

3-2012

## Note – Private Eyes Watching You: Google Street View and the Right to an Inviolable Personality

Roger C. Geissler

Follow this and additional works at: [https://repository.uchastings.edu/hastings\\_law\\_journal](https://repository.uchastings.edu/hastings_law_journal)



Part of the [Law Commons](#)

---

### Recommended Citation

Roger C. Geissler, *Note – Private Eyes Watching You: Google Street View and the Right to an Inviolable Personality*, 63 HASTINGS L.J. 897 (2012).

Available at: [https://repository.uchastings.edu/hastings\\_law\\_journal/vol63/iss3/6](https://repository.uchastings.edu/hastings_law_journal/vol63/iss3/6)

This Note is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings Law Journal by an authorized editor of UC Hastings Scholarship Repository.

# Private Eyes Watching You: Google Street View and the Right to an Inviolable Personality

ROGER C. GEISLER\*

*Google's rollout of its Street View service in North America in 2007 provoked little concern about the privacy implications of private homes and individuals being easily viewed by potentially millions of persons. In contrast, Street View's reception in Europe, particularly in Germany, has been marked by episodes of both public outrage and government concern. These divergent reactions can be explained in part by differing conceptions of the right to privacy—with European concepts of privacy based generally on the notion that an individual's "dignity" should be protected—and the differing levels of protection afforded by those conceptions to aspects of a person's identity.*

*This Note compares the legal protections afforded to individuals' privacy in the U.S. and in Germany. In particular, this Note looks at the concept of the right to an "inviolable personality" that pervades privacy protection in Germany. This Note argues that such a right can be found in U.S. privacy jurisprudence, and that this right protects persons against the actions of private as well as government agents. Lastly, this Note argues that privacy rights must be defined broadly in an era when Street View is expanding to cover not just public streets and alleys, but also the interiors of museums and even places of business.*

---

\* J.D. Candidate, University of California, Hastings College of the Law, 2012. I would like to thank Professor Ashutosh Bhagwat for invaluable discussions that helped me formulate my initial interest in this topic. I would also like to give thanks to Kathleen for her incredible support and patience during long stretches while I was researching and writing this Note, and to Liam and Declan for reminding me to also take time to play.

## TABLE OF CONTENTS

INTRODUCTION.....	898
I. PRIVATE EYES: STREET VIEW'S INTIMATE IMAGERY .....	901
II. PRIVACY AND GOOGLE STREET VIEW IN THE U.S. ....	904
A. LITIGATION AGAINST STREET VIEW.....	904
B. DEFINITIONS OF PRIVACY: RESPONSES TO TECHNOLOGICAL ADVANCES.....	908
C. U.S. CONSTITUTIONAL BASES FOR A RIGHT TO PRIVACY .....	911
D. PROPOSALS FOR A "PRIVACY BILL OF RIGHTS" .....	914
III. GERMAN PRIVACY RIGHTS: PROTECTION FOR THE INVOLATE PERSONALITY .....	917
IV. AN INTERNATIONAL APPROACH TO PROTECTING PRIVACY RIGHTS.....	922
CONCLUSION .....	925

## INTRODUCTION

The 2006 German film *Das Leben der Anderen* [*The Lives of Others*] portrays the dehumanizing effects of an all-pervasive state security apparatus on a citizenry that knows no privacy.<sup>1</sup> It tells the story of an East German playwright, Georg Dreyman, who becomes subject to intense surveillance by the detested Stasi, or secret police, when he is suspected of turning against the regime. After placing microphones and training cameras in and around his apartment to monitor his movements, Stasi agents recorded the minutia of Dreyman's most mundane activities in painfully detailed dossiers that remained classified until after the German Democratic Republic vanished in 1990. This depiction of a totalitarian government spying on its citizens resonated widely with the German public: after fifteen months in German theaters, over two million people had seen the film,<sup>2</sup> which grossed over nineteen million euros.<sup>3</sup> In April 2007 it won in seven categories, including best film, of the *Deutscher Filmpreis*, Germany's equivalent of the Oscar.<sup>4</sup>

The specter of the Stasi haunted Europe again in 2010. Only this time, the menace was not German police-spies but legions of nondescript vehicles with roof-mounted cameras deployed to photograph ordinary

---

1. DAS LEBEN DER ANDEREN (Buena Vista Pictures 2006).

2. *Data Base on Admissions of Films Released in Europe*, LUMIERE, [http://lumiere.obs.coe.int/web/film\\_info/?id=26055](http://lumiere.obs.coe.int/web/film_info/?id=26055) (last visited Feb. 14, 2012).

3. *Box Office/Business for The Lives of Others*, INTERNET MOVIE DATABASE, <http://www.imdb.com/title/tt0405094/business> (last visited Feb. 14, 2012).

4. *Preisträger 2006*, DEUTSCHER FILMPREIS, <http://www.deutscher-filmpreis.de/archiv/2005-2010/2006/deutscher-filmpreis-2006/preistraeger-2006.html> (last visited Feb. 14, 2012).

avenues and alleys. And unlike the snooping of the Cold War era, these cameras were not in the service of a proletarian dictatorship, but a Silicon Valley corporation recently valued at \$192 billion.<sup>5</sup> Google's Street View service is a feature of Google Maps and displays a 360-degree street-level panorama of a given point on a map, including whatever and whomever happened to be caught on camera at the instant the photos were taken. In Europe, the presence of the Google Street View cameras was met with a degree of resistance that was almost entirely absent when it was first introduced in the U.S. in May 2007. In the United Kingdom, residents of a Buckinghamshire village formed a human chain to keep one of Google's cars from taking pictures of their homes.<sup>6</sup> In Greece and the Czech Republic, the Hellenic Data Protection Authority and the Office for Personal Data Protection, respectively, forbid Google from taking any further images while they investigate possible privacy violations.<sup>7</sup>

But nowhere has resistance to Street View been as widespread as in Germany in the months leading up to the nationwide launch of the service on November 18, 2010. State and federal politicians accused Google of flouting privacy laws. One member of the Hamburg city government temporarily brought Street View to a halt worldwide.<sup>8</sup> The president of a national association of homeowners called for a law requiring Google to obtain permission from each owner of every private house visible on Street View.<sup>9</sup> An editorial in a national newspaper stated that the "Stasi would be green with envy" if it possessed the data about people that Google does, and proclaimed that "the surveillance state was yesterday, today it's Street View."<sup>10</sup>

Street View has aroused far less opposition in Google's native U.S., although concern has been mounting. The first voices of opposition came

5. Reuven Brenner, *Putting a Value on Google and Facebook*, FORBES BLOG (Feb. 3, 2011, 3:13 PM), <http://blogs.forbes.com/leapfrogging/2011/02/03/putting-a-value-on-google-and-facebook/>.

6. Robert Hardman, *A Very English Revolt Sees Off Google's Spies*, DAILY MAIL (U.K.) (last updated Apr. 6, 2009, 8:06 AM), <http://www.dailymail.co.uk/debate/article-1167211/ROBERT-HARDMAN-A-English-revolt-sees-Googles-spies.html>.

