Spring 2011

Re-Mapping Privacy Law: How the Google Maps Scandal Requires Tort Law Reform

Lindsey A. Strachan
University of Richmond

RE-MAPPING PRIVACY LAW: HOW THE GOOGLE MAPS SCANDAL REQUIRES TORT LAW REFORM

By Lindsey A. Strachan

Cite as: Lindsey Strachan, *Re-Mapping Privacy Law: How the Google Maps Scandal Requires Tort Law Reform*, XVII RICH. J.L. & TECH. 14 (2011), http://jolt.richmond.edu/v17i4/article14.pdf.

I. INTRODUCTION

[1] In the Internet savvy and technology dependent world of today, it is difficult to imagine life without Google Maps. The pioneer web-mapping platform provides users with a number of free services, ranging from simple directions to high-resolution imagery of terrain. The service has revolutionized travel, providing guidance and resources to more than just the directionally challenged. Contributing to this notoriety was Google's addition of "Street View" to the array of mapping functions in May of 2007.[1] As its name implies, the Street View function allows users to view enhanced, 360-degree snapshots of homes, streets and other public property.[2] According to Google, the Street View photographs further aided users of the platform by providing accurate images of destinations,

[1] *See* Stephen Chau, *Introducing… Street View!*, GOOGLE LAT LONG BLOG (May 29, 2007, 10:11 AM), http://google-latlong.blogspot.com/2007/05/introducing-street-view.html.

[2] *See Cars, Trikes & More*, GOOGLE MAPS, http://maps.google.com/help/maps/streetview/technology/cars-trikes.html (last visited Apr. 4, 2011).

but revealed no more than "what any person can readily . . . see walking down the street."[3]

[2] Despite Google Map's ubiquity, the Street View application has faced controversy since inception.[4] Often capturing more than just streets, Street View photographs have garnered a reputation for catching unlucky subjects in embarrassing, compromising or even revealing situations.[5] Legal scholars point to these images as gross invasions of privacy, using the publicity of the photos to bolster the growing movement in favor of expanding tort privacy law.[6] Bloggers have had a field day over the number of strange and amusing images that appear on Street View, with some websites hosting competitions for the "Best Urban Images Captured,"[7] and others creating a gallery of images, ranking, cataloging, and displaying provocative photos.[8]

---

[3] Miguel Helft, *Google Zooms in Too Close for Some*, N.Y. TIMES, June 1, 2007, http://www.nytimes.com/2007/06/01/technology/01private.html.

[4] *See, e.g.*, Boring v. Google, Inc., 362 F. App'x 273, 276 (3d Cir. 2010) (involving a privacy suit brought against Google for images posted on Google Maps Street View program); Transfer Order, *In re*: Google Inc. Street View Elec. Commc'ns Litig., 733 F. Supp. 2d 1381, 1382 (J.P.M.L. 2010) (involving a number of suits consolidated into one class action against Google for violations of the Wiretap Act).

[5] *See, e.g.*, GOOGLE STREET VIEW SIGHTINGS, http://www.gstreetsightings.com/ (last visited Mar. 23, 2011); STREETVIEWFUNNY.COM, http://www.streetviewfunny.com/streetviewfunny/index.php (last visited Jan. 10, 2010); *TOP 100 STREETVIEW – HIGHEST RATED*, STREETVIEWFUN, http://www.streetviewfun.com/top-100/ (last visited Mar. 23, 2011).

[6] *See, e.g.*, Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity*, 49 SANTA CLARA L. REV. 313, 354-55 (2009) (calling for a new tort, "The Right to Your Digital Identity"); Andrew Lavoie, *The Online Zoom Lens: Why Internet Street-Level Mapping Technologies Demand Reconsideration of the Modern-Day Tort Notion of "Public Privacy,"* 43 GA. L. REV. 575, 606-08 (2009).

[7] Ryan Singel, *Request for Urban Street Sightings: Submit and Vote on the Best Urban Images Captured by New Google Maps Tool*, WIRED (May 30, 2007), http://www.WIRED.COM/threatlevel/2007/05/request_for_urb/.

[8] *See* STREETVIEWFUNNY.COM, *supra* note 5; *TOP 100 STREETVIEW – HIGHEST RATED*, *supra* note 5.

[3] However, the public photographs of unknowing subjects are not the only cause for concern. In May of 2010, the Internet giant publicly admitted to inadvertently collecting private and personal information via Street View mapping camera cars.[9] In the face of looming lawsuits, and with more than thirty countries affected, Google's *mea culpa* reassured the public it would delete some of the information, change its privacy policies, and promise never to use the collected data.[10]

[4] This Comment explores how the law should handle such privacy claims. In analyzing both the photographic privacy claims as well as the Wi-Fi data privacy claims, this paper argues that current tort law is inadequate for such technologically advanced legal issues. Section II explores the background of Google Maps Street View and current privacy law, while Section III looks at the holes in current privacy torts in the context of the images displayed on Street View. Section IV examines the privacy implications surrounding the Wi-Fi scandal, and finally, Section V reviews the solution and provides a conclusion.

II. BACKGROUND AND HISTORY

A. Google Maps and Street View

[5] In May of 2007, Google added the Street View platform to its already popular and successful Google Maps Internet service.[11] The service initially allowed users to access panoramic views of only five

[9] *See Wi-Fi Data Collection: An Update*, THE OFFICIAL GOOGLE BLOG (May 14, 2010, 1:44:00 PM), http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html ("But it's now clear that we have been mistakenly collecting samples of payload data from open (i.e. non-password protected) WiFi networks, even though we never used that data in any Google products.").

[10] *See* Cecilia Kang, *Promise by Google Ends FTC's Privacy-Breach Probe*, WASH. POST, Oct. 28, 2010, at A15 [hereinafter Kang, *Promise by Google*] ("In a letter to Google on Wednesday, the FTC said privacy concerns over its Street View cars' data collection were allayed when the search giant announced that it would beef up privacy training for employees and not use any collected data for any Google products or services.").

[11] *See* Chau, *supra* note 1.

major U.S. cities, but since the platform's launch, "almost a dozen countries around the world in North America, Europe and the Asia-Pacific region" are now accessible via Street View.[12] According to Google, the images are collected using vehicles equipped with special cameras to capture 360-degree views of streets, GPS units to track and position the photographs, and laser range scanners.[13] However, Google's camera-equipped vehicles are not limited to the streets; vans, cars and "trikes" have helped Street View access a wider variety of terrain in order to help field the growing platform.[14]

[6] After the initial collection of photographs, the images must thereafter undergo processing to become Street View ready.[15] Google takes the overlapping photographs gathered by the fleet of camera-equipped vehicles and "stitches" them together in order to produce the 360-degree panoramic shot users of Google Maps see.[16] Navigational arrows, along with Street View's iconic "Pegman" allow users to explore the platform by "walking" down streets and rotating the camera view, giving the illusion of physically being on the street.[17]

[7] Inevitably, the images' ease of accessibility, in conjunction with the lack of any prior consent from subjects raises a number of privacy issues for the platform.[18] Although websites track and make light of

[12] Matt Williams, *Behind the Scenes*, GOOGLE MAPS UK, http://maps.google.co.uk/intl/en/help/maps/streetview/behind-the-scenes.html (last visited Apr. 7, 2011).

