphones' activation.[22]

---

[17] *Id.*

[18] *Id.*

[19] Pub. L. No. 99–508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[20] Stortz et al., *supra* note 15; Michael J. Stortz et al., *Plaintiffs Face Challenges in Cellular Phone Application Privacy Litigation*, 3 PRATT'S PRIVACY & CYBERSECURITY REPORT 159, 159–62, (June 2017) (last visited Apr. 30, 2018) [hereinafter Stortz et. al, *Plaintiffs*, PRATT'S]

[21] Stortz et al., *supra* note 15.

[22] *Id.*

2. Beacon technology litigation under the Wiretap Act

Alarmed by the extraordinary amount of personal data collected by beacon technology smartphone apps, plaintiffs immediately turned to the Wiretap Act as a tool of privacy protection.[23]

a. In re iPhone Application Litigation

One of the first cases to touch upon issues relating to the collection of mobile data through third party applications, *In re iPhone Application Litigation* ("*iPhone*")[24] featured consumer Plaintiffs asserting claims under the Stored Communications Act,[25] the Wiretap Act,[26] and other federal and state laws.[27] Specifically, Plaintiffs brought suit against Apple, Inc., Admob, Inc., Flurry, Inc., AdMarval, Inc., Google, Inc., and Medialets, Inc. (aside from Apple, referred to as "Mobile Industry Defendants"), for allegedly violating federal and state privacy laws, by providing a space for third-party application makers to gain unauthorized access to users' personal information over devices like the iPhone, iPad, and iPod Touch.[28] Such information included Plaintiffs' locations, the iPhones' unique device identifiers (i.e. the device serial code numbers), and users' ages or genders.[29] Additionally, Plaintiffs claimed that in violation of the Wiretap Act, Apple utilized the GPS data cell phone towers and Wi-Fi networks to "develop an expansive database of information about the geographic location of cellular towers and wireless networks through the United States."[30]

The District Court for the Northern District of California dismissed the claims arising under the Stored Communications Act, the California Constitutional right to privacy, the Computer Fraud and Abuse Act, as well as the trespass, conversion and unjust enrichment

---

[23] BROWNSTONE & NEWBY, *supra* note 3, § 9:154 ("mobile apps' gathering of information on device users—as well as other "tracking" methods—have come to the forefront in civil lawsuits and government enforcement proceedings. . . . In a number of the civil enforcement actions, multiple theories are interposed as bases for claims for relief, including alleged violations of the Electronic Communications Privacy Act, state wiretap acts, the federal Computer Fraud and Abuse Act and its state law counterparts, state unfair competition laws and common law claims for invasion of privacy, conversion and trespass to chattels.").

[24] 844 F. Supp. 2d 1040 (N.D. Cal. 2012).

[25] 18 U.S.C. § 2701 (2012).

[26] 18 U.S.C. § 2511 (2012).

[27] *iPhone*, 844 F. Supp. 2d at 1040; *see also* Shelton Abramson & Mali Friedman, *Key Holdings in the In re iPhone Application Dismissal Order*, COVINGTON & BURLING LLP: INSIDE PRIVACY (June 18, 2012), https://www.insideprivacy.com/advertising-marketing/district-court-dismisses-stored-commuications-act-and-wiretap-act-claims-against-apple-for-iphone-da/ [https://perma.cc/RY4P-T392].

[28] iPhone, 844 F. Supp. 2d at 1048–49.

[29] *Id.* at 1050.

[30] *Id.* at 1048.

claims.[31] In dismissing the class claims against the Wiretap Act, the district court cited Ninth Circuit authority in contending that "'content' is limited to information the user intended to communicate, such as the words spoken in a phone call."[32] Because the alleged "content" that Apple collected was solely the mobile device users' geolocation data, which was generated automatically, such did not constitute "content" susceptible to interception under the Wiretap Act."[33]

Although the court's ruling was promising to tech defendants in Silicon Valley, plaintiffs' claims under the Wiretap Act would take a slightly more creative form four years later in *Satchell v. Sonic Notify, Inc.*,[34] and *Rackemann v. LISNR, Inc.*[35]

b. Satchell v. Sonic Notify, Inc.

Satchell, the first case to truly test the applicability of the Wiretap Act to smartphone apps with "tracking" features, resulted in a motion to dismiss in February 2017.[36] Like the Plaintiffs in *iPhone*[37] the *Satchell* plaintiff, a Golden State Warriors fan, alleged that the team's mobile application—which utilized new technology to provide users up-to-date scores, statistics, schedules, and news about the team—had recorded her conversations without her knowledge or consent.[38] The corporations defended the use of the technology, arguing that it offers a valuable service to consumers in the form of "targeted and specific advertisements, promotions, [and] content," as informed by the consumer's precise GPS location.[39] However, Satchell offered a strong rebuttal, stating that the mobile application, in violation of the Wiretap Act, was programmed to "turn on a consumer's Microphone," which would then allow the App to "listen[] [t]o and pick[] up any and *all* audio within range. . . . until [the App] is closed—either when the consumer's smartphone is shut off or when the consumer 'hard closes' the App."[40] Moreover, although the app did request Satchell's permission for certain features, the Defendants had failed to inform consumers

[31] *Id.* at 1078.

[32] *Id.* at 1061.

[33] *Id.*

[34] 234 F. Supp. 3d 996 (N.D. Cal. 2017).

[35] No. 17-CV-624, 2017 WL 4340349 (S.D. Ind. Sept. 29, 2017).

[36] 234 F. Supp. 3d at 999.

[37] 844 F. Supp. at 1041.

[38] 234 F. Supp. *3d* at 1000.