7. *Google Street View Blacked Out in Greece*, CNN WORLD (May 13, 2009), [http://articles.cnn.com/2009-05-13/world/greece.google.street.view.blocked\\_1\\_google-earth-search-giant-google-maps?\\_s=PM:WORLD](http://articles.cnn.com/2009-05-13/world/greece.google.street.view.blocked_1_google-earth-search-giant-google-maps?_s=PM:WORLD); Ian Willoughby, *Google Street View Cameras Infringe on Privacy, Says Czech Data Protection Agency*, ČESKÝ ROZHLAS (Sept. 22, 2010), <http://www.radio.cz/en/section/curraffrs/google-street-view-cameras-infringe-on-privacy-says-czech-data-protection-agency>.

8. Matthias Popien & Ulf B. Christen, *Caspar Brems Google aus—und Zwar Weltweit*, HAMBURGER ABENDBLATT (Ger.), May 27, 2010, at S12.

9. Lucas Wiegelmann, *Hauseigentümer Fordern Gesetze Gegen Google*, DIE WELT (Ger.) (Feb. 8, 2010), <http://www.welt.de/wirtschaft/webwelt/article6306988/Hauseigentuemmer-fordern-Gesetze-gegen-Google.html>.

10. Berthold Kohler, Editorial, "Street View" Statt "Schnüffelstaat," FRANKFURTER ALLGEMEINE ZEITUNG (Ger.) (Aug. 10, 2010), <http://www.faz.net/s/Rub7FC5BF30C45B402F96E964EF8CE790E1/Doc~E864171A474794449D1C4DF8CABD4A3E~ATpl~Ecommon~Spezial.html>.

less than a week after Street View was launched, when the *New York Times* interviewed the resident of an apartment building in Oakland, California, who expressed dismay that her cat was clearly visible through her living room window on Street View.<sup>11</sup> The issue, she explained, is that the line separating “public photos” from “peeping” has gotten blurrier with Street View.<sup>12</sup> More recently, a Pennsylvania couple brought suit against Google for invasion of privacy, and a class-action suit is currently pending in the District Court for the Northern District of California.<sup>13</sup>

This Note considers the privacy issues that Street View has raised in the U.S. in the broader context of the reactions in other countries, specifically Germany. It also considers the recent revelations that Google has used its fleet of Street View vehicles to collect personal data about private citizens. This Note will recommend that the data-protection legislation proposed by Senators Kerry and McCain should include stringent privacy safeguards to reflect the common law and constitutional assurances of an “inviolable personality.” This Note proposes that the data-collection aspect of Street View cannot be considered in isolation from its image-gathering and image-distribution aspects.

This Note is divided into four parts. Part I demonstrates how Street View’s technology has compromised privacy since its introduction in 2007. Part II discusses the right to privacy in the U.S. as it has been applied to Street View thus far. It begins by looking at litigation in the U.S. against Street View. It then examines the ways in which the definition of privacy has expanded to meet the novel situations that technological innovations have brought about since the late nineteenth century, and argues that a competing concept of privacy rights, expressed as the right to control information about oneself, is too limited. It then looks at the bases under the U.S. Constitution for a right to privacy and argues that a right to an “inviolable personality,” or the “right to be let alone,” is one of the fundamental rights implicit in that document. Next, it considers the calls in the Senate and by the Department of Commerce for a “Privacy Bill of Rights.” Part III compares American privacy concepts with the more vigorous privacy protections afforded to residents of Germany and analyzes recent litigation in Germany against Street View. Part IV proposes that U.S. lawmakers consider broader international trends in privacy protection because the traditional concept of a “privacy tort” is too limited to adequately redress the harm that can arise from the use of rapidly changing technology. It proposes technological solutions that nongovernmental entities such as Google can

---

11. 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?\\_r=1](http://www.nytimes.com/2007/06/01/technology/01private.html?_r=1).

12. *Id.*

13. See discussion *infra* Part II.A.

implement to reduce their exposure to expensive litigation and to respect American and European norms of privacy.

### I. PRIVATE EYES: STREET VIEW'S INTIMATE IMAGERY

It would not be a stretch to say that Street View's cameras have caught some people in situations in which they might have preferred not to be photographed. In one of the more notorious early images available on Street View, one man in San Francisco was seen scaling the gates of an apartment building.<sup>14</sup> Speculation as to his intent ranged from a burglary in progress to a resident trying to enter his own apartment after losing his keys.<sup>15</sup> Many more instances of unambiguously legal behavior have been recorded by Google's cameras and made available to millions of Internet users. Another infamous image in Street View's first days was of two women sunbathing on Stanford University's campus.<sup>16</sup> Debate on a Stanford blog captured both sides of the privacy implications of such an image being taken and made widely available: One student commented that if the women truly were concerned about their privacy, they would not sunbathe in swimsuits in a park where any number of passersby might see them,<sup>17</sup> while the blog's author and another commenter opined that the students "probably wouldn't be too happy that anyone with an Internet connection could see" them.<sup>18</sup> Because anyone with an Internet connection could view this image so easily, "the photo [was] being viewed in the tens of thousands of times each and every day often with not so innocent intent."<sup>19</sup>

While these two photos have since been removed from Street View, many others have been posted. A quick Internet search shows many websites dedicated to collecting images that might be embarrassing to those captured by Street View. Media throughout the world also have featured such photos. One mother in Northern England told the *Manchester Evening News* that she "just felt sick to [her] stomach" when saw a picture on Street View of her three-year-old son playing naked in his grandmother's yard on a hot day: "I'm angry, disgusted and upset about it," she said.<sup>20</sup> One man in Finland was seen in his backyard,

---

14. S. James Snyder, *Google Maps: An Invasion of Privacy?*, TIME MAG. (June 12, 2007), [http://www.time.com/time/photogallery/0,29307,1630926\\_1379845,00.html](http://www.time.com/time/photogallery/0,29307,1630926_1379845,00.html).

15. *Id.*

16. Joshua Glenn, *Sunbathers and Jaywalkers, Where RU?*, BOS. GLOBE BRAINIAC BLOG (June 1, 2007, 9:04 AM), [http://www.boston.com/news/globe/ideas/brainiac/2007/06/sunbathers\\_and.html](http://www.boston.com/news/globe/ideas/brainiac/2007/06/sunbathers_and.html).

17. Christian, *Google Street View Attacks Stanford Students' Privacy?*, UNOFFICIAL STAN. BLOG (June 1, 2007, 1:25 PM), [http://tusb.stanford.edu/2007/06/google\\_street\\_view\\_attacks\\_stu.html](http://tusb.stanford.edu/2007/06/google_street_view_attacks_stu.html).

18. *Id.*

19. W., *Google Street View Attacks Stanford Students' Privacy?*, UNOFFICIAL STAN. BLOG (Aug. 28, 2008, 3:45 PM), [http://tusb.stanford.edu/2007/06/google\\_street\\_view\\_attacks\\_stu.html](http://tusb.stanford.edu/2007/06/google_street_view_attacks_stu.html).