[13] *See id*.

[14] *See Cars, Trikes & More*, *supra* note 2. For instance, Google Maps uses a bicycle creatively dubbed a "Trike," a snowmobile, and even a trolley to allow cameras access to areas not easily traversed by cars or vans. *Id.*

[15] *See Turning Photos into Street View*, GOOGLE MAPS, http://maps.google.co.uk/help/maps/streetview/technology/ photos-into-street-view.html (last visited Apr. 4, 2011).

[16] *See id.*

[17] *See Who Is Pegman?*, GOOGLE MAPS, http://maps.google.co.uk/help/maps/streetview/learn/pegman.html (last visited Apr. 4, 2011).

[18] *See generally Investigations of Google Street View*, EPIC, http://epic.org/privacy/streetview/ (last visited Apr. 4, 2011).

humiliating images captured by Street View, to most, appearing on the mapping website can be both personally alarming and publically humiliating.[19] Consider first the blatantly harmful images: young girls scantily clad, advertising a car wash in Texas;[20] a teenager aiming a gun at a child;[21] policemen at a crime scene;[22] a man walking down the street with a large rifle;[23] or a man entering a pornographic bookstore.[24] It does not take a legal scholar to recognize the privacy implications inherent in such photographs. Yet, even the seemingly harmless images spark privacy concerns.[25] For instance, the shot of a boy falling off his bike at his home might seem harmless, but in reality, it reveals the exact address and photo of a minor's home.[26] On the other hand, images of pedestrians, a person enjoying a cigarette, or cars parked in driveways are not overtly revealing, but still provoke a sense of illegal infringement into personal matters.[27]

---

[19] *See, e.g.*, Helft, *supra* note 3 (describing the reactions of a woman who could see her cat sitting in the living room of her apartment on Street View).

[20] *See Galleries: The Best of Google Street View*, NEWS.COM.AU, http://www.news.com.au/technology/gallery-e6frflwi-1111120174373?page=10 (last visited Jan. 10, 2011).

[21] *See Google Maps Catches Chicago Kid About to Shoot Someone*, GAWKER (May 20, 2008, 12:24 EST), http://gawker.com/392059/google-maps-catches-chicago-kids-about-to-shoot-someone.

[22] *See* Sam Knight, *All-seeing Google Street View Prompts Privacy Fears*, THE TIMES (June 1, 2007), http://technology.timesonline.co.uk/tol/news/tech_and_web/article1870995.ece.

[23] *See What is This Man Doing?*, STREETVIEWFUN (Jan. 11, 2009), http://www.streetviewfun.com/2009/what-is-this-man-doing/.

[24] *See* Helft, *supra* note 3.

[25] *See, e.g.*, *id.* (discussing how a woman felt that even the image of her apartment was an uncomfortable infringement upon her privacy).

[26] *See Galleries: The Best of Google Street View*, *supra* note 20.

[27] *See* Helft, *supra* note 3 (describing the debate over the privacy concerns raised by Street View).

[8] One couple in Pennsylvania felt so wrongfully violated they sued Google over images of their home posted on Street View.[28] Despite the fact that the Plaintiffs lived on a private road, a search for their address on the mapping platform resulted in "colored imagery of their residence, including the swimming pool."[29] Even in the face of similar pending litigation and accusations of privacy infringement, Google maintains it has done nothing illegal.[30] Reasoning that Street View technology is no more revealing than what is already public, the company insists there is no privacy breach.[31]

[9] In addition to the Street View image privacy claims, the Wi-Fi data collection, first reported in May 2010, has renewed the growing calls for investigations of and prosecutions against the Internet giant for breach of privacy.[32] D.C. Council Member Jim Graham has even ventured so far as to term the data collections "'big brother-like' invasion[s] of privacy."[33] While the term "big brother" might, at first gloss, seem overly paranoid and extreme, upon discovery of the type of information Google intercepted, the reference is more appropriate.[34] Google has admitted that,

---

[28] *See* Boring v. Google, Inc., 362 Fed. App'x 273, 276 (3d Cir. 2010). The court, however, found that this was not enough to hold Google liable for breach of privacy. *See id.* at 283.

[29] *Id.* at 276 (citation omitted).

[30] *See Privacy*, GOOGLE MAPS, http://maps.google.com/help/maps/streetview/privacy.html (last visited Apr. 4, 2011) (reassuring the public that Street View imagery is from "[p]ublic access only," is "not [in] real time," and blurs all faces and licenses plates).

[31] *See* Helft, *supra* note 3. Anchoring Google's promises of legality is the notion that there is no breach of privacy when any Joe takes a stroll in his neighborhood. *See id.* "[C]ourts have consistently ruled that people in public spaces can be photographed. 'In terms of privacy, I doubt if there is much of a problem.'" *Id.* (citation omitted).

[32] *See* Cecilia Kang, *Growing Anger over Google Street View Privacy Breach*, POST TECH (May 20, 2010 8:00 AM), http://voices.washingtonpost.com/posttech/2010/05/the_anger_is_growing_over.html [hereinafter Kang, *Growing Anger*].

[33] *Id.* (quoting D.C. Council Member Jim Graham).

[34] *C.f. id.* (acknowledging that Google's intercept of "private data from residental [sic] WiFi networks" might be enough to justify Graham's push for investigations).

in trying to collect "names of and indentifying information of Wi-Fi access points," it mistakenly collected three years of data from unsecured wireless networks.[35] This "mistake" resulted in Google's collection of private and personal "e-mail addresses, e-mails (with usernames and passwords, home addresses, phone numbers and more)."[36] In response to Google's admission, both the U.S. Federal Trade Commission ("FTC"), and the U.S. Federal Communications Commission ("FCC") launched investigations into potential violations of U.S. Wiretap Act and the U.S. Communications Act.[37] Even though public opinion might agree more with Graham's "big brother" assertion, the FTC dropped their investigation without penalty or sanction.[38] The FCC investigation, however, remains open and ongoing.[39]

[10] The most popular reason for the lack of penalty against Google is Google's self-initiated response to the Wi-Fi scandal.[40] Google has assured the public that "the company has not used and will not use any of the payload data collected in any Google product or service, now or in the future."[41] Additionally, the search engine has subsequently altered its

[35] David Kravets, *FCC Probing Google Wi-Fi Spy Scandal*, WIRED (Nov. 11, 2010, 2:29 PM), http://www.wired.com/threatlevel/2010/11/fcc-googleWi-Fi-probe/ [hereinafter Kravets, *FCC Probing Google*].

[36] Matt McGee, *Google Maps Privacy: The Street View & Wifi Scorecard*, SEARCH ENGINE LAND (Nov. 11, 2010, 2:07 PM), http://searchengineland.com/google-street-view-scorecard-55487.

[37] *See* Kravets, *supra* note 35; *see also* Amy Schatz & Amir Efrati, *FCC Investigating Google Data Collection*, WSJ.COM (Nov. 11, 2010, 2:01 PM), http://online.wsj.com/article/SB10001424052748704804504575606831614327598.html.

[38] *See* Clint Boulton, *FTC Forgives Google Street View Wi-Fi Privacy Gaffe*, EWEEK.COM (Oct. 27, 2010), http://www.eweek.com/c/a/Security/FTC-Forgives-Google-Street-View-WiFi-Privacy-Gaffe-839368/.