[39] *Id.*

[40] *Id.*

that the "App uses audio beacon technology that surreptitiously turns on consumers' smartphone microphones and listens in."[41]

While the court found that the violation of Satchell's privacy rights was sufficient to show injury-in-fact, the court ultimately held that she had failed to allege facts demonstrating that the Warriors had intercepted her oral communications within the meaning of the Act.[42] Furthermore, with regards to both defendants, the court ruled that Satchell had failed to state a claim based on illegal "use" of her information under the Wiretap Act. She did not allege sufficient facts to demonstrate that the contents of her communication were utilized to craft the targeted advertising sent to her via the application.[43] Notably, however, the court found that Signal360, the technology provider of the app, did "intentionally intercept" her communications, given the deliberate design of the app's technology that enabled the collecting of such information.[44]

c. Rackemann v. LISNR, Inc.

Facing similar allegations as the Golden State Warriors in *Satchell*, in *Rackemann v. LISNR, Inc.*,[45] the Indianapolis Colts football franchise, and its mobile application developers (LISNR, Inc. and Adept Mobile, LLC) were sued for alleged violations of federal anti-wiretapping laws in the operation of the Colts' mobile application.[46] Filing as a putative class action in the Northern District of Illinois, the representative plaintiff, Alan Rackemann, alleged that Defendants had violated the Wiretap Act by "hijacking" application users' smartphones with the intent of transforming them into listening devices that possessed the capability to surreptitiously record application users' personal communications.[47] Specifically, under § 2511(1)(a) of the Wiretap Act, Rackemann claimed that the applications were programmed to intercept users' "private conversations, including oral communications," despite the "exhibited expectations" of himself and other class members that "such communication were to remain private and would not otherwise be subject to interception under circumstances justifying such expectation."[48] Under § 2511(d) of the Wiretap Act,

---

[41] *Id.*

[42] *Id.* at 1008 (N.D. Cal. 2017).

[43] *Id.* at 1008–09.

[44] *Id.* at 1006–08. Note, however, the court concluded that the plaintiff failed to allege sufficient facts to show that any of the defendants intercepted her communications.

[45] No. 17-CV-624, 2017 WL 4340349 (S.D. Ind. Sept. 29, 2017).

[46] *Id.* at *1.

[47] *Id.* at *1–2.

[48] *Id.* at *3.

Plaintiff also alleged that Defendants subsequently used these intercepted communications to their economic benefit in the form of direct marketing.[49]

The court dismissed the unlawful "use" claim given Plaintiff failed to demonstrate any plausible connection between the specific contents of the allegedly intercepted communications, and the advertising subsequently directed at him.[50] However, the "interception" claims were maintained.[51] In making the decision, the court deferred to Rackemann's allegations that during the four years the app was installed on his smartphone, it was *plausible* that the listening function had been activated during periods in which he engaged in private oral communications.[52] In reaching the decision, the court was sympathetic to Rackemann's inference of interception because the app was deliberately designed to receive instructions developed by the Colts and Adept Mobile, which designated a number of date and time intervals during which the "listening" microphone was to be activated by the Application.[53] The court rejected Defendants' contention that "interception" under the Wiretap Act means that a defendant must have come "into possession of" the oral communications of the app users[54] instead adopting the more plaintiff-friendly definition of "interception" advanced by the Ninth Circuit, which requires simply that the "contents of a . . . communication are captured or redirected in any way." [55] The court agreed that the Plaintiff's communications had been intercepted because the app had built activity logs based on aggregated beacon signals and recorded portions of audio collected from Plaintiff's cellphone activities (when the microphone was activated).[56] Lastly, although Defendants referred the court to a technical description on the LISNR website, which explicitly states that the embedded microphones *only* record beacon tones, and do not record any other audible

---

[49] *Id.*

[50] *Id.* at *8–9. Based on the court's dicta and dismissal without prejudice, it would seem that if Plaintiff could manage to trace the content of his advertising directly to the content of his conversations, he would have a better case. However, this seems to be an incredibly difficult hurdle to overcome, as it would require Plaintiff to essentially eliminate any influence of the Beacon symbols and his corresponding physical locations (that matched with the Beacon signals), on the content of the advertisements.

[51] *Id.* at *9.

[52] *Id.* at *5–6. It is important to note that the court agreed with this premise even though *Rackemann* could not provide any specific dates and times in which his private conversations had been recorded.

[53] *Id.* at *5.

[54] *Id.* at *6.

[55] *Id.*

[56] *Id.*

sounds or communications,[57] the court was unwilling to entertain this written explanation at the motion to dismiss stage, as defendants had not incorporated such into their response.[58]

C. The Legal Framework of a Successful Intrusion upon Seclusion Opinion for Electronic Privacy Litigants in California

1. *Opperman v. Path, Inc.*

Notwithstanding Plaintiff's limited initial success in *Rackemann*,[59] beacon fact patterns of this nature seem relatively unlikely to even survive summary judgment under § 2511(1)(a) of the Wiretap Act, let alone result in a successful verdict for plaintiffs upon the conclusion of trial. However, an alternative route via a common law intrusion upon seclusion privacy claim seems viable, based on the legal analysis offered in a successful ruling for litigants in *Opperman v. Path, Inc.*,[60] an electronic privacy case filed in 2014 within the District Court of the Northern District of California.[61] Representing a long-running set of consolidated cases against Apple and other social and gaming mobile app developers, *Opperman* featured an attempted class of consumer plaintiffs asserting a number of common law and statutory claims against Defendants.[62] Specifically, the class alleged unlawful privacy intrusions into their personal contact information based on the app developers' intentional programming of the applications to access users' iPhone address books without their consent.[63] As

---

[57] *Id.* at *7.

[58] *Id.* Under the Wiretap Act, "contents" must include "any information concerning the substance, purport, or meaning of that [oral] communication." 18 U.S.C. § 2510(8) (2012). Invoking this definition, defendants attempted to undermine Plaintiff's claim that the App had actually acquired the "content" of his communications by explaining that the app's technological functions are limited to "temporarily record[ing]" portions of "audio" for limited periods of time. *Id.* at *6. Moreover, according to Defendants, no audible communications are actually recorded; rather, once all of the data from a user's phone is aggregated, it is stripped down for the purpose of only "analyz[ing] and monitor[ing]" the beacon tones. *Id.* at *7.