20. Alice McKeegan, *Mum's Outrage over Picture of Naked Son on Google Street View*, MANCHESTER EVENING NEWS (June 29, 2010), <http://menmedia.co.uk/manchestereveningnews/news/s/>

behind a fence shielding his property from the street, with his genitals exposed and his faced unblurred.<sup>21</sup>

The foregoing examples illustrate that the manner in which Google collects its images for Street View compromises privacy in a way that ordinary people, even those who publish images on the Internet, cannot. The Stanford image shows how a psychological barrier that might ordinarily prevent someone from taking a photograph of sunbathers is utterly absent in Street View. While it is undeniable that the students in swimsuits were plainly visible in a public place, any person who might have tried to photograph them from the sidewalk while standing still and not seated in a car would have run the risk of being discovered by the camera's subjects or a passerby who could have objected. Instead, Google collects images automatically from a camera mounted on a car; the vehicle is not stationary, but instead moves along with the flow of traffic. The image of the Stanford sunbathers could have been taken at a speed of up to twenty-five miles per hour,<sup>22</sup> which would not have alerted them to the fact that they were being photographed, even if the camera was visible to them. The fact that the images are taken mechanically means that there is zero possibility that the picture-taker can exercise discretion to refrain from taking a photo at an inappropriate moment. Certainly there is no chance that the risk of social opprobrium would act as a restraint on the photographer of two students enjoying the sun with their backs turned toward the photographer.

The problematic Street View images from Europe demonstrate another difference between Google and a casual observer on the street. The cameras are mounted on Google's vehicles at a height of approximately 2.7 meters, or nearly nine feet.<sup>23</sup> This vantage point allows Google to peer over fences to photograph, for example, a child playing in a yard or a man sunning himself behind his house—neither of which would be visible to an ordinary person walking down the street. Furthermore, Street View allows users to zoom in on images, enlarging them to many times the size at which they are initially shown on Google Maps. This permits users to view people clearly despite the distance that otherwise would render the photographed subject indistinct to a casual viewer—as if each image were taken with a telephoto lens. This feature exemplifies the great distinction that exists between what is visible with Street View and what is visible to an ordinary observer. It shows why the

---

1279455\_mums\_outrage\_over\_picture\_of\_naked\_son\_on\_google\_street\_view?rss=yes.

21. Lester Haines, *Street View Catches Finn with His Pants Down*, REGISTER (U.K.) (Feb. 11, 2010), [http://www.theregister.co.uk/2010/02/11/street\\_view\\_finland/](http://www.theregister.co.uk/2010/02/11/street_view_finland/).

22. STANFORD UNIV. PARKING & TRANSP. SERVS., CONDITIONS AND REGULATIONS FOR DRIVING, OPERATING, STOPPING, STANDING AND PARKING OF MOTOR VEHICLES ON STANFORD UNIVERSITY GROUNDS § SU-13 (2005).

23. See Willoughby, *supra* note 7.

service cannot be considered to be capturing what any ordinary person can see—all the more so because Google is constantly improving the resolution of its images to replace older, fuzzier ones showing less detail.<sup>24</sup> Along with newer higher-resolution images, Google has recently added tricycles to its fleet of camera-equipped vehicles, which according to one Silicon Valley newspaper “will increasingly allow Google to extend Street View beyond the public streets onto private property.”<sup>25</sup> While that article hastens to add that Street View might extend to private property “if an owner [so] requests,”<sup>26</sup> the facts in *Boring v. Google*, discussed in Part II.A, demonstrate that a clear signal that a particular property is private does not necessarily deter Google from capturing images on that property.<sup>27</sup> Even if Google’s tricycles were to stay entirely on public property, its cameras (which capture images from seven feet off the ground) likely will go to less-trafficked places where residents have a heightened expectation of privacy.<sup>28</sup>

Google claims that Street View shows what is visible when “driving or walking down the street.”<sup>29</sup> And in late 2009, Google CEO Eric Schmidt explained that when it comes to Google’s ability to retain information, “[i]f you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”<sup>30</sup> While this might be true of clearly illicit behavior, it is a facile characterization of privacy concerns. Any unobjectionable activity can take on an unintended appearance once divorced from its context of time and place, especially once it is visible not just to those in proximity to the activity, but to Google Maps users worldwide.<sup>31</sup> Moreover, few people stand nine feet tall, and none has 360-degree vision. The fact that most Street View imagery is created in a way that exceeds normal human capability thus militates against the argument that no privacy concern is raised because anything shown on Street View is what anybody else can see. Street View

---

24. See LadyBugz, *Street View High Resolution vs. Lower Resolution*, GOOGLE EARTH FORUM (Feb. 3, 2010), <http://www.google.com/support/forum/p/earth/thread?tid=134bf23cf2c866f4&hl=en>.

25. *Google Street View Now Goes Places Cars Can't*, PALO ALTO BLOG (Mar. 1, 2011), <http://paloaltocal.com/google-street-view-now-goes-places-cars-cant>.

26. *Id.*

27. See *infra* note 40 and accompanying text.

28. Steve Mostyn, *Google Improves Street View with Off-Road Tricycle Cameras*, TECH HERALD (Mar. 11, 2011, 3:43 PM), <http://www.thetechherald.com/article.php/201109/6884/Google-improves-Street-View-with-off-road-tricycle-cameras>.

29. See *Privacy*, GOOGLE MAPS, <http://maps.google.com/help/maps/streetview/privacy.html> (last visited Feb. 14, 2012).

30. Richard Esguerra, *Google CEO Eric Schmidt Dismisses the Importance of Privacy*, ELECTRONIC FRONTIER FOUND. (Dec. 10, 2009, 5:05 PM), <http://www EFF.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy>.

31. Dan Costa, *Mayer Maps Out Google's Coming Location Dominance at SXSW*, PC MAG. (Mar. 13, 2011, 1:15 PM), <http://www.pcmag.com/article2/0,2817,2381880,00.asp> (stating that forty percent of Google Maps users, or 150 million people, access the service using mobile devices).

allows viewers to see far more than they possibly could otherwise in the ordinary course of a day.

The possibilities for innocent activities to be misconstrued once visible on Street View—bringing distress not only to the persons photographed but also to others having dealings with them—were illustrated in a complaint that Privacy International lodged with the British government.<sup>32</sup> Some two hundred Britons contacted the group about problems that Street View had brought them. Among them was a “married man . . . speaking at close proximity with a female colleague. Because of nearby noisy road works he was forced to speak into her ear, but the image created the appearance of intimacy. This image created a tense argument between the married couple.”<sup>33</sup> More disturbingly, a woman who moved from house to house for several years to hide from a violent ex-partner complained “that she felt extreme distress when Street View identified her outside her new home.”<sup>34</sup>

These examples show that it is no solution merely to refrain from any activity we would not want anyone else to know about. It simply is not possible to predict which one of our many activities might be misconstrued when an image removes that action from its context or when it might reveal sensitive information. Nor is it possible to rely on Google’s face-blurring technology, which at the initial stage is done automatically rather than by Google personnel, to conceal our identities.<sup>35</sup> Not only does this technology fail to blur faces over ten percent of the time<sup>36</sup> (even as it overzealously pixelated Colonel Sanders’ face at every KFC outlet in Britain),<sup>37</sup> faces are just one of a person’s many identifiers. Even if technology can successfully blur someone’s face, their hair, body, and clothes remain distinctly visible and may reveal their identity to others.

## II. PRIVACY AND GOOGLE STREET VIEW IN THE U.S.

### A. LITIGATION AGAINST STREET VIEW

Legal action in the U.S. against Street View has come exclusively from private parties filing suit seeking a remedy for alleged harm that Google caused. To date there have been very few complaints filed

---

32. *PI Files Complaint About Google Street View*, PRIVACY INT’L (Mar. 23, 2009), <https://www.privacyinternational.org/article/pi-files-complaint-about-google-street-view>.