[39] *See* Kravets, *supra* note 35; Schatz & Efrati, *supra* note 37.

[40] *See* Boulton, *supra* note 38.

[41] John D. Sutter, *FTC Ends Google 'Street View' Investigation without Fines*, CNN TECH (Oct. 27, 2010), http://articles.cnn.com/2010-10-27/tech/ftc.google.investigation_1_wi-fi-data-alan-eustace-google-maps?s=PM:TECH (quoting David C. Vladeck, Director for Consumer Protection, FTC).

privacy policies, adding new face-blurring technology, and allowing users to request blurring or complete removal of images.[42] The company even went a step further by reminding users that the photographs are no different from what any person could see driving or walking around themselves, and that the images are not in real time.[43]

B. Privacy Law

[11] Although the privacy implications in Google Maps Street View photographs and data collections seem well founded, privacy laws have remained relatively stagnant in the latter part of the twentieth century.[44] It is precisely this inflexibility and reliance upon out-dated and "fossilized" principles that render current privacy law inept for the complexities related to issues over Internet mapping.[45]

[12] The United States Constitution tangentially provides many protections of privacy rights, such as the guarantee that the government will refrain from intruding in private speech, religion, homes, or thoughts.[46] As Justice Douglas noted in *Griswold v. Connecticut*, "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy . . . . [T]he right of privacy . . . is a legitimate one."[47] In conjunction with the privacy guarantees in the

---

[42] *See Privacy*, *supra* note 30.

[43] *See id*. ("Street View contains imagery that is no different from what you might see driving or walking down the street.").

[44] *See, e.g.*, Daniel Solove, *The Slow Demise of Defamation and Privacy Torts*, CONCURRINGOPINIONS (Oct. 11, 2010, 4:42 PM), http://www.concurringopinions.com/archives/2010/10/the-slow-demise-of-defamation-and-the-privacy-torts.html ("The privacy torts are fossilized into the forms they were in circa 1960, and they haven't evolved to address modern privacy problems. Moreover, courts cling to antiquated notions of privacy . . . .").

[45] *Id.*

[46] *See generally* U.S. CONST. amends. I – V.

[47] Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (citations omitted).

"penumbras," codified and common law privacy rights also exist.[48] Currently, each state develops its own tort law system, and consequently, its own privacy tort scheme.[49] Despite the lack of a federal, unified code, such systems stem from two prototypal privacy doctrines; that from Warren and Brandeis in the late nineteenth century,[50] and that from Dean Prosser and the RESTATEMENT (SECOND) OF TORTS in the mid-twentieth century.[51]

[13] The founders of privacy law, Warren and Brandeis, recognized the need for an acknowledged and legitimized right to privacy, defining the right as the "right to be let alone."[52] Building upon similar rights found in other areas of law, the privacy pioneers sought to construct a right of privacy responsive to the advancement of the media and of the photographer.[53] In viewing privacy as a right held by the individual, Warren and Brandeis wanted to prevent the affairs of a non-public person "from being dragged into an undesirable and undesired publicity."[54] Further, Warren and Brandeis wisely confined the right of privacy so that those persons who live in the public eye could not take protection in the

---

[48] *See id.*; *see also* RESTATEMENT (SECOND) OF TORTS § 652A (1977) (outlining the four torts enumerated by Prosser).

[49] States can accept the Restatement and Prosser's Torts as they desire. *See generally id.* § 652A.

[50] *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890).

[51] *See generally* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

[52] Warren & Brandeis, *supra* note 50, at 193.

[53] *See id.* at 196-97, 206 ("The press is overstepping in every direction the obvious bounds of propriety and of decency . . . . It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.").

[54] *Id.* at 214.

right.[55] Recognizing "public interest" can warrant publicity of private facts, the duo made sure to identify the scope of the privacy right.[56]

[14] Stepping in where Warren and Brandeis left off, Dean Prosser established the principles of privacy law still in effect today.[57] Prosser outlined four torts within the umbrella tort of invasion of privacy; "1. Intrusion upon the plaintiff's seclusion, solitude, or into his private affairs, 2. Public disclosure of embarrassing private facts about the plaintiff, 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness."[58] With each tort designed to protect a different aspect of privacy, it is readily apparent that Prosser carefully crafted these torts to cover the more egregious intrusions of privacy and protect the privately innocent.[59] However, regardless of Prosser's genius and initiative, the lack of changes to privacy law in over forty years leaves the tort system unprepared to handle Google Maps Street View claims.[60]

III. STREET VIEW PHOTOGRAPHS AND PRIVACY

[15] The debate ensues regarding the privacy implications of images seen on Google Street View, with many scholars calling for vast tort reform to better keep up with evolving technology.[61] Most scholars

[55] *See id.* at 214-15.

[56] *Id.* at 214.

[57] *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977); *see also* William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960), *available at* http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf.

[58] Prosser, *supra* note 57, at 389.

[59] *See generally* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977).

[60] *See* Daniel Solove, *supra* note 44 ("The privacy torts are fossilized into the forms they were in circa 1960, and they haven't evolved to address modern privacy problems. Moreover, courts cling to antiquated notions of privacy . . . .").

[61] *Compare* Blackman, *supra* note 6, at 353-54, *and* Jamuna D. Kelley, Note, *A Computer with a View*, 74 BROOK. L. REV. 187, 229 (2008), *with* Jordan E. Segall, *Google Street*

rationalize the need for expansion of the privacy tort by pointing to a resultant chilling effect on behavior, the loss of control over personal information and pictures, and the lack of consent and threat to reputation.[62] However, others view these concerns as misplaced, arguing that the current privacy torts, namely intrusion upon seclusion,[63] are adequate to handle claims related to Google Street View.[64] This argument hinges on the fact that Google Maps takes pictures of things so highly public that there is no privacy right to begin with.[65] As this Comment will demonstrate, not only is this assumption inherently flawed, but the need for revamped privacy torts is crucial in order to give justice to the plaintiffs injured by the Street View images.

[16] The international scorecard of Google Maps Street View investigations reveals not only that Google violated national laws, but also a global feeling of unease over the photographs accessible on the Google Maps platform.[66] Whether or not nations can conclusively point to specific laws that prohibit Google from posting images online, it is clear the international community feels in some way violated by the process.[67] It is precisely this innate feeling of wrongdoing that fuels and rationalizes an improved tort system capable of punishing such indiscretions. After

View: Walking the Line of Privacy – Intrusion upon Seclusion and Publicity Given to Private Facts in the Digital Age, 10 U. PITTSBURGH J. TECH. L. & POL'Y 1, 27-30 (2010).

[62] *See* Segall, *supra* note 61, at 2.

[63] *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[64] Simply because claims fail under a tort does not mean the structure of the tort is inherently flawed; a failed cause of action might instead be in-actionable. *See* Segall, *supra* note 61, at 3. ("Calls for an expanded tort of privacy to encompass the Street View program are in error. Current doctrine surrounding the tort of invasion of privacy is wholly adequate to address the advent of Google Street View due to the highly public nature of the activity in which the individuals are implicated through the program.").

[65] *See* Helft, *supra* note 3 (quoting a Google spokesperson statement which claims Street View only used images taken from public property).