[59] Following the district court's partial granting of defendant's motion to dismiss in *Rackemann,* it does not appear that plaintiff pursued further action. No. 17-CV-624, 2017 WL 4340349 (S.D. Ind. Sept. 29, 2017).

[60] 87 F. Supp. 3d 1018 (N.D. Cal. 2014).

[61] *Id.*

[62] *Id.*

[63] *Id.* at 1029. As additional evidence of the troubles plaintiffs have faced in utilizing state and federal statutory privacy laws as a medium through which to advance beacon technology claims, it is relevant to note *Opperman v. Path, Inc.*, No. 12-CA-219, 2012 WL 4105189 (W.D. Tex. Aug. 23, 2012). In the earliest filing of this class action, the court dismissed plaintiffs' original and amended class action complaints alleging that apps from Path, Facebook, Twitter, Apple, Beluga, Yelp, Burbn, Instagram, Foursquare Labs, Gowalla, Foodspoting, Hipster, LinkedIn, Rovio Mobile, ZeptoLap, Chillingo, Electronic Arts and Kik Interactive secretly and unlawfully copy, upload, and store users' address book data without their knowledge or consent in violations of the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the Tex-

countered by Defendants, the purpose of this design feature was to assist users in locating other users whom they already knew within the app network.[64] Nonetheless, Plaintiffs asserted a number of common law claims for invasion of privacy, including intrusion upon seclusion, conversion, negligence, and trespass to chattels.[65] In addition, Plaintiffs asserted violations of state and federal wiretap laws.[66]

Like the court in *iPhone*, the *Opperman* court dismissed both the federal and state wiretap claims, given that Plaintiffs alleged access to stored data, as opposed to showing an *interception* of *oral communication.*[67] The court also dismissed the majority of Apple's defenses based on Plaintiffs' lack of Article III standing.[68] Notably, however, the Court did find for the common law intrusion upon seclusion claim.[69]

In fact, the court's lengthy intrusion upon seclusion reasoning is worth elaborating on, given such analysis sheds light upon the heightened protections California's case law affords to the privacy of citizens. This type of environment could prove particularly conducive for the legal battles waged by future mobile phone users' in their challenges against the use of mobile tracking technology.

2. Intrusion upon seclusion analysis

California's intrusion upon seclusion standard mirrors the Second Restatement of Torts requirement. Under the California standard, a plaintiff must show a defendant has "(1) intru[ded] into [plaintiff's] private place, conversation or matter, (2) in a manner highly offensive to a reasonable person"[70] before an actionable claim can be made. In the backdrop of this test, California courts emphasize the importance of "personal isolation and personal control," and the connection of such concepts to "personal freedom and dignity."[71] However, courts will only find an intrusion if the plaintiff demonstrates "an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source," which is evaluated based on several factors, including: a

---

as Wiretap Act, among others.

[64] *Id.* at 1029.

[65] *Id.* at 1030.

[66] *Id.* at 1029–30. In addition to violations of federal and state wiretap laws, Plaintiff asserted violations of the following: California's Unfair Competition Law, California's False and Misleading Advertising Law, the California Comprehensive Computer Data Access and Fraud Act, California and Texas Wiretap Acts, the federal Computer Fraud & Abuse Act, the federal Wiretap Act, and the Racketeer Influenced and Corrupt Organizations Act.

[67] *Id.* at 1063–64.

[68] *Id.* at 1036–39.

[69] *Id.* at 1058–61.

[70] *Id.* at 1058.

[71] *Id.*

plaintiff's advance notice of an impending action, industry customs, industry practices, and any private physical settings, which could "create or inhibit reasonable expectations of privacy."[72]

Similarly, when evaluating the reasonableness of the privacy expectation, courts contend that "the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant."[73] As per the "offensiveness" prong, California courts require that the "interference with the plaintiff's seclusion" be a "substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object."[74] In analyzing the factual circumstances related to such, courts look to: "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."[75]

Determining if a legally protected privacy interest is at stake is a question of law, while plaintiff's reasonable expectation of privacy and the offensiveness of defendant's conduct as a serious invasion of privacy are analyzed as mixed questions of law and fact.[76] In making the claim, plaintiffs need not allege any damages or economic injury from the intrusion upon seclusion, as the "intrusion" itself represents the injury.[77] Thus, if a plaintiff prevails on the claim, he may recover damages for "anxiety, embarrassment, humiliation, shame, depression, feelings of powerlessness, anguish, etc."[78]

Conforming to the state standard, the *Opperman* Plaintiffs alleged in their complaint that "[b]y surreptitiously obtaining, improperly gaining knowledge, reviewing and retaining Plaintiffs' private mobile address books (or substantial portions thereof), the App Defendants intentionally intruded on and into each respective Plaintiff's solitude, seclusion or private affairs."[79] Moreover, in asserting that this type of intrusion should be viewed as "highly offensive to a reasonable person," Plaintiffs referenced the significant amount of public and governmental criticism of this practice, which has been captured in "myriad newspaper articles, blogs, op eds., and investiga-

---

[72] *Id.* at 1059.

[73] *Id.*

[74] *Id.* at 1060.

[75] *Id.* (citing Miller v. Nat'l Broad. Co., 187 Cal. App. 3d 1463, 1483–84 (1986)).

[76] *Id.* at 1059.

[77] *Id.* at 1061.

[78] *Id.* at 1061 (citing Operating Eng'rs Local 3 v. Johnson, 110 Cal. App. 4th 180, 187 (2003) (quoting Miller v. Nat'l Broad. Co., 187 Cal. App. 3d 1463, 1485 (1986)).