33. *Id.*

34. *Id.*

35. ANDREA FROME ET AL., *LARGE-SCALE PRIVACY PROTECTION IN GOOGLE STREET VIEW* 3–7 (2009).

36. *Id.*

37. *Google Street View Blurs Face of Colonel Sanders at Every KFC*, TELEGRAPH (London) (May 20, 2009, 3:17 PM), <http://www.telegraph.co.uk/technology/google/5356031/Google-Street-View-blurs-face-of-Colonel-Sanders-at-every-KFC.html>.

against Street View. In the 2008 case *Boring v. Google, Inc.*, a couple living in a suburb of Pittsburgh, Pennsylvania, sued Google for, inter alia, invasion of privacy.<sup>38</sup> The Borings alleged that the inclusion of “‘colored imagery’ of their residence, outbuildings, and swimming pool” on Street View—photographed “from a vehicle in their residence driveway” located on a road that is “unpaved and clearly marked with ‘Private Road’ and ‘No Trespassing’ signs,” “significantly disregarded [their] privacy interests.”<sup>39</sup> Regarding the claim for intrusion upon seclusion, the district court stated that “[l]iability attaches only when the intrusion is substantial and would be *highly offensive* to ‘the ordinary reasonable person.’”<sup>40</sup> While the court found it “easy to imagine that many whose property appears on [Street View] resent the privacy implications” of such public display, only “the most exquisitely sensitive . . . would suffer shame or humiliation” from it.<sup>41</sup> Mere inclusion of one’s home, even one that is relatively secluded, did not, in the court’s view, establish that the plaintiffs’ “alleged pain” and “suffering” at Google’s actions rose to the level of being “highly offensive.”<sup>42</sup> Accordingly, the district court granted Google’s motion to dismiss.<sup>43</sup>

The Third Circuit upheld the dismissal, noting that “[p]ublication is not an element” of intrusion upon seclusion and that a court “must examine the harm caused by the intrusion itself,” which in this case the court found to be “arguably less intrusive” than if someone had knocked on their front door.<sup>44</sup> The court found it significant that the Borings were not “themselves . . . viewed inside their home,” which is a “relevant factor” in intrusion on seclusion claims.<sup>45</sup> The only one of the Borings’ claims that the Third Circuit found had merit was their trespassing claim.<sup>46</sup> In late 2010, Google settled with the Borings, paying them one dollar in compensation on that claim.<sup>47</sup>

---

38. 598 F. Supp. 2d 695, 698 (W.D. Pa. 2009). The court clarified that the Borings’ “action for invasion of privacy embraces four analytically distinct torts: (1) intrusion upon seclusion; (2) publicity given to private life; (3) appropriation of name or likeness; and (4) publicity placing a person in a false light.” *Id.* at 699. The tort intrusion upon seclusion “is established where a plaintiff is able to show: (1) physical intrusion into a place where he has secluded himself; (2) use of the defendant’s senses to oversee or overhear the plaintiff’s private affairs; or (3) some other form of investigation into or examination of the plaintiff’s private concerns.” *Id.* (quoting *Borse v. Piece Goods Shop, Inc.*, 963 F.2d 611, 621 (3d Cir. 1992)).

39. *Id.* at 699.

40. *Id.* (emphasis added) (quoting *Harris by Harris v. Easton Publ’g Co.*, 483 A.2d 1377, 1383–84 (Pa. Super. Ct. 1984)).

41. *Id.* at 700.

42. *Id.*

43. *Id.* at 698.

44. *Boring v. Google, Inc.*, 362 F. App’x 273, 279 (3d Cir. 2010).

45. *Id.*

46. *Id.* at 283.

47. Chris Davies, *Google Pays \$1 Compensation in Street View Privacy Case*, SLASHGEAR.COM (Dec. 3, 2010), <http://www.slashgear.com/google-pays-1-compensation-in-street-view-privacy-case-03117450/>.

Currently pending in the District Court for the Northern District of California is another suit, *In re Google Street View Electronic Communications Litigation*, a class-action complaint involving allegations of invasions of privacy far beyond Google's gathering and dissemination of images of private property.<sup>48</sup> In May 2010, Google acknowledged that, while the company was creating images with its camera-fitted cars, it had "mistakenly collect[ed] samples of payload data from . . . non-password-protected . . . WiFi networks" of private individuals.<sup>49</sup> In October 2010 Google conceded that "entire emails and URLs were captured, as well as passwords."<sup>50</sup> The plaintiffs claim that Google's actions violated the Wiretap Act, which prohibits the "[i]nterception and disclosure of wire, oral, or electronic communications,"<sup>51</sup> thus criminally invading the plaintiffs' "reasonable expectations of privacy."<sup>52</sup>

Technology has progressed in ways lawmakers could not have contemplated when they enacted the privacy laws the plaintiffs relied upon in these two cases. Congress passed the law at issue in *In re Google* in 1968;<sup>53</sup> the Borings alleged that Google violated the Pennsylvania common law tort of intrusion upon seclusion in accordance with section 652B of the Restatement (Second) of Torts, written in 1977.<sup>54</sup> Neither Congress nor the drafters of the Restatement (and common law courts before them) could have anticipated a world in which images of places and people could be retrieved almost instantaneously with a few clicks of a mouse.<sup>55</sup> By limiting the definition of *privacy* to the sense of *seclusion* which can only be disturbed by someone being viewed *in real time* by a person in close proximity to the person in seclusion, the Restatement becomes too rigid to accommodate the technological innovations since its drafting, especially those innovations of the last half-decade. Similarly, the emphasis in the Wiretap Act on protecting the integrity of electronic communications might not extend to now-common household realities, such as private WiFi signals, which broadcast information about their respective computer networks but which might not be considered

---

48. 794 F. Supp. 2d 1067 (N.D. Cal 2011).

49. See *WiFi Data Collection: An Update*, OFFICIAL GOOGLE BLOG (May 14, 2010, 1:44 PM), <http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>.

50. See *Creating Stronger Privacy Controls Inside Google*, OFFICIAL GOOGLE BLOG (Nov. 22, 2010, 12:00 PM), <http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html>.

51. 18 U.S.C. § 2511 (2010).

52. *In re Google Street View*, 794 F. Supp. 2d at 1082.

53. See 18 U.S.C. § 2511.

54. Complaint, *supra* note 52, at 3 (referring to RESTATEMENT (SECOND) OF TORTS § 652B (1977)). See generally *Pacitti v. Durr*, 310 F. App'x 526 (3d Cir. 2009).

55. To give some idea of the state of technology at the time, computers manufactured in 1968 had only alphanumeric displays and largely performed sophisticated mathematic calculations. A typical example of a state of the art computer at that time is the Hewlett-Packard 9100, which cost \$4,900 (the equivalent of over \$31,000 in 2011) and which was used almost exclusively for business applications. For a brief description of the 9100, see [http://www.hpmuseum.net/display\\_item.php?hw=50](http://www.hpmuseum.net/display_item.php?hw=50).