[66] *See Investigations of Google Street View*, *supra* note 18; McGee, *supra* note 36.

[67] *See, e.g.*, McGee, *supra* note 36.

all, this is what a system of justice should be based upon: instinctive notions of right and wrong. Although lawmakers all over the world struggle to identify exactly what laws Google violates when it posts images of persons and homes on its Internet mapping platform, the inherent justice in all resonates a need to fill the gap. It is exactly this back and forth, between knowing there was a crime committed and not having a legitimate crime to charge that plays out in the scorecard.

[17] Eight countries, as well as the European Union as a whole, have opened investigations relating to the Street View photography.[68] Of those nine investigations, two are ongoing (either pending or unfinished),[69] and six ended with Google either promising to blur images,[70] reduce photo storage,[71] provide advanced notice of Street View car itineraries,[72] re-shoot photography,[73] or suspend Street View photography temporarily,[74] and only one found Google *not* in violation of any privacy laws.[75] While the international community remains all over the map in its handling of Street View privacy cases for photographic images, the United States has also conducted its own informal investigation.[76] Certain localities and municipalities protested against the service on their own, and in fact, North Oaks, a private town in Minnesota, was successful in convincing Google to remove all photos from its mapping platform.[77] For security

[68] *See id.*

[69] *See id*. (listing Czech Republic and Switzerland).

[70] *See id*. (listing Canada and Germany).

[71] *See id*. (listing the European Union).

[72] *See* McGee, *supra* note 36 (listing Italy).

[73] *See id.* (listing Japan).

[74] *See id*. (listing Greece).

[75] *See id*. (listing United Kingdom).

[76] *See id*. (noting that an "FCC investigation remains open" concerning Street View privacy cases).

[77] *See* McGee, *supra* note 36.

reasons, the federal government ordered Google to take down all images of military bases, and similarly, National Network to End Domestic Violence petitioned Google to have all domestic violence shelters removed from the site as well.[78]

[18] Despite the lack of a privacy violation charges, or even a formal investigation from the U.S. government at all, Google still made sure to delete compromising or inappropriate images.[79] For instance, one blogger found a very revealing photograph of a woman entering her truck.[80] The picture was subsequently removed, with only the message, "[t]his image is no longer available" remaining, presumably after complaints were filed with Google.[81] Further, Google's own privacy policy acknowledges that individual faces and license plates warrant blurring to protect the privacy of those represented in the photographs.[82] It is situations like these, where Google faces no legal repercussions, yet still feels the need to delete images, that further underscore the need for more adept privacy torts.[83]

---

[78] *See* Elinor Mills, *Google's Street-level Maps Raising Privacy Concerns*, USA TODAY (June 4, 2007, 11:53 AM), http://www.usatoday.com/tech/news/internetprivacy/2007-06-01-google-maps-privacy_N.htm; Jonathan Richards, *Pentagon Bans Google from US bases*, THE SUNDAY TIMES (Mar. 7, 2008), http://technology.timesonline.co.uk/tol/news/tech_and_web/article3503624.ece.

[79] *See* Tamar Weinberg, *Google Maps: Invading Your Privacy? (Not Anymore!)*, SEARCH ENGINE ROUNDTABLE (June 8, 2007, 10:37 A.M.), http://www.seroundtable.com/archives/013780.html.

[80] *See id*.

[81] *Id*.

[82] *See Privacy*, *supra* note 30.

[83] *Cf. id.* ("Street View contains imagery that is no different from what you might see driving or walking down the street . . . . [but] if one of our images contains an identifiable face (for example that of a passer-by on the sidewalk) or an identifiable license plate, our technology will automatically blur it out . . . . If our detectors missed something, you can easily let us know.").

[19] A closer look into the elements of Prosser's privacy torts further reveals why the current system is incapable of providing an adequate medium for Street View claims.[84] The Borings raised the first two, intrusion upon seclusion and publicity given to private life, in their civil suit against Google, and hence these torts warrant the most consideration on their potential to provide relief.[85]

[20] In looking at the intrusion upon seclusion tort, plaintiffs must prove "'an intentional intrusion upon the seclusion of their private concerns which was substantial and *highly offensive to a reasonable person*, and aver sufficient facts to establish that the information disclosed would have caused mental suffering, shame or humiliation to a person of ordinary sensibilities.'"[86] The first hurdle created by this tort is that, in order for a claim to be actionable, it must consist of an intrusion that is "'highly offensive to a reasonable person.'"[87] This objective standard creates a multi-dimensional problem for Street View plaintiffs. While it is arguable that certain images posted on the mapping platform are highly offensive, such as the lewd photograph of the woman entering her car, it is more difficult to say the pictures of homes and cars, or people walking down the street rise to such a level. Furthermore, how should one react to the image of a woman entering an abortion clinic, or a man leaving an Alcoholics Anonymous meeting? It is hard to say whether these socially offensive images rise to the level of "highly offensive to a reasonable person."[88]

[21] Compounding the issue is Goggle's blurring policy.[89] Even when the image was taken with a high resolution zoom camera that can see over

[84] *See generally* RESTATEMENT (SECOND) OF TORTS §§ 652B-652E (1977).

[85] *See* Boring v. Google Inc., 362 F. App'x 273, 278, 280 (3rd Cir. 2010).

[86] *Id.* at 279 (emphasis added) (quoting Pro Golf Mfg., Inc. v. Tribune Review Newspaper Co., 809 A.2d 243, 247 (Pa. 2002)); *see also* RESTATEMENT (SECOND) TORTS § 652B (1977).

[87] *Boring*, 362 F. App'x at 279 (quoting *Pro Golf Mfg.*, 570 Pa at 809).

[88] *Id.*

[89] *See generally Privacy*, *supra* note 30.

fences and into homes, clearly more than what the public sees, Google's promise to blur faces and license plates raises questions of whether subsequent remedial measures nullify the harm and void claims.[90] Additionally, Google has the cognizable defense that Street View exposes no more than what is already in public view, which might lead courts to not even view the pictures as offensive, let alone *highly* offensive.[91] Clearly, not only is the intrusion upon seclusion tort an inept vehicle for Street View image claims, but pursuing this line of recourse could lead to conflicting court decisions and arbitrary line drawing.

[22] The second Prosser privacy tort, publicity given to private life, requires "'(1) publicity, given to (2) private facts, (3) which would be highly offensive to a reasonable person, and (4) is not of legitimate concern to the public.'"[92] Again, the "highly offensive" bar for recovery poses a problem with the Street View images, but it is not the only hurdle facing plaintiffs.[93] The fourth element, the "newsworthy exception," is broad, undefined, and overly dependent on current societal views.[94] The public might find freely accessible virtual maps of enough interest to fall under the exception, thereby preventing potential Google plaintiffs from

---

[90] *See id.*; *see also* Mills, *supra* note 78. Whether or not an image rises to the level of "highly offensive" when it is only public on the Internet for a short length of time has yet to be determined. *See Privacy*, *supra* note 30 ("Users can also request the removal of images that feature inappropriate content (for example: nudity or violence)."). In the same vein, it is equally uncertain whether deletion of an inappropriate photograph cures any privacy infringements. *See id.* However, using this tort in the Street View context encourages courts to engage in arbitrary line drawing, potentially looking at factors like how many people viewed the image, how long the image was posted, how many times the image was downloaded.