[79] *Id.* at 1058.

tive exposes" written in objection to Defendant's specific conduct and beacon technology in general.[80] As further proof of the outrageous nature of Defendants' practices, Plaintiffs highlighted the number of Federal Trade Commission and Congressional inquiries and investigations that have been conducted on app developers' technologies.[81] Although the App Defendants did not contest that Plaintiffs' had a legally protectable privacy interest in their mobile address books, and that the applications intruded upon that interest by accessing the content of such books, they argued that Plaintiffs did not have (1) a reasonable expectation of privacy in such information, and (2) the intrusion was "not sufficiently offensive to give rise to a claim for intrusion upon seclusion."[82]

a. Reasonable expectation of privacy

Perhaps operating under the weight of the high protections the state of California places on cell phone data, as well as the influential dicta offered on this matter by the Supreme Court,[83] the *Opperman* court had little hesitation concluding that Plaintiffs' expectation of privacy in the content of their iDevice address books was reasonable as a matter of law.[84] The court also concluded that Plaintiffs maintained a reasonable expectation of privacy even after applications like Gowalla and Instagram had explicitly asked for their consent to use of the microphone upon application download, and even after the Apps

---

[80] *Id.*

[81] *Id.* at 1061.

[82] *Id.* at 1059.

[83] In refusing to extend the holdings of Chimel v. California, 395 U.S. 752 (1969) and United States v. Robinson, 414 U.S. 218 (1973) (precedent allowing for broader officer exemptions to search a suspect's possessions without a judicial warrant) the *Riley* court found an important distinction in the vast quantity of information that could be collected from the search of cell phones:

> [*Robinson* and *Chimel*] require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy. A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones. See A. Smith, Pew Research Center, Smartphone Ownership—2013 Update (June 5, 2013) . . .
>
> There are no comparable risks when the search is of digital data. In addition, *Robinson* regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*.

Riley v. California, 134 S. Ct. 2473, 2484-85 (2014).

[84] *Opperman*, 87 F. Supp. 3d at 1059.

had provided further notification of the microphones' activation.[85] In fact, the court declared the users' submission of consent had been "invalid" because it was "obtained by fraud."[86] The court explained its fraud determination was a function of Plaintiffs' allegation that App Defendants misrepresented their purpose when asking for consent: specifically, App Defendants had advertised that the app would only "'scan' Plaintiffs' address books for purposes of the 'find friends' feature."[87] Problematically, the app failed to disclose that as it scanned their address books, it would also be "transmit[ting] a copy of the address book to Defendants for their own [future] use."[88] According to Plaintiffs, if they had known of this future illicit purpose, they "would not have consented."[89]

b. Offensiveness

The most promising finding for future plaintiffs in beacon tracking suits seems to be the *Opperman* court's decision that Defendants' conduct was not "routine commercial behavior," and therefore, could be considered "highly offensive to the ordinary reasonable man."[90] In reaching this decision, the *Opperman* court first dismissed the prevailing precedent of the *iPhone* court, which had determined that App Defendants' "surreptitious tracking of personal data and geolocation information was not an 'egregious breach of social norms'" as to constitute "offensive [conduct] to the ordinary reasonable man."[91] In coming to this finding, the *iPhone* court relied on the holding of a 2011 case, *Folgelstrom v. Lamps Plus, Inc.*,[92] where Plaintiff advanced an intrusion upon seclusion claim based on defendant retailers' customary request for customers' zip codes in order to match them to home mailing addresses for future mail marketing.[93] Ultimately, the *Folgel-*

---

[85] *Id.* at 1060–61.

[86] *Id.* at 1060 ("*See* Rest. (2d) of Torts § 892B (1979) ("If the person consenting to the conduct of another is induced to consent by a substantial mistake concerning the nature of the invasion of his interests or the extent of the harm to be expected from it and the mistake is known to the other or is induced by the other's misrepresentation, the consent is not effective for the unexpected invasion or harm."); Sanchez–Scott v. Alza Pharm., 86 Cal. App. 4th 365, 377–78 (2001) (sustaining intrusion upon seclusion claim where doctor obtained consent of patient to breast examination in front of a drug salesperson without disclosing salesperson was not a medical professional).

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] *Id.* at 1060–61.

[91] *Id.* at 1060 (citing In re iPhone Application Litigation, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012)).

[92] 195 Cal. App. 4th 986 (2011).

[93] *Opperman*, 87 F. Supp. 3d at 1060 (citing *id.* at 992).

strom court dismissed the intrusion upon seclusion claim, concluding Plaintiffs did not have a legally protected private interest in their mailing addresses, and retailer's conduct was not egregious, but merely represented "routine commercial behavior."[94]

However, the *Opperman* court swiftly distinguished *Folgelstrom* from the facts at hand, after determining that the instant situation involved actual *theft* of the Plaintiffs' *personal* contact lists, which were deemed "more private than a person's mailing address."[95] Furthermore, although the court was cognizant of the argument that reasonable expectations should be eroded in the modern age of a connected and somewhat free-flowing Internet, it refused to agree that a "surreptitious theft of personal contact information" could be characterized as "routine commercial behavior."[96] Plaintiffs' evidence of wide public and Congressional condemnation of beacon tracking data collection, which included documented investigations and public statements made by consumer groups, the media, the Federal Trade Commission and Congress, added legitimacy to the court's affirmation of offensiveness.[97]

c. Damages

The court determined that Plaintiffs had successfully demonstrated Article III standing because the "intrusion" itself, represents an injury.[98] Therefore, App Defendants' defense that Plaintiffs had failed to adequately allege economic injury was to no avail.[99] According to the court, and in keeping pace with historic common law privacy actions, if Plaintiffs were to succeed on this claim, they could recover damages correlating to their "anxiety, embarrassment, humiliation, shame, depression, feelings of powerlessness, anguish, etc."[100]

---

[94] *Id.*

[95] *Id.* at 1061.