“communication” in the sense that such information has no intended recipient as initially contemplated by the Act.<sup>56</sup>

The fact that the publication of images of one’s property or person is not an element of a claim of intrusion upon seclusion indicates that common law concepts of privacy are inadequate to grapple with the reality that images can now be reproduced ad infinitum anywhere in the world. Moreover, limiting the legal field to a tort of privacy for the dissemination of personal images leaves open the possibility that only those who possess a requisite knowledge of the latest technology would know if they have been injured by such images. For example, Google could capture an image of a person of “ordinary sensibility” who is completely unfamiliar with technology and does not know about Street View. Yet this person might find herself in a situation that causes her mental suffering after someone else (such as her employer) sees the image and acts upon it in some way, all without her ever knowing about this image of her. Under the common law, an invasion of privacy claim requires at a minimum that a plaintiff knows that the defendant viewed her in a protected environment.<sup>57</sup>

The common law tort of invasion of privacy is ineffective to protect against an injury resulting from the wide dissemination of an image, because that tort is concerned only with the moment at which an individual is initially viewed.<sup>58</sup> But with technologies like Street View, the moment of being viewed necessarily occurs prior to—sometimes years before—the dissemination of that image, without which the harm does not occur. Criminal law also is inadequate to counter such an injury. For example, the plaintiffs in *In re Google* allege that Google violated a federal criminal statute that protects against deliberately intercepting electronic communications. Apart from the issue of whether the plaintiffs’ broadcast of non-password-protected data over WiFi constitutes “communication,” a difficulty arises in determining whether Google collected such data with the requisite knowledge of illegality.<sup>59</sup>

---

56. In passing the Wiretap Act, Congress was concerned largely with preventing and punishing eavesdropping, whereby an oral communication from one party to another party is intercepted by a third party. See Omnibus Crime Control and Safe Streets Act of 1968, § 801(a), Pub. L. No. 90-351, 82 Stat. 197, 211 (codified as amended at 18 U.S.C. § 2510 (2010)) (“There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation. Electronic, mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications.”); see also *Heggy v. Heggy*, 944 F.2d 1537, 1540 (10th Cir. 1991) (“[T]he legislative history of [the Wiretap Act] evinces a congressional awareness of the widespread use of electronic eavesdropping in domestic relations cases . . .”).

57. *Boring v. Google, Inc.*, 362 F. App’x 273, 279 (3d Cir. 2010).

58. *Id.*

59. See *Fernicola v. Specific Real Prop. in Possession*, No. 00-CIV-5173(MBM), 2001 WL 1658257, at \*7 (S.D.N.Y. Dec. 26, 2001).

The debate surrounding Street View in Europe might provide a way for courts and legislatures in the U.S. to safeguard against harms that potentially invasive technologies such as Street View might cause. This should be done without shifting the burden exclusively to private citizens to protect their privacy, as under tort law. Such protection also should avoid the potentially devastating costs on businesses that federal criminal statutes would impose.

#### B. DEFINITIONS OF PRIVACY: RESPONSES TO TECHNOLOGICAL ADVANCES

Because there are a number of different concepts that can be subsumed under the broad term “privacy,” it is first necessary to determine which of these definitions is relevant to an analysis of Street View. An early attempt to define privacy in the context of the mechanical reproduction and dissemination of images of one’s person appeared in 1890, in *The Right to Privacy* by Samuel Warren and Louis Brandeis.<sup>60</sup> There, Warren and Brandeis argued that the advent of new technologies, which can create “instantaneous photographs,” permits the “unauthorized circulation of portraits of private persons” by newspapers, requiring legal recognition of “the right to be let alone.”<sup>61</sup> This right to be let alone was an extension of the common law right of the individual to determine “to what extent his thoughts, sentiments, and emotions [were to] be communicated to others.”<sup>62</sup>

Another, more recent definition of privacy emerged in the context of the dissemination of data about one’s person. Richard Posner formulated this definition and noted that the word “privacy” can mean “the withholding or concealment of information.”<sup>63</sup> This, he argued, was one of three possible meanings then in current use.<sup>64</sup> Under Posner’s understanding of privacy, a “right to be let alone” does not mean much, because “[v]ery few people want to be let alone.”<sup>65</sup> Indeed, the right to privacy—which Posner described as “the right to control the flow of information about” a person<sup>66</sup>—has a downside in allowing people “to manipulate the world around them by selective disclosure of facts about

---

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

61. *Id.* at 195.

62. *Id.* at 198.

63. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393 (1978) [hereinafter Posner, *The Right of Privacy*]. The other two definitions Posner advanced could be understood either as the equivalent of “peace and quiet,” that is, the state that is disturbed when an unwanted telephone solicitation “invades” one’s privacy, or as a synonym for “freedom and autonomy,” the meaning the Supreme Court used in identifying a right to abortion as subsumed under a right to privacy. Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 216; see also *Roe v. Wade*, 410 U.S. 113 (1973); *Griswold v. Connecticut*, 381 U.S. 479 (1965).

64. Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 405 (1981).

65. Posner, *The Right of Privacy*, *supra* note 63, at 400.

66. *Id.* at 395.

themselves.”<sup>67</sup> Information about others is not a final goal, but is instead used as an instrument in the production of income.<sup>68</sup> While individuals should be assigned a property right in personal information, this right is a byproduct of “socially productive activity.”<sup>69</sup> The property right to privacy should not extend to situations where there is “an element of misrepresentation”<sup>70</sup> in information one presents about oneself, because such information has utilitarian value to others who have dealings with that individual. Limiting the property right to privacy thus would reduce transaction costs while also increasing efficiency.<sup>71</sup>

Posner criticizes Warren and Brandeis’s argument for a “right to be let alone” for being narrowly focused and little more than a “right not to be talked about in a newspaper gossip column.”<sup>72</sup> While Warren and Brandeis did indeed deplore the increase of information available in the press as a result of technological advances,<sup>73</sup> Posner disagrees that such media portrayals are little more than a result of “idle curiosity.”<sup>74</sup> Rather, he argues, “gossip columns” have a genuine utility: On the one hand, they offer to ordinary persons information about “wealthy and successful people” so that the former may model their own career and other decisions on those portrayed in the media. On the other hand, gossip columns also offer cautionary tales about “the pitfalls of success” so that the readers presumably might avoid a similar fate.<sup>75</sup> Posner claims that “[p]eople are not given to random, undifferentiated curiosity.”<sup>76</sup> Since there is no risk of people randomly snooping into others’ affairs for no purpose, a privacy concern does not exist.<sup>77</sup>

Posner’s analysis regarding the utilitarian function of gossip media may be less compelling now than when it was written in 1978. In 2011, it is difficult to state, as Posner did, that “[g]ossip columns . . . are genuinely informational.”<sup>78</sup> However, *Us* magazine was founded just one year, and *People* magazine four years, prior to the publication of Posner’s article. Thirty-three years later, his position may be harder to defend, as a result

---

67. *Id.* at 400.

68. *Id.* at 394.

69. *Id.* at 403.

70. *Id.* at 414.

71. *Id.* at 397–99.

72. *Id.* at 406–07.