[91] *See, e.g.*, *Boring*, 362 F. App'x at 279.

[92] *Id.* at 280 (quoting Harris by Harris v. Easton Pub. Co., 483 A.2d 1377, 1384 (Pa. Super. Ct. 1984)).

[93] *Id*.

[94] *See* Blackman, *supra* note 6, at 321. By carving out all those facts that are "of legitimate concern to public," what constitutes a violation of publicity given to private life is largely determined by public opinion. *Boring*, 362 F. App'x at 280.

raising this tort. However, even if a plaintiff could bring their claim to the level of "highly offensive" and avoid the newsworthy exception, he or she would still face a problem with the rule for photographs.[95] For a plaintiff to recover on a photograph of his or her image, the image must reveal the plaintiff's identity.[96] Once again, blurring technology employed by Google makes it unlikely for images to meet this standard.[97]

[23] The final two privacy torts, "publicity placing person in false light"[98] and "appropriation of name or likeness,"[99] while not viewed as viable options by the Borings, still warrant brief consideration in light of their ability to provide recourse to Street View plaintiffs. False light, specifically, is equally as ineffective as the torts previously discussed in providing justice to potential plaintiffs. With false light, plaintiffs must show that the publicized information was highly offensive to a reasonable person, and that the defendant not only *knew* the information was untrue, but intentionally disregarded the truth.[100] In terms of photographic images, it is unlikely Street View plaintiffs could call a photograph posted on Google Maps "untrue."[101]

[24] The tort "appropriation of name or likeness," similarly fails all potential Street View plaintiffs in serving as a legitimate, actionable tort.[102] There are a number of reasons preventing a plaintiff from prevailing on an appropriation claim; the plaintiff must show that the

[95] *See* Kelley, *supra* note 61, at 209 (stating that recovery based on the disclosure of a photograph requires that "a plaintiff's identity must be revealed by the image . . . .").

[96] *Id.* (citing Clay Calvert & Justin Brown, *Video Voyeurism, Privacy, and the Internet: Exposing Peeping Toms in Cyberspace*, 18 CARDOZO ARTS & ENT. L.J. 469, 564 (2000)).

[97] *See Privacy*, *supra* note 30.

[98] RESTATEMENT (SECOND) OF TORTS § 652E (1977).

[99] *Id.* at § 652C.

[100] *See id.* at § 652E.

[101] *See id.*

[102] *See generally* RESTATEMENT (SECOND) OF TORTS § 652C (1977).

defendant used the plaintiff's identity for his or her own advantage, that there was a lack of prior consent, and that the plaintiff suffered an injury as a result.[103] However, the largest bar to recovery for Street View images is that an appropriation claim disallows claims originating with a public privacy invasion.[104] It is a general notion that photographs taken in public are public, and thereby do not qualify as an invasion of privacy.[105]

[25] In *Boring v. Google Inc*., the plaintiffs ran into the same problems addressed above in their attempt to sue Google for images posted on Street View.[106] The Borings noticed "Google had taken colored imagery of their residence, including the swimming pool, from a vehicle in their residence driveway months earlier without obtaining any privacy waiver or authorization."[107] Because the Borings' road was marked as a private drive with a "Private Road, No Trespassing" sign, they felt the images on Street View violated their right of privacy,[108] and consequently sued Google on claims of intrusion upon seclusion and publicity given to private life.[109] The court, in addressing both claims individually, concluded that neither claim succeeded because the alleged conduct did not rise to the level of highly offensive to a reasonable person.[110]

---

[103] *See id.*; *see also* Wendt v. Host Int'l, Inc., 125 F.3d 806, 811 (1997).

[104] *See* Prosser, *supra* note 57, at 391-92 ("On the public street, or in any other public place, the plaintiff has no right to be let alone, and it is no invasion of his privacy to do no more than follow him about.").

[105] *See id.* ("Neither is it such an invasion to take [a plaintiff's] photograph in such a place, since this amounts to nothing more than making a record, not differing essentially from a full written description, of a public sight which any one present would be free to see.").

[106] *See* Boring v. Google Inc., 362 F. App'x 273, 283 (2010).

[107] *Id*. at 276 (citation omitted) (internal quotation marks omitted).

[108] *Id.*

[109] *See id*. at 278-80.

[110] *See id.* at 279 ("No person of ordinary sensibilities would be shamed, humiliated, or have suffered mentally as a result of a vehicle entering into his or her ungated driveway and photographing the view from there.").

[26] Because none of the four Prosser privacy torts are able to address the concerns raised by Street View, and because the invasions are severe enough for Google to change its privacy policies,[111] the need for revamped privacy torts is apparent. While supporters of the mapping platform argue that the lack of successful claims simply means Street View has not violated any laws, scholars are quick to note that, under the current scheme, Google has no "legal incentive" to refrain from invading privacy.[112] As previously acknowledged, the pictures posted on Street View invoke an innate recognition of wrongdoing, and the only backstop in place is Google's own corporate ethics.[113]

[27] In coming to conclusion that the tort system needs reform,[114] one must first recognize not only that some Street View images are such blatant violations of privacy that legal remedies are necessary, but also that the current tort system is inept at providing such a remedy because of the disconnect between views of privacy in the 1960's, and views today.[115] Highlighting the problem with the current tort scheme is the number of issues that arise when applying Street View claims to the elements of the privacy torts.

[28] The first, and perhaps most important flaw with the current tort privacy scheme in addressing Street View claims is the underlying assumption inherent in all four torts: by going out in public, one

---

[111] *See* Andrea Frome, *Street View Revisits Manhattan*, GOOGLE LAT LONG BLOG (May 12, 2008, 6:00 PM), http://google-latlong.blogspot.com/2008/05/street-view-revisits-manhattan.html (introducing the new face blurring technology).

[112] *See* Blackman, *supra* note 6, at 353.

[113] *See* s*upra* Part III.

[114] *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev. 1887, 1891 (2010).

[115] *Compare* Prosser, *supra* note 57, at 389, *with* Richards & Solove, *supra* note 114 at 1922-24.

necessarily consents to the public gaze.[116] However, the technology employed by Google in creating the Street View maps, which notably involves high-resolution zoom and pan cameras, often goes beyond what is visible with the naked eye. [117] Justifying these invasive photographs as legal on the premise that public places carry no privacy rights creates a loophole that would allow any website to post private photos under the guise that they were taken from a public street. The resultant chilling effect whereby people would no longer feel comfortable driving to work, walking outside, sitting on their porches, etc., could lend way to a Big-Brother like world. It is much better to acknowledge that people go into public because they must as members of society, than to claim they consent to their picture being taken and posted online simply by walking out their front door. As the Supreme Court in *Katz v. United States* wisely noted, "[w]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[118]

[29] An additional problem with the torts, as seen in *Boring*, is that the highly offensive standard is inappropriate for Street View and similar claims.[119] Societal views are largely determinative as to what is and what is not reasonable, and in today's technologically connected world, posting pictures online is the norm.[120] Yet, social media sites should not be the

[116] *See* Kelley, *supra* note 61, at 213 (explaining that a plaintiff assumes risk, under a comparative fault analysis, whenever he or she voluntarily enters a public space and knows he or she can be seen). *See generally* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

[117] *See Cars, Trikes & More*, *supra* note 2 ("[T]he latest car has 15 lenses taking 360 degrees of photos. It also has motion sensors to track its position, a hard drive to store data, a small computer running the system, and lasers to capture 3D data to determine distances within the Street View imagery."); *see also* Helft, *supra* note 3 (explaining that Street View even captured images from inside the Brooklyn Battery Tunnel, an area which, due to its proximity to the site of the World Trade Centers, is clearly high security).