[96] *Id.*

[97] *Id.*

[98] *Id.* at 1061.

[99] *Id.*

[100] *Id.* (citing Operating Eng'rs Local 3 v. Johnson, 110 Cal. App. 4th 180, 187 (2003) (quoting Miller v. Nat'l Broad. Co., 187 Cal. App. 3d 1463, 1485 (1986))).

III. NUANCED CONSIDERATIONS AND ARGUMENTS WITHIN THE SPECIALIZED SPHERE OF ELECTRONIC PRIVACY LAW

A. The Wiretap Act & Other Federal Privacy Statutes Offer Plaintiffs Unpredictable Privacy Protections

A difficult problem posed to future plaintiffs affected by beacon technology is that any privacy intrusions wrought by the technology fail to neatly trigger a violation under one of the main existing federal privacy statutes, including: the Computer Fraud and Abuse Act,[101] the Stored Communications Act (Title II of the ECPA),[102] the Federal Wiretap Act (Title I of the ECPA),[103] the CAN-SPAM Act,[104] the Telephone Consumer Protection Act (TCPA),[105] the Children's Online Privacy Protection Act,[106] and the Video Privacy Protection Act.[107] While plaintiffs' challenges in this domain make sense theoretically—as beacon technology is arguably "acquiring" information about the user for a targeted marketing purpose—plaintiffs will likely continue to lose at the motion to dismiss stage. As evident in the *Satchell* court's analysis, despite Plaintiff showing the app had intentionally "intercepted" her oral communications based on its deliberate design features, the Court concluded she had not plausibly demonstrated that the apps had "captured" the content of her conversations by actually exercising possession or control over them.[108]

Relatedly, Plaintiff could not allege facts showing the app was even "activated" at the exact moment she had been engaged in the allegedly "captured" private conversations, thus leading to speculation as to whether contents of the conversation were actually acquired (as opposed to the Defendants merely collecting the beacon signals).[109] *Satchell* and *Rackemann* further demonstrate another perilous obstacle for future plaintiffs as presented by the "unlawful use" claim, wherein Plaintiffs must advance sufficient facts to demonstrate that the specific content of the alleged "intercepted" conversations correlated positively with the content of the subsequently targeted ads sent by the application.[110] This is an especially difficult task, as it will require

---

[101] 18 U.S.C. § 1030 (2012).

[102] 18 U.S.C. §§ 2701–2712 (2012).

[103] 18 U.S.C. § 2510 (2012).

[104] 15 U.S.C. §§ 7701–7713 (2012).

[105] 47 U.S.C. § 227 (2012).

[106] 15 U.S.C. §§ 6501–6506 (2012).

[107] 18 U.S.C. § 2710 (2012).

[108] Satchell v. Sonic Notify, Inc., 234 F. Supp. 3d 996, 1005–08 (N.D. Cal. 2017).

[109] *Id.* at 1006–07.

[110] *Id.* at 1008–09; Rackemann v. LISNR, Inc., No. 17-CV-624, 2017 WL 4340349, at *8–9

plaintiffs to eliminate all potentially contributing variables, namely the beacon signals, as being responsible for the content of the ads.

While the Plaintiff's claim in *Rackemann* survived the motion to dismiss stage an analysis suggests this was based on the Defendants' failure to include critical facts in its response about the limits of the beacon technology in its app. Namely, Defendants' failed to respond with documentation .hat the app merely captured inaudible beacon signals, as opposed to intercepting audible sounds or communications. Moreover, the Defendants failed to provide important documented explanations related to the limited activation periods in which the microphone is turned on (a function that is controlled by the App Developers and the Colts).[111] If the Defendants were able to show specific times and limits to the microphone's use in an amended response, it would be unlikely that a plaintiff could fully document that her conversations took place at the exact moments the microphone was activated.

B. The Threat of Common Law Privacy Claims Against Defendants Offers More Consistent Protection for Plaintiffs, Particularly in California

However, based on the *Opperman* court's promising analysis of Plaintiffs' intrusion upon seclusion claim, not all hope is lost for future beacon technology litigants. In fact, throughout history, common law privacy claims have been seen as particularly useful when a particular privacy issue fails to fall neatly within the scope of statutory relief offered by current privacy statutes.[112] The limits of these statutes, as evident by the unsuccessful electronic privacy suits in Northern California, are likely a function of the rapid pace in which technology shifts, leaving the legislature in the dust when it comes to the creation of encompassing laws.

1. Main differences between federal privacy laws and the common law avenue

Unlike federal and state privacy statutes, common law privacy theories require that plaintiffs mount an additional hurdle of having to show that the information invaded is sufficiently "private."[113] Moreover, unlike California courts, a number of other state courts will require plaintiffs to prove injury beyond the mere invasion, which can

(S.D. Ind. Sept. 29, 2017).

[111] *Rackemann*, 2017 WL 4340349, at *6–7 (S.D. Ind. Sept. 29, 2017).

[112] BROWNSTONE & NEWBY, *supra* note 3 § 9:120.