73. See Warren and Brandeis, *supra* note 60, at 195–96.

74. Posner, *The Right of Privacy*, *supra* note 63, at 396.

75. *Id.* This “patterning” function of gossip media explains why such media focus almost exclusively on the wealthy rather than on the poor: because the latter by nature provide less useful information for patterning our own lives. Whatever poor people are portrayed in gossip columns, according to Posner, were once wealthy but became poor, thus such portrayals have a “cautionary function” for an “ordinary person.” *Id.*

76. *Id.*

77. *Id.*

78. *Id.*

of advances in technology that were practically undreamed of in the 1970s. Today's gossip media constantly demands ever-new information that might be of uncertain utility in "open[ing] people's eyes to [new] opportunities."<sup>79</sup>

Just as advances in communications have undermined Posner's claim of the ability of "gossip columns" to empower readers to make well-informed life choices, so has such technology weakened his argument that people do not engage in "random, undifferentiated curiosity."<sup>80</sup> If this were still the case, then it is difficult to explain how the website Chatroulette, which allows users to connect via webcam with other, completely random users, could generate 3.9 million users just four months after it launched.<sup>81</sup> It is precisely the "random" quality of the glimpses into others' lives that thrills so many Chatroulette "voyeurs."<sup>82</sup> This phenomenon makes Posner's blanket denial of undifferentiated interest in information about strangers difficult to support.

However, there are several arguments why interactions like those on Chatroulette do not constitute an invasion of privacy. First, both parties agree to each encounter by logging into the website and clicking a button to be connected with another user on the network. Second, there is a mutual exchange of images: every user that views another in an intimate setting simultaneously and willingly broadcasts to that other user a real-time image of herself as well; nobody is viewed unwillingly. Lastly, there is almost complete anonymity on the website: nobody knows the identity of the other party unless that party chooses to reveal it, although users' faces are generally plainly viewable to others (but not always).<sup>83</sup>

While indeed it does not make sense to agree to an invasion of privacy, it cannot be the case, as Posner asserts, that random, undifferentiated curiosity of others does not exist. It seems very likely that users would be even more inclined to peep at others via webcam if they did not have to reveal anything about themselves first. It might not even matter to the user that the person viewed did not consent to, or was even aware of, the fact that others were viewing an image of her. Otherwise, there would have been no audience for a live streaming video secretly taken by a Rutgers freshman of his roommate in an intimate

---

79. *Id.*

80. *Id.*

81. Erick Schonfeld, *Chatroulette Quadruples to 4 Million Visitors in February*, TECHCRUNCH.COM (Mar. 29, 2010), <http://techcrunch.com/2010/03/29/chatroulette-4-million-visitors>.

82. Bobbie Johnson, *Online Voyeurs Flock to the Random Thrills of Chatroulette*, GUARDIAN (U.K.) (Feb. 13, 2010), <http://www.guardian.co.uk/technology/2010/feb/14/chatroulette-sex-voyeurs-website>.

83. Nick Bilton, *The Surreal World of Chatroulette*, N.Y. TIMES (Feb. 20, 2010), <http://www.nytimes.com/2010/02/21/weekinreview/21bilton.html>.

encounter with another man.<sup>84</sup> There, viewers were invited to participate via an announcement on the freshman's Twitter account, thereby eliminating any anonymity that might have lessened the harm of the filming and broadcasting.<sup>85</sup>

### C. U.S. CONSTITUTIONAL BASES FOR A RIGHT TO PRIVACY

A right to privacy is not mentioned in the U.S. Constitution.<sup>86</sup> Rather, a right to privacy may be inferred from the fact that the Constitution limits government action in such a way that “guarantee[s] that the individual, his personality, and those things stamped with his personality” are free from “official interference.”<sup>87</sup> The U.S. Supreme Court did not address the issue of constitutional guarantees to privacy until 1886, when it held in *Boyd v. United States* that “the very essence of constitutional liberty” lies in an “indefeasible right of personal security, personal liberty and private property.”<sup>88</sup> In *Boyd*, the Court held that a violation of the Fourth Amendment resulted when the government attempted to compel petitioners to produce certain documents in connection with an investigation into possible customs fraud.<sup>89</sup> The Court's earliest jurisprudence on privacy was based on the inviolability of private property. Because the documents the government sought were the respondents' “goods and chattels,” and thus their “dearest property,” to compel their production to find evidence of wrongdoing violated the Fourth Amendment's prohibition on unreasonable searches and seizures.<sup>90</sup> This right in private property was construed very liberally. In *Boyd*, the government sought the production of petitioners' private papers by court order.<sup>91</sup> Yet that order was held to be unconstitutionally “unreasonable search or seizure” even though petitioners and government agents did not have to produce the documents.<sup>92</sup>

Later, the Court stated in *Gouled v. United States* that the Fourth Amendment was to be given a “liberal construction.”<sup>93</sup> But despite the technological advances that have given the government unprecedented

---

84. Lisa W. Foderaro, *Private Moment Made Public, Then a Fatal Jump*, N.Y. TIMES, Sept. 30, 2010, at A1.

85. *Id.*

86. William M. Beaney, *The Constitutional Right to Privacy in the Supreme Court*, 1962 SUP. CT. REV. 212, 214.

87. *Id.*

88. 116 U.S. 616, 630 (1886).

89. *Id.* at 638.

90. *Id.* at 627–28 (quoting *Entick v. Carrington*, (1765) 95 Eng. Rep. 807); *see also* *Adams v. New York*, 192 U.S. 585, 598 (1904) (“The security intended to be guaranteed by the Fourth Amendment against wrongful search and seizures is designed to prevent violations of private security in person and property and unlawful invasion of the sanctity of the home of the citizen.”).

91. *Boyd*, 116 U.S. at 618.

92. *Id.* at 639.

93. 255 U.S. 298, 304 (1921).

access into the private lives of its citizens, the Court has continued to hold fast to a reading of the Fourth Amendment that was rooted in a right to be secure in one's tangible property. In *Olmstead v. United States*, for example, the Court declared that *Gouled's* liberal construction could not mean that the Fourth Amendment extends beyond citizens' "houses, persons, papers, and effects."<sup>94</sup> Accordingly, the Court in *Olmstead* deemed wiretapped conversations obtained by the government without a warrant to be admissible because the conversations were recorded "without trespass upon any property of the defendants."<sup>95</sup>

In his dissent in *Olmstead*, Justice Brandeis echoed the themes of invasion of privacy resulting from technological advances. Stating that the majority opinion read the language of the Fourth Amendment too narrowly, Justice Brandeis claimed that "[t]he makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness."<sup>96</sup> Instead of merely securing for citizens a right in "material things," the Framers "sought to protect Americans in . . . their thoughts, their emotions and their sensations."<sup>97</sup> In essence, the Framers "conferred . . . the right to be let alone," which is "the most comprehensive of rights and the right most valued by civilized [persons]."<sup>98</sup> As a result, Brandeis stated, the Fourth Amendment prohibits "every unjustifiable intrusion by the Government upon the *privacy* of the individual, *whatever* the means employed."<sup>99</sup>

By the time *Boyd* and *Olmstead* were overruled in 1967 by *Warden v. Hayden*,<sup>100</sup> the Court's privacy jurisprudence had already strayed far from the common law property right that formed the basis of the *Boyd* decision. Justice Brennan stated in *Hayden* that the Court had "recognized that the principal object of the Fourth Amendment [was] the protection of *privacy* rather than *property*."<sup>101</sup> The Court concluded that because the Fourth Amendment protects only against unreasonable "searches and seizures," no generalized right to privacy can be found in that provision alone—even if *Boyd* and *Gouled* can be read to imply such a broad right.<sup>102</sup> Indeed, that same year the Court stated in *Katz v. United*

---

94. 277 U.S. 438, 465 (1928), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967).