[118] Katz v. United States, 389 U.S. 347, 351 (1967).

[119] *C.f.* Boring v. Google Inc., 362 F. App'x 273, 278-80 (2010).

[120] *C.f.* Jonathan B. Mintz, *The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain*, 55 MD. L. REV. 425, 446 (1996) ("'[P]laintiffs' privacy rights rarely

reason Street View plaintiffs are precluded from successfully pleading their claims. The unrestricted access, lack of privacy settings and absence of prior consent for Street View photographs differentiates those injured by the images seen on Google Maps from those injured by pictures posted to some social media site.[121] Further, the issue remains as to whether Google's blurring policy completely bars images from rising to the level of highly offensive.[122]

[30] The final problem with the current scheme lies in damages, presuming that a Street View plaintiff successfully presented a cognizable claim before a court.[123] Damages in torts rely on the defendant owing a duty to the plaintiff, and in the case of Google, it is hard to imagine such an existing duty.[124] These three problems, taken together, amplify the need for some kind of change to the existing tort structure.

IV. STREET VIEW WI-FI SCANDAL AND PRIVACY

[31] Taking indecent, inappropriate, or even just embarrassing photographs of unknowing persons is not the full extent of the privacy controversy surrounding Google Maps. In a remarkably overt invasion of privacy, the Internet giant publically admitted in May of 2010 to inadvertently collecting private data over the course of three years with their special Street View cars.[125] However, the current tort laws provide

prevail over the public's interests, rendering the limitation on the scope of the public interest essentially theoretical and leaving plaintiffs with rare success.").

[121] *Compare Facebook's Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last updated Dec. 22, 2010) (describing measures Facebook users can take to ensure their own privacy), *with Privacy*, *supra* note 30.

[122] *See Privacy*, *supra* note 30.

[123] *See, e.g.*, Solove, *supra* note 44.

[124] *See Boring*, 362 F. App'x at 277 ("Google did not owe a duty to the Borings . . . .").

[125] *See WiFi Data Collection: An Update*, *supra* note 9.

impractical recourse for injured persons, and the only thing stopping Google from continued invasions is its own ethics.[126]

[32] Unlike the invasion of privacy claims relating to the photographs on Street View, the U.S. government has understandably taken a more active role in investigating the Google Wi-Fi scandal.[127] Here, Google has actually intercepted private data on private Wi-Fi access points, effectively eliminating the defense that the company impinged on nothing more than what was already public.[128] At the request and urging of the privacy protectionist group, Electronic Privacy Information Center ("EPIC"), two governmental agencies formally investigated the scandal – the FTC[129] and the FCC.[130] When the FTC closed its investigation, concluding that Google's deletion of the material and revised privacy procedures sufficiently remedied the situation,[131] the FCC decided to pick up the

---

[126] *See* David Kravets, *Packet-Sniffing Laws Murky as Open Wi-Fi Proliferates*, WIRED.COM (June 22, 2010, 6:04 PM), http://www.wired.com/threatlevel/2010/06/packet-sniffing-laws-murky/ [hereinafter Kravets, *Packet-Sniffing Laws*].

> 'We believe it does not violate U.S. law to collect payload data from networks that are configured to be openly accessible . . . (i.e., not secured by encryption and thus accessible by any user's device). We emphasize that being lawful and being the right thing to do are two different things, and that collecting payload data was a mistake for which we are profoundly sorry,' Google wrote Congress.

Id.

[127] *See* Kravets, *FCC Probing Google*, *supra* note 35.

[128] *See id.*

[129] *See* Letter from Marc Rotenberg, Exec. Dir., Elec. Privacy Info. Ctr., to Julius Genachowski, Chairman, Fed. Commc'ns Comm'n (May 18, 2010), *available at* http://epic.org/privacy/cloudcomputing/google/EPIC_StreetView_FCC_Letter_05_21_10.pdf (noting that two senior members of the House Commerce Committee urged the FTC "to undertake an investigation and to reply to certain questions by June 2, 2010.").

[130] *See* Kravets, *Packet-Sniffing* Laws, supra note 126.

[131] *See* Letter from John Verdi, Dir., EPIC Open Gov't Project, to Office of Gen. Counsel, Fed. Trade Comm'n (Feb. 11, 2011), *available at* http://epic.org/privacy/ftc/google/FTC_Streetview_FOIA_Appeal2.pdf (appealing administratively the FTC's

investigation.[132] Dissatisfied with the *post-hoc* rationale of the FTC, the FCC rationalized its investigation by stating, "'[a]s the agency charged with overseeing the public airwaves, we are committed to ensuring that the consumers affected by this breach of privacy receive a full and fair accounting.'"[133] The FCC investigation is currently ongoing.[134] Outside of the federal investigations, states have responded in their own ways.[135] Five state attorney generals have publically responded to the Wi-Fi intercepts, either via press releases, investigations, or subpoenas of information.[136]

[33] Similar to the Street View photograph privacy claims, members of the international community share the concerns of the United States.[137] In addition to the FCC and FTC investigations, seventeen countries and thirty-eight States have opened investigations of their own into the Wi-Fi scandal.[138] Australian, South Korean and Canadian governments all found Google in violation of their privacy laws, and the Communications minister of Australia went as far to label the breach the "single greatest breach in the history of privacy."[139] Eight of the countries have yet to

---

decision to close the investigation, believing that the FTC should have pursued the claim further).

[132] *See* Chloe Albanesius, *FCC Investigating Google Street View Wi-Fi Data Collection*, PCMAG.COM (Nov. 10, 2010), http://www.pcmag.com/article2/0,2817,2372498,00.asp.

[133] *Id.* (citation omitted).

[134] *Id.*

[135] *See, e.g.*, *Investigations of Google Street View*, *supra* note 18.

[136] *See id.* (referring to actions by Connecticut, Illinois, Michigan, Virginia, Missouri Attorney Generals).

[137] *See, e.g.*, McGee, *supra* note 36.

[138] *See id.*; *see also Investigations of Google Street View*, *supra* note 18.