[113] *Id.*

prove a difficult burden when dealing with speculative invasions of privacy. However, generally, the heart of a court's analysis for this theory will still center upon the issues of (1) whether plaintiffs had a reasonable expectation of privacy in the information, and (2) whether the conduct of the defendant was "sufficiently egregious or offensive to justify relief."[114]

2. The general common law invasion of privacy umbrella

States vary in the degree to which they recognize the four common law privacy causes of action, which include: (a) intrusion upon the seclusion of another; (b) appropriation of another's name or likeness; (c) public disclosure of private facts; and, (d) publicity that places the other in a false light before the public.[115] For example, some states like North Dakota and Wyoming refuse to recognize any of the theories in common law or statutory form.[116] On the other hand, California, a state where a vast quantity of technology litigation occurs because of the presence of technology companies, recognizes all four common law privacy theories.[117] Nonetheless, plaintiffs engaging in most types of electronic privacy litigation, including plaintiffs in *Opperman*, most commonly invoke: (1) intrusion upon the seclusion or solitude of another; and (2) public disclosure of private facts.[118]

3. Intrusion upon seclusion in California

Guided by the Second Restatement of Torts, California's "intrusion upon seclusion" framework requires a plaintiff to demonstrate a defendant's: (1) intentional intrusion into a private place, conversation, or matter, (2) in a manner "highly offensive to a reasonable person."[119] To satisfy the first element, a plaintiff must demonstrate that "the defendant penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data . . . [and] the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source."[120] A plaintiff's reasonable expectation of privacy in the information disclosed is a question of fact analyzed based on contextual circumstances.[121]

---

[114] *Id.*

[115] *Id.* § 9:123.

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.* § 9:124 (citing Restatement (Second) Torts § 652B (1977 & Supp. Oct. 2014)).

[120] *Id.* (citing Shulman v. Grp. W. Prods., Inc. 955 P.2d 469 (Cal. 1998)).

[121] *Id.* (citing Sanders v. Am. Broad. Cos. 978 P.2d 67, 69 (Cal. 1999)).

California's guaranteed constitutional protections of privacy, coupled with the state's strong historic precedent supporting common law privacy actions, foster a powerful environment for future plaintiffs litigating electronic privacy claims. For example, the California Supreme Court has made clear through a number of rulings that "targeted video surveillance" by private and public employers can represent an intrusion into employees' reasonable expectation of privacy, even if the private sector employer "did not expect or intend to catch plaintiffs on tape."[122] Moreover, echoing the state's long line of judicial decisions on the matter, California statutes strictly prohibit all forms of video surveillance in a number of listed locations, as well as "*any other area* in which the occupant has a reasonable expectation of privacy," the latter of which based on circumstances and context.[123] In the backdrop of these rulings and statutory provisions, it would seem beacon litigants could make a strong case that courts should view prohibited video surveillance in the same light as pervasive beacon audio and physical tracking surveillance. Both forms of surveillance provide a comprehensive biographical picture of plaintiff's whereabouts, habits, and activities. Moreover, in anticipation of defendant application developers' argument that a beacon powered app is not designed intentionally to track the oral communications of plaintiffs, plaintiffs can counter with the argument that users' microphones turn on and off (based on users' physical location), without explicitly notifying the users of every activation or requiring consent at the given moment the technology begins collecting data.[124]

Although California's intrusion upon seclusion precedent has not been tested fully in the electronic privacy sphere, the notably progressive tendency of California's federal and state courts' decision-making on electronic privacy issues suggests that judges will likely be willing to accept litigants' arguments regarding the "offensive" and "unreasonable" nature of beacon technology intrusions into individuals' "physical" and "sensory" zones of privacy.[125] In fact, as outlined above,

---

[122] *Id.* (citing Hernandez v. Hillsides, Inc., 211 P.3d 1066 (Cal. 2009)).

[123] *Id.* at n.14.

[124] A court could in fact, conclude this is an "egregious" or "offensive" lack of consent, even after users' offered general consent to the microphone's use upon download.

[125] *Opperman*, 87 F. Supp. 3d 1018, 1059 (N.D. Cal. 2014) ("*See, e.g.*, United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) ('[C]ell phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber numbers. Zavala had a reasonable expectation of privacy regarding this information.'); United States v. Cerna, No. 08-CV-730, 2010 WL 5387694 (N.D. Cal. Dec. 22, 2010) (citing *Zavala*) ('Luis Herrera had a reasonable expectation of privacy in the contents of the seized phones as his physical possession of the cell phones created a reasonable expectation of privacy in their contents.'); United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993) (criminal defendant had expectation of privacy in contents of pager because '[t]he expectation of privacy in an electronic repository for personal data is therefore analogous to that in a personal address book or other repository for such infor-

California courts have already gotten a sense of this type of litigation in *Opperman*.[126] Furthermore, although the factual scenarios presented by *Satchell* and *Opperman* were not analogous, it is not a stretch to pinpoint relevant parallels between both complaints as to warrant an extension of the *Opperman* analysis to future beacon litigation.

Particularly, while *Satchell* can be viewed as a case centered upon defendant app developers' surreptitious collection of identifying information about phone users' via users' address books, *Opperman* can be viewed similarly as defendant app developers undertaking a surreptitious collection of identifying information about phone users' via their locations and audible noises. In both cases, it is clear that the defendants' intentional actions contributed to the building of a comprehensive biographical profile of application users without their explicit consent.[127] Because plaintiffs were bringing the action under common law intrusion upon seclusion (as opposed to the Wiretap Act), the courts were able to decisively make a ruling that the "surreptitious theft of personal contact information," was sufficiently offensive, and did not qualify as "routine commercial behavior."[128]

Future litigants can also take solace in the *Opperman* court's decision to dismiss Defendants' undisputed assertion that Plaintiffs had voluntarily installed the applications on their phones and *had voluntarily* consented to turning on the app's scanning feature during the application download process.[129] In so doing, the court dismissed Defendant's central claims that Plaintiffs' voluntary consent should bar them from alleging Defendants' conduct was highly offensive.[130] Critically, the court accepted Plaintiffs' standing based on the simple existence of an alleged "intrusion," which qualified as the "injury."[131] Accordingly, Defendants' contestation that Plaintiffs lacked standing because of failure to allege any harm or calculate damages was ignored.[132]

Also relevant for future litigants is the California courts' general willingness to accept that citizens have a reasonable expectation of privacy in the contact information stored in their phones, as held by

---

mation')").

[126] *Id.* at 1018.

[127] *See id.* at 1033; *see also* Satchell v. Sonic Notify, Inc., 234 F. Supp. 3d 996, 999–1000 (N.D. Cal. 2017).