95. *Id.* at 457; *see* *Goldman v. United States*, 316 U.S. 129, 134 (1942) (finding no Fourth Amendment violation despite government agents' entry onto the defendants' property to install a "detectaphone" to listen in on phone conversations, and finding likewise that the use of the "detectaphone" in an office adjoining that of the defendants was not unconstitutional), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967).

96. 277 U.S. at 478.

97. *Id.*

98. *Id.*

99. *Id.* (emphasis added).

100. 387 U.S. 294 (1967).

101. *Id.* at 304 (emphasis added).

102. Beane, *supra* note 86, at 250.

States that the “Fourth Amendment cannot be translated into a general constitutional ‘right to privacy.’”<sup>103</sup>

By the 1960s, the Constitution was read to include much more privacy protection than just that of “material things.”<sup>104</sup> In what might be the most expansive enumeration of privacy rights the Court had ever announced, Justice Douglas’ opinion in *Griswold v. Connecticut* stated that “specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees,” which “create zones of privacy.”<sup>105</sup> The right to marital privacy secured by *Griswold* was “created by several fundamental constitutional guarantees,” even if was not mentioned explicitly in the Constitution,<sup>106</sup> similar to the way the right of association (also not mentioned in the Constitution) is guaranteed by the First Amendment.<sup>107</sup> *Griswold* and the cases it cites are but a few examples of the Court’s movement away from a privacy right wedded to a common law property right and toward a more comprehensive right. As Warren and Brandeis expressed in 1890 and as Justice Douglas wrote over half a century later, there is a right “to be let alone” that “draws substance from several provisions of the Constitution, including the First, the Fourth, and the Fifth Amendments.”<sup>108</sup>

The Court has read an increasingly expansive right to privacy in the Constitution, and it is difficult to imagine a turn of phrase as vague and therefore as potentially all-encompassing as “emanations, formed from penumbras.” However, the likelihood of the Court finding a general right to privacy in the Constitution that would restrict the actions of private entities is remote, even if such a right exists in other democratic constitutions such as Germany’s.<sup>109</sup> This is not to say that such a privacy right does not exist, even if it is not explicit in the Constitution. Justice Douglas described the “right to [be] let alone,” which he claimed protects “the privacy of the home and the dignity of the individual,” by protecting not only against intrusions by government agents such as “lawless police” but also against private individuals such as Peeping Toms.<sup>110</sup> Under this rationale, while a Peeping Tom would not be committing a constitutional violation per se, he unquestionably would encroach on a person’s rights, and courts unquestionably would have the power to punish him for violating a law rooted in the right to be let alone.

---

103. *Katz v. United States*, 389 U.S. 347, 350 (1967).

104. *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965).

105. *Id.*

106. *Id.* at 485.

107. *Id.* at 483 (quoting *NAACP v. Alabama*, 357 U.S. 449, 462 (1958)).

108. WILLIAM O. DOUGLAS, *THE RIGHT OF THE PEOPLE* 57–58 (1958).

109. *See infra* Part III.

110. *Id.* at 57–58, 95.

#### D. PROPOSALS FOR A “PRIVACY BILL OF RIGHTS”

The notion that a quasi-constitutional right to privacy or right to be let alone could restrict the actions of private, nongovernmental entities also has appeared in recent proposals in both the legislative and executive branches. Recently, constitutional language has been used to frame proposed legislation to respond to the fact that “modern technology allows *private entities* to observe the activities and actions of Americans on a scale previously unimaginable.”<sup>111</sup> In December 2010, the U.S. Department of Commerce released a report offering recommendations for protecting consumers’ online privacy by “keep[ing] pace with changes in technology, online services and Internet usage.”<sup>112</sup> The key recommendation in that report was the need for “the broad adoption of comprehensive Fair Information Practice Principles (“FIPPs”),”<sup>113</sup> which were likened to a “Privacy Bill of Rights” for online consumers.<sup>114</sup> The FIPPs would promote “informed consent” by consumers, as well as “transparency through simple notices, clearly articulated purposes for data collection, commitments to limit data uses to fulfill these purposes, and expanded use of robust audit systems to bolster accountability.”<sup>115</sup>

The Department of Commerce noted, however, that the proposed FIPPs do not involve a “full right to control” information about oneself. Rather, the framework “articulates rights and obligations in personal information, such as a right to access and correct information about oneself and an obligation to use personal information only for specified purposes.”<sup>116</sup> In advocating for stronger informed-consent provisions, the Department of Commerce invoked a concept of privacy closer to that which Posner uses—the right to control information about oneself<sup>117</sup>—rather than Warren and Brandeis’s definition of privacy as the right of the individual to determine “to what extent his thoughts, sentiments, and emotions shall be communicated to others.”<sup>118</sup> This sense of privacy, restricted to the control of personal information that is ultimately analyzed and put to “economic use” by a third party, is as limited and

---

111. *Kerry Urges Common Sense Commercial Privacy Protections*, JOHN KERRY (Mar. 16, 2011) <http://kerry.senate.gov/press/release/?id=d18a9191-7fa3-437c-af24-3b6ca3a28f10> (emphasis added).

112. *Commerce Department Unveils Policy Framework for Protecting Consumer Privacy Online While Supporting Innovation*, U.S. DEP’T COM. (Dec. 16, 2010), <http://www.commerce.gov/news/press-releases/2010/12/16/commerce-department-unveils-policy-framework-protecting-consumer-priv>.

113. LAWRENCE E. STRICKLING ET AL., *Introduction* to U.S. DEP’T OF COMMERCE, *COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK* vii (2010); *id.* at 23–29.

114. JOHN KERRY, *supra* note 111.

115. *See* U.S. DEP’T OF COMMERCE, *supra* note 113, at 4.

116. *Id.* at 10 n.17.

117. *See* Posner, *The Right of Privacy*, *supra* note 63, at 395.

118. *See* Warren & Brandeis, *supra* note 60, at 198.

unsatisfactory as Posner's analysis.<sup>119</sup> The Department of Commerce fails to consider that such information can have no economic value in itself. Yet the ability of such information to adversely impact a person if communicated is real.<sup>120</sup> A right to privacy cannot be limited to the purely economic sphere. Here, it is worth repeating Justice Douglas' words that a right to privacy also protects individuals from Peeping Toms.<sup>121</sup> Whatever the "benefits" that voyeurs derive from their voyeurism, presumably they are not economic in nature.

Calls for a "Privacy Bill of Rights" increased beginning in March 2011. At a hearing of the Senate Committee on Commerce, the White House showed support for such a "Bill of Rights" when Lawrence Strickling, the Administrator of the National Telecommunications and Information Administration, stated that "[t]he administration is now at the point of recommending that this be dealt with in legislation," abandoning its earlier stance that data companies and advertisers should adopt voluntary codes of conduct.<sup>122</sup> At the same time, Senators John Kerry and John McCain announced their cooperation to create an online "privacy bill of rights" that "should respect the consumers' ability to control the use of their personal information."<sup>123</sup>

The wording of such proposed legislation remains to be seen. If the Department of Commerce's report serves as a guide, however, the approach likely will be one that seeks to empower consumers to have some measure of control over any personal information that might have economic potential. In doing so, the proposed legislation likely would be too narrowly focused on the transmission of data to a limited number of parties, such as advertisers, while ignoring the activities of Internet companies like Google that make personal information widely available to the broader public. Yet the recognition of a privacy right to information about oneself must also be read to include images of oneself. An image is data about a person: driver licenses, passports, employee security badges, and gym membership cards all use photographs to identify their owners because photographs corroborate other data about the person. Google acknowledges as much by blurring faces of people shown by Street View just like they do license plates, though it began to do only after Street View had been available for almost a year, and only in response to public complaints.<sup>124</sup>

---

119. See *supra* Part II.B.

120. See U.S. DEP'T OF COMMERCE, *supra* note 113, at 16.

121. See DOUGLAS, *supra* note 108, at 95.

122. Diane Bartz, *Obama Administration Seeks Internet Privacy Bill*, REUTERS (Mar. 16, 2011, 4:32 PM), <http://www.reuters.com/article/2011/03/16/us-privacy-obama-idUSTRE72F83U20110316> (quoting Lawrence Strickling, Nat'l Telecomm. & Info. Admin.).