[139] Josh Halliday, *Google Street View Broke Canada's Privacy Law with Wi-Fi Capture*, GUARDIAN.CO.UK (Oct. 20, 2010, 7.00 BST), http://www.guardian.co.uk/ technology/ 2010/oct/19/google-street-view-privacy-canada (citation omitted) (internal quotation marks omitted); *see* McGee, *supra* note 36.

resolve their investigations,[140] and four nations required Google to delete all collected data.[141]

[34] Privately, individuals and groups have sought remedies from Google's data intercept through a number of class actions.[142] Most recently, a panel granted Google's motion to consolidate eight private actions alleging violations of the federal Wiretap Act in the Northern District of California.[143] Claiming that "Google intentionally intercepted electronic communications sent or received over . . . open, non-secured wireless networks," the class members are hoping that the Wiretap Act's criminalization of electronic communication interception will successfully remedy the privacy breach.[144] However, the Wiretap Act is not the only potential statutory avenue to justice for those injured by Google's privacy gaffe.[145] The Communications Act, for instance, prohibits the receipt and transmission of "interstate or foreign communication by wire or radio."[146]

[35] Unfortunately for the class members in the pending litigation against Google, the statutory route in this particular context is less than satisfying. First, pursuing statutory claims over privacy tort claims does not provide the plaintiffs and class members with any tangible award or recoupment.[147] In the Wiretap Act language, for example, violations

[140] *See* McGee, *supra* note 36 (listing Austria, Czech Republic, Germany, Hungary, Italy, Sinagpore, Spain and South Korea).

[141] *Id.* (listing Austria, Canada, Denmark and Ireland).

[142] *See Investigations of Google Street View*, *supra* note 18.

[143] *See* Transfer Order, In Re: Google Inc. Street View Elec. Commc'ns Litig., 733 F. Supp. 2d 1381, 1382 (J.P.M.L. 2010).

[144] *Id.* The Wiretap Act explicitly makes illegal any intentional intercepts or procures of "any wire, oral, or electronic communication." Wiretap Act, 18 U.S.C. § 2511 (2006).

[145] *See Investigations of Google Street View*, *supra* note 18 (listing the Wiretap Act, the Communications Act, the Pen/Trap Act and 18 U.S.C. §1030 as federal statutes potentially relevant to the class actions against Google for intercepting Wi-Fi data).

[146] Communications Act, 47 U.S.C. § 605(a) (2006).

[147] *See, e.g.*, 18 U.S.C. § 2511(4).

result in fines.[148] Successful tort claims, on the other hand, can potentially produce nominal, compensatory, or punitive damages, which directly compensate plaintiffs for their injury.[149] Secondly, these communication statutes require that interceptions be intentional, an element unlikely true for Google.[150] Finally, the federal statutes cannot cover all the privacy issues surrounding Google Maps. For instance, the Wiretap Act could only conceivably protect e-mails collected by Google, because the "usernames and passwords, home addresses, phone numbers and more" are not necessarily "communication."[151] Further, the Street View images clearly do not fall under the purview of the federal communications statutes, which might create unnecessary, overlapping, costly and inefficient litigation.[152]

[36] Even though statutory solutions to the Google Wi-Fi breach are imperfect, the privacy torts once again are not without their own problems.[153] The largest factor preventing the torts from realistically serving Street View plaintiffs is that Google has not disseminated any of this information publically.[154] Even if they had, the claims would still be improbable for a number of reasons. In the cases of intrusion upon

---

[148] *See id.* Simply put, civil redress is more appropriate for Google plaintiffs.

[149] *See* RESTATEMENT (SECOND) TORTS §§ 903, 907, 908 (1977).

[150] *See, e.g.*, 18 U.S.C. § 2511(1)(a). As widely publicized, Google acknowledged that the Wi-Fi intercept was accidental. *See Wi-Fi data collection: An Update*, *supra* note 9; *see* Kang, *Growing Anger*, *supra* note 32 ("Google has said the data was collected by mistake, an error it blamed on an engineering glitch.").

[151] McGee, *supra* note 36; *see* 18 U.S.C. §2511(1)(a).

[152] *See generally* 18 U.S.C. § 2511. In no way can taking photographs be deemed the equivalent of intercepting "wire, oral, or electronic communication." *Id*.

[153] *See generally* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977).

[154] *See Wi-Fi data collection: An Update*, *supra* note 9 ("We want to delete this data as soon as possible, and are currently reaching out to regulators in the relevant countries about how to quickly dispose of it."); *see also* RESTATEMENT (SECOND) OF TORTS § 652D (1977) ("One who gives publicity to a matter concerning the private life . . . .").

plaintiff's seclusion and publicity given to private life, courts will likely find that the intercepted information was not sufficiently private because it existed on unsecured wireless networks, or was unencrypted data.[155] Technically, anyone could legally access the same information.[156] It is unlikely that a court would protect the privacy of someone who failed to take the available means necessary to ensure privacy. Further, the third tort, false light, is inapplicable because the "e-mail, browser and password data" collected in residential areas is inherently "true."[157] Finally, the appropriation tort would only work for potential plaintiffs if Google, for some reason, used the information collected commercially.[158] However, Google repeatedly made promises to delete all information.[159]

[37] Again, current privacy law is inept to handle such technologically advanced litigation. Although the trend internationally is to let Google off charge and fine free for confirmed deletion of any collected material, such a *post hoc* approach is inappropriate in the U.S.[160] While leniency should certainly be considered, it does not completely eradicate the breach committed. Doing so simply encourages wrongdoers to commit crimes

[155] *See* Kravets, *Packet-Sniffing Laws*, *supra* note 126 ("Google, in response to government inquiries and lawsuits, claims it is lawful to use packet-sniffing tools readily available on the internet to spy on and download payload data from others using the same open Wi-Fi access point. . . . It's not considered felony wiretapping 'to intercept or access an electronic communication made through an electronic communication system that is . . . readily accessible to the general public.'") (quoting Wiretap Act 18 U.S.C. § 2511); David Kravets, *Google Wi-Fi Spy Lawsuits Head to Silicon Valley*, WIRED.COM (Aug. 20, 2010, 2:16 P.M), http://www.Wired.com/threatlevel/ 2010/08/google-spy-lawsuits/ [hereinafter Kravets, *Google Wi-Fi Spy Lawsuits*] ("[Google] collect[ed] fragments of data from unencrypted wireless networks as its fleet of camera-equipped cars moseyed through neighborhoods snapping pictures for its Street View program.").

[156] *See* Kravets, *Packet-Sniffing Laws*, *supra* note 126.

[157] Boulton, *supra* note 38.

[158] Google, however, has repeatedly reaffirmed their promise to delete any intercepted information. *See Wi-Fi data collection: An Update*, *supra* note 9.

[159] *See id.*

[160] *See, e.g.*, McGee, *supra* note 36 (listing countries that have declined to delineate punishments for Google's privacy breach).

and subsequently claim they deleted the wrongfully obtained information. In the debates surrounding the Fourth Amendment Supreme Court cases, a delicate balancing between freedom and social organization and control is necessary, as is here.[161] The technology Google employed in the Street View cars was clearly not what the framers of the Constitution could have possibly imagined, and it is no longer easy to protect oneself against such privacy breaches.[162] It is not plausible to ask people to stay inside all day to avoid Street View cars and cameras, nor is it rational to expect people to protect themselves against Wi-Fi breaches similar to those Google committed. This Comment does not argue for a rewriting of the Constitution, but rather, for the revamping of privacy law to give credible and legitimate causes of actions to those who wish to pursue legal remedies for Google's over privacy infringement.