[128] *See* 87 F. Supp. 3d at 1061.

[129] Opperman v. Path, Inc., 87 F. Supp. 3d 1018, 1060 (N.D. Cal. 2014) (stating that if activated by consent, the app's scanning feature would scan users' address books to connect such user to other "friends" in the app's network).

[130] *Id.* at 1060.

[131] *Id.* at 1061.

[132] *Id.*

the *Opperman* court.[133] That ruling notably breaks pace with other federal courts, who have suggested that in the modern age of technology, phenomena like data-sharing, Cloud enabled devices, and an increasingly connected, public internet atmosphere, can erode such expectations.[134]

Clearly then, when drafting their intrusion upon seclusion common law claims for California courts, beacon litigants should emphasize the following in their complaints:

1) Assert their Article III standing by demonstrating the simple existence of an unlawful "intrusion," as defined by beacon-detecting microphones operating at unknown intervals at unknown times when the phone was turned on;

2) Argue that despite their voluntary consent to the activation of microphones upon app download, they "would not have consented" had they known *all* of the specific times in which the microphone would be on, as well as the *specific unlawful purposes* for which the microphone would be used by app developers and third-parties: namely, that the content would be used for the collection of data about the user's identity and activities to be utilized for future marketing purposes;

3) Argue that they were not offered an opportunity to explicitly consent to *each* instance in which the microphone was turned on, which included potential periods where the microphone was activated during their private conversations;

4) Argue that the *Opperman* ruling related to Plaintiffs' reasonable expectation of privacy to contact information in their phone (the data in their mobile address book) can be easily extended to include phone users' reasonable expectation of privacy in the content, sounds and locations of their bodies while carrying their phones; and,

5) Reference Congressional hearing and investigations to support the claim that unexpected beacon tracking is "highly offensive," which in no way should qualify as "routine commercial behavior," based on industry standards.

Although the aforementioned intrusion upon seclusion factors could compel a number of California judges, they would likely not car-

---

[133] *See id.* at 1059; *see also* BROWNSTONE & NEWBY, *supra* note 3, § 9:124 at n.29 (citing *Chan*, 830 F. Supp. 531, 534–35 (N.D. Cal. 1993)).

[134] *See* BROWNSTONE & NEWBY, *supra* note 3, § 9:124 at n.30.

ry the same force under a state or federal Wiretap Act theory given the legal limits of the latter.

C. Constitutional Backdrop Will Favorably Influence the Way Judges Evaluate State Common Law Privacy Claims

The most important justification for plaintiffs to take advantage of common law intrusion upon seclusion theories relates to the Supreme Court's significant holding in *Riley v. California*,[135] where the Justices held that a law enforcement officer's warrantless search of the contents of a defendant's cell phone incident to his arrest violated the Fourth Amendment.[136] When reaching the decision in *Riley*, the high court made clear that individuals have reasonable and strong expectations of privacy in the data stored on their mobile phones, which may even exceed the privacy interests they have in physical objects and documents located in their homes.[137] Although the case related to Fourth Amendment searches of an alleged subject's cell phone, in dicta, the majority speculated about privacy concerns in other areas, particularly in connection to mobile phone applications and embedded tracking technology. Of special note, the Court elaborated about the dangers posed by the expansive capabilities of GPS monitoring devices:

> Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life.[138]

Both of these significant premises have, and will continue, to impact the factors evaluated by California courts in an electronic privacy intrusion upon seclusion common law claim and relate critically to fact patterns involving beacon technology. In taking advantage of this holding in the future, beacon litigants should be prepared to argue:

> 1) They have reasonable and strong expectations of privacy regarding the data stored on their mobile phones, which in-

---

[135] 134 S. Ct. 2473 (2014).

[136] BROWNSTONE & NEWBY, *supra* note 3, § 9:124 (citing *Riley*, 134 S. Ct. at 2473).

[137] *Id.* (citing *Riley*, 134 S. Ct. at 2490).

[138] *Id.*

> cludes any audible noises, or movements, captured by their phones through their basic use;
>
> 2) As similar to GPS monitoring devices, which the Supreme Court now expresses concerns about, beacon technology allows for the generation of a "precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations."[139] However, technology experts contend that beacon technology is even more invasive than GPS tracking technology, in that it: (1) can be activated even when the phone is not connected to the internet; and (2) has the power to track physical *and* audio data.[140]

Another influential finding by the Supreme Court, which could serve as helpful backdrop for future beacon litigation, is derived from Justice Sonia Sotomayor's concurrence (signed onto by five Justices) in *United States v. Jones*, where she suggested the necessity of maintaining high protections for person's privacy interests during the routine and voluntary disclosure of electronic data to third party service providers:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[141]

With the *Opperman* court's example, courts will likely find the weight of this statement to be particularly influential when evaluating companies' defenses that their behavior was not "offensive" under the in-

---

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

[140] Newman, *supra* note 16.

[141] BROWNSTONE & NEWBY, *supra* note 3, 9:124 (citing *Jones*, 565 U.S. at 417); *See also* Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) (holding that Defendant had reasonable expectation of privacy under Massachusetts Constitution in cell site location information maintained by Defendant's mobile phone provider)); *but see* United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (holding that third-party doctrine applies to cell site location information); *see also* United States v. Post, 997 F. Supp. 2d 602 (S.D. Tex. 2014) (holding that Defendant had no privacy interest in metadata of photos posted online).

trusion upon seclusion standard because plaintiffs had *voluntarily* provided consent to the use of the microphone. In fact, it would seem that all future "voluntary consent" defenses, particularly when used by application developers who incorporate beacon technology into their products, will be moot. Instead, judges will likely sympathize with users' lack of awareness that they were consenting to such an extraordinary disclosure of identifying information in the course of performing a mundane task like downloading a mobile phone application.