V. IN RE: GOOGLE AND GOING FORWARD

[38] The best solution to the existing problems is to create a new privacy tort. Instead of editing the existing torts, or pursing a combination of statutory and tort remedies, a new tort could provide effective and efficient protection of privacy the best. In reverting to the ideology of Warren and Brandeis, there are certain elements and principles that this new tort should encompass.[163]

A. Applicability to Google Maps

[39] The new tort should be able to protect current and potential plaintiffs both in actions against Google for photographs posted on Street View, and in actions for the Wi-Fi data collection. Currently, without any promising options, persons injured by Google's privacy breaches can only find recourse only in Google's own promises to either blur images on

[161] *Cf.* Katz v. United States, 389 U.S. 347, 359 (1967) (recognizing the right of citizens to be free from unreasonable intrusions into their private lives, concurrent with the right of the government to intrude that right upon appropriate justification).

[162] *See Cars, Trikes & More*, *supra* note 2.

[163] *See generally* Warren & Brandeis, *supra* note 50, at 193-97.

Street View or delete collected Wi-Fi data.[164] Admittedly, with two very different privacy breaches – one involving un-consented photographs published on a freely accessible website and the other involving intercepted personal data deleted upon discovery – the task of shaping a tort that covers plaintiffs in both situations is a tall order. However, expanding the idea of *informational privacy*[165] is perhaps the best approach in meeting this goal. If the new privacy tort could define private information as not only that which is stored on a computer, like passwords, e-mails, addresses, etc., but also that which can be evoked from a public photograph, then the two types of Google plaintiffs would be protected. To explain further, certain images posted on Street View convey private information about private persons – that the individual attends Alcoholics Anonymous meetings or that a child lives at a certain address[166] – and the new tort protecting informational privacy would cover these images.

B. Reasonable Expectation of Privacy

[40] While the new tort should cover Street View plaintiffs and Wi-Fi plaintiffs, it should not be so expansive as to provide recourse to every person who has shared information via the Internet or who has had a picture posted without his or her consent. In the world of Facebook, Twitter and MySpace, a sweeping privacy right online is not only impractical, but also unnecessary. Members of the Facebook community knowingly consent to "tagging" of images and posting of information,[167] and as such, this tort should not cover these situations.

---

[164] *See* Andrea Frome, *supra* note 111 (introducing the new face blurring technology); *Wi-Fi data collection: An Update*, *supra* note 9 (promising to delete all the collected information after meeting with "regulators" in "relevant countries"); *see also* Kang, *supra* note 32.

[165] *See* Richards & Solove, *supra* note 114, at 1919. The authors take care to discuss other scholars' suggestions for new privacy torts, and even highlight Jullie Cohen's informational privacy idea as a potential solution "to . . . the collection, use, and dissemination of personal information in computer databases." *Id.*

[166] *See Galleries*, *supra* note 20.

[167] *See Facebook's Privacy Policy, supra* note 121.

[41] Hence, a check on this new tort is necessary to ensure it is not overly encompassing. Borrowing from the line of criminal cases involving the Fourth Amendment protections against warrantless eavesdropping and nonconsensual interceptions of communications,[168] whether a plaintiff had a reasonable expectation of privacy allows the new privacy tort to protect non-Facebook plaintiffs.[169] As Warren and Brandeis aptly said, protection should be afforded "upon the ground of [a] . . . breach of an implied contract or of trust or confidence."[170] Thus, there is a reasonable expectation of privacy in the information stored on personal and private Wi-Fi networks, just as there is a reasonable expectation of privacy in keeping images of your front porch offline.

C. Harm

[42] One of the main tenets of the Warren and Brandeis article centered on the idea of "legal *injuria.*"[171] The duo ensured that harm expands beyond notions of physical harm to encompass mental harm as well.[172] In keeping with this notion, the new tort that protects informational privacy should only guard against invasions that legitimately cause some degree of "mental suffering," or, harm.[173]

---

[168] *See generally* Oliver v. United States, 466 U.S. 170, 171 (1984); Katz v. United States, 389 U.S. 347 (1967).

[169] Blackman also used "reasonable expectation of privacy" as an element of his suggested tort, "the right to your digital identity." Blackman, *supra* note 6, at 354. This suggestion was in response to "Omniveillance" and the invasiveness of Street View images. *See id.* at 314-15.

[170] Warren & Brandeis, supra note 50, at 207.

[171] *Id.* at 213("If the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation.").

[172] *See id.* at 197 ("Injury of feelings may indeed be taken account of in ascertaining the amount of damages when attending what is recognized as a legal injury . . . .").

[173] *Id.* at 213; *see also* Richards & Solove, *supra* note 114, at 1922 (arguing generally that tort law should be updated to include a "more sophisticated conception of harm.").

D. Societal Perceptions of Public and Private

[43] Warren and Brandeis reference the fact that society is largely determinative of what constitutes justice, "intolerable abuse," and essentially, privacy.[174] However, as Neil Richards and Daniel Solove note, the identifiable point at which something is private or public is no longer so clear, but rather, a graduated continuum.[175] With the ubiquity of the Internet and social media, this "more nuanced" approach is much more appropriate for determinations of public and private.[176] If anything, the debate surround the privacy of Street View highlights the need for a graduated continuum from private to public.[177] Therefore, this new tort should allow for flexibility and defer to public perceptions of public and private in order to protect things not traditionally private.

E. Defenses

[44] The creation of any new tort necessitates consideration of possible defenses. In keeping with the idea of deferring to Warren and Brandeis ideology, a number of the points they raised are relevant in this context.[178] First, consent to publication of an image or to dissemination of personal data over a Wi-Fi connection should override any claim to privacy.[179] Secondly, accuracy and truth of the information intercepted or the picture uploaded does not justify a breach.[180] Finally, intent on behalf of the

[174] Warren & Brandeis, supra note 50, at 210.

[175] Richards & Solove, *supra* note 114, at 1922 ("[T]he law must abandon the binary all-or nothing approach toward privacy in favor of a more modern and nuanced understanding of the gradations between purely public and purely private.").

[176] *Id.*

[177] *Compare* Blackman, *supra* note 6, at 353-54, *and* Kelley, *supra* note 61, at 207-08, *with* Segall, *supra* note 61, at 27-30.

[178] *See* Warren & Brandeis, *supra* note 50, at 218.

[179] *See id.*

[180] *See id.*

person committing the breach, or in this case, Google, is not a required element, and thus the lack of such is not a defense.[181]

V. CONCLUSION

[45] Google Maps Street View made the news not only for its contribution to technology and the Internet, but also for its breaches of privacy. The U.S. and other nations have questioned Google's policies, but have been largely unable to pinpoint legitimate crimes or breaches.[182] Unfortunately, plaintiffs injured by either Street View pictures or the Google Map Wi-Fi data collection are left without any plausible remedy.[183] Current privacy torts and statutory schemes are not fit to address such technologically tied privacy issues. However, in the words of privacy pioneers Warren and Brandeis, "[p]olitical, social, and economic changes entail the recognition of new rights, and the common law . . . grows to meet the demands of society."[184] Thus, today's technological society demands that the antiquated privacy torts to be updated by adding a new tort more adept at addressing emerging privacy issues.

[181] S*ee id.*

[182] *See generally Investigations of Google Street View*, *supra* note 18.

[183] *See, e.g.*, Boring v. Google, Inc., 362 F. App'x 273, 283 (3d Cir. 2010) (denying plaintiffs' claims of breach of privacy against Google).

[184] Warren & Brandeis, *supra* note 50, at 193.