D. Why Common Law Theories Are Superior to a Legislative Response within the Electronic Privacy Sphere

Given the increasing ubiquity of beacon-like technology within mobile phone applications, observers of this legal quandary likely believe Congress or state legislatures will have sufficient incentive to propose another electronic privacy law tailored to the specific nuances of audio-GPS tracking technology. But while a statute to fill this legal hole would prove helpful, its effectiveness would be severely limited. This is because the rate of change within various technology subsectors may present complex issues defying simple statutory solutions. The burgeoning beacon audio-tracking technology industry is of no exception, as the profits of commercial advertising are tied to beacon developers' abilities to continually enhance the capturing capabilities of their technology in order to present their clients with the greatest information related to consumers' preferences.

Validating this conclusion with empirical evidence, law and economics scholars Luca Anderlini, Leonardo Felli, and Alessandro Riboni suggest that common law theories of relief provide far greater flexibility and efficiency than statutes if the legal environment is "sufficiently heterogeneous and/or changes sufficiently often."[142] Alternatively, the three assert, if the legal environment is "sufficiently homogenous and/or does not change very often, the Statute Law regime dominates," and benefits society by restraining courts from "behav[ing] myopically and neglect[ing] *ex-ante"* welfare and policy considerations in their statutory interpretation.[143] This thesis is well-applied within the context of beacon audio-tracking technology, where the flexibility and factually sensitive nature of the "reasonable expectations of privacy" and "offensiveness" prongs of an intrusion upon seclusion claim can be adapted progressively to the nuanced circumstances presented by novel beacon fact patterns. As a result, plaintiffs

[142] Luca Anderlinie et al., Statute Law or Case Law?, (July 2008) (unpublished manuscript) (on file with author), https://www.econstor.eu/bitstream/10419/26403/1/577103636.PDF [https://perma.cc/WDZ9-KLRW].

[143] *Id.* (emphasis added).

will be offered far greater leeway in advancing compelling arguments within their complaints and at summary judgment that underscore the seriousness and unexpected nature of the privacy violation. Unique arguments of this nature rarely fit within the rigid statutory framework of provisions like § 2511(1)(a) and § 2511(1)(d) of the Wiretap Act.

In addition, the political realities of the legislative process suggest that common law theories would offer a more reliable mechanism in which to protect plaintiffs' privacy rights. Unlike Congress or state legislatures, state and federal judges are isolated from the overwhelming influence levied by interest groups in the crafting and interpretation of law.[144] America's technology sector in particular, which includes the "repeat" offenders in beacon litigation, is represented by prominent and well-funded lobbyists in Washington, D.C., who exert enormous pressure in ensuring sector-specific laws do not hamstring the use and profitability of their clients' main products.[145] Such influence suggests that any state or federal legislative response could be watered down significantly at the peril of consumers' rights.

In comparison to distant state legislatures and Congress, district judges within certain regions of the country are beginning to see more derivations of general electronic privacy issues and specific beacon claims. Repeated exposure to similar facts, evidence, and expert witnesses lends itself to judges' greater familiarity with the problems posed by these new technologies. Ultimately, judges' increased knowledge and specialized understanding of this area of law could be used most effectively in their informed weighing of the equities and merits of the common law privacy standards through which plaintiffs assert their grievances.

IV. CONCLUSION

At present, America is confronting an uneasy tug-of-war between the benefits bestowed by technology designed to provide users "the best experience possible" and consumers' long-cherished expectations that their actions relating to their cell phone usage will remain private. Unfortunately, beacon technology, with its hybrid GPS location tracking features and auditory capturing mechanisms, penetrates into

---

[144] Roger Hayes, *Living by the Rule of Law*, IANPJ ON POLITICS (last visited Feb. 23, 2018), https://pjcjournal.wordpress.com/common-law-vs-statutes/ [https://perma.cc/3PWA-CXFB].

[145] *See, e.g.*, Information Technology Industry Council, *https://www.itic.org/* [https://perma.cc/2QJT-6QKW]; *see also* Kieran McCarthy, *Biggest Washington DC Lobbyist Is Now a Tech Giant (Yes, It's Google)*, THE REGISTER (Jan. 24, 2018), https://www.theregister.co.uk/2018/01/24/google_washington_lobbying/ [https://perma.cc/LFC7-EZJD].

two sacred spheres of citizens' space, and does so without any explicit consent by users.

Fortunately citizens can "pushback" against unwanted intrusions within the court system, with the very act of filing cases sending a powerful message to application developers and their clients that beacon technology must be limited. As this Comment has discussed, given the slowness in which privacy laws are amended and the very segmented nature of this set of laws in the first place, the beacon fact pattern fails to fall neatly into any present legal framework. Even the Wiretap Act, which initially appeared to offer the most promising vehicle for beacon technology intrusions, has produced unpredictable results for plaintiffs. As a result, the privacy rights of unwitting beacon technology users have remained vulnerable and inconsistently protected.

Accordingly, the uncomfortable lapse in the law should encourage plaintiffs to reconsider trying their beacon claims under the old but continuously flexible state common law privacy theories, particularly the intrusion upon seclusion theory. Although not originally intended for such novel privacy scenarios, the intrusion upon seclusion theory has proven powerful in providing plaintiffs an adaptable and favorable framework through which to establish defendant's "intentional" intrusion into any private *place*, *conversation*, *matter*, or *data source*. The positive direction of recent Supreme Court decisions, such as *Riley v. California*[146] and *United States v. Jones,*[147] where the Justices have expressed concerns about the "highly offensive" nature of certain conduct and the "reasonableness" of technology users' expectations, provides future plaintiffs an opportunity to draft their complaints in a compelling manner that will satisfy both prongs of the intrusion upon seclusion test, while avoiding having to overcome the "interception" hurdle of the Wiretap Act.

[146] 134 S. Ct. 2473 (2014).

[147] 565 U.S. 400 (2012).