123. Jennifer Valentino-Devries, *Privacy Measure Draws Support*, WALL ST. J. (Mar. 17, 2011), <http://online.wsj.com/article/SB10001424052748703899704576204932250006752.html>.

124. See Stephen Shankland, *Google Begins Blurring Faces on Street View*, CNET NEWS (May 13,

We have already seen how Warren and Brandeis argued that the “latest advances in photographic art have rendered it possible to take pictures surreptitiously,” so that doctrines of contract or privity could not be applied to invasions of privacy occasioned by “the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds.”<sup>125</sup> Accordingly, the fact that individuals whose images are disseminated by Street View cannot consent to their images being so used requires that privacy protection of a person’s image be more forceful than protection of other types of personal data. Internet users presumably set up accounts on Facebook and Gmail voluntarily and agree, at least perfunctorily, to the terms of service, which may permit the collection of personal data.<sup>126</sup> Those whose identities are revealed on Street View, however inadvertently, have no such opportunity. The Department of Commerce recommendation that consumers be able to “access” and “correct” personal data presumes that the consumers are aware or informed that such information exists.<sup>127</sup> As the Privacy International report shows, “consumers” might not even know that Street View has collected and made available data about them until their identities have been compromised and the harm has been done.<sup>128</sup>

It was against the invasive potential of “surreptitious” photography that Warren and Brandeis advocated for a privacy right to protect the dissemination of one’s image. The principle that protected against the involuntary dissemination of one’s image, and indeed that had protected a right to privacy at common law, was the “right to an inviolate personality.”<sup>129</sup> Another way to understand the concept of “inviolable personality” is “human dignity and individuality”<sup>130</sup> or an “individual’s independence . . . and integrity.”<sup>131</sup> The right to an inviolate personality permits “the individual to do what he will.”<sup>132</sup>

The right to an inviolate personality is the “common thread of principle” that “runs through [privacy] tort cases, the criminal cases involving the rule of exclusion under the Fourth Amendment, criminal statutes prohibiting Peeping Toms, wiretapping, eavesdropping, the possession of wiretapping and eavesdropping equipment, and criminal

---

2008, 10:01 AM), [http://news.cnet.com/8301-10784\\_3-9943140-7.html](http://news.cnet.com/8301-10784_3-9943140-7.html).

125. Warren & Brandeis, *supra* note 60, at 211, 206.

126. See *Google Terms of Service*, GOOGLE, <http://www.google.com/policies/terms/> (last visited Feb. 14, 2012); *Statement of Rights and Responsibilities*, FACEBOOK, <https://www.facebook.com/legal/terms?ref=pf> (last visited Feb. 14, 2012).

127. See U.S. DEP’T OF COMMERCE, *supra* note 113, at 10 n.17.

128. See *supra* notes 32–34 and accompanying text.

129. Warren & Brandeis, *supra* note 60, at 211.

130. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971, 991 (1964).

131. *Id.* at 971.

132. *Id.* at 1003.

statutes or administrative regulations prohibiting the disclosure of confidential information obtained by government agencies.”<sup>133</sup> While an “affront to dignity” can be “affected by physical interference with the person,” it can also be “affected, among other means, by using techniques of publicity to make a public spectacle of an otherwise private life.”<sup>134</sup> To be subject to “public scrutiny” is to be “deprived of [one’s] individuality and human dignity.”<sup>135</sup>

It remains to be seen if any proposed “Privacy Bill of Rights” would include protections of a person’s right to dignity and would afford protections to individuals to such an extent that it would not be left up to each individual to police her own identity and image and assume the burdens of bringing a tort claim against an alleged infringer. Other democratic nations have been more vigorous and active in protecting their citizens. France, for example, just days after the still-nebulous “Privacy Bill of Rights” was floated before the Senate Commerce Committee, fined Google 100,000 euros for improperly collecting personal data from WiFi networks using its Street View cars.<sup>136</sup> Because Congressional and judicial action is still largely *terra incognita* with regard to services like Street View, it is instructive to look to foreign nations to see how they have enforced privacy protections, how they have approached the issue of privacy violations occasioned by Street View, and whether their approaches are applicable in the U.S. context. A look at the debate surrounding Street View in Germany is particularly illuminating because the debate there has been more vigorous than perhaps anywhere else, and because it is a nation with a large portion of Internet users—some seventy percent of the population.<sup>137</sup>

### III. GERMAN PRIVACY RIGHTS: PROTECTION FOR THE INVIOULATE PERSONALITY

As demonstrated, the U.S. Constitution affords protection to an individual’s “invioilate personality,” even if such a right is not expressed explicitly and must be inferred from provisions that were not part of the original document. By contrast, the foundations of the German right to privacy are found at the very beginning of the text of the German constitution, or *Grundgesetz* (“Basic Law”).<sup>138</sup> Article 2, section 1 of the

---

133. *Id.* at 1000–01.

134. *Id.* at 1003.

135. *Id.*

136. Greg Keller, *France Fines Google over Street View Privacy Breach*, SALON.COM (Mar. 21, 2011, 2:19 PM), [http://www.salon.com/2011/03/21/france\\_privacy\\_google\\_fined](http://www.salon.com/2011/03/21/france_privacy_google_fined).

137. *See Internet Usage in Germany Increases to Almost 70 Percent*, YOUNG GERMANY (July 1, 2009), <http://www.young-germany.de/nc/news-verwaltung/news-singleview/article/internet-usage-in-germany-increases-to-almost-70-percent.html?mobile=1&cHash=df398d653f3f3288b193ca12af6ca2e1>.

138. Rosalind English, *Protection of Privacy and Freedom of Speech in Germany*, in DEVELOPING KEY PRIVACY RIGHTS 77, 78–82 (Madeleine Colvin ed., 2000).

*Grundgesetz* states, “Everyone has the right to the free development of his personality,”<sup>139</sup> while Article 1, section 1 protects “[t]he dignity of the human being.”<sup>140</sup> German courts have interpreted these two sentences in case law to imply a right to privacy that not only encompasses an affirmative government obligation to protect this right, but one that also constrains private parties’ interactions with other private parties.<sup>141</sup> The prominent placement of guarantees of human dignity and liberty was a conscious choice of the drafters of the *Grundgesetz* during the constitutional convention of 1948, who sought to correct the flaws of Germany’s previous constitution. The drafters considered that document—in force from the founding of the Weimar Republic in 1919 until the defeat of the Third Reich in 1945—partly responsible for giving the Nazis the ability to seize power.<sup>142</sup>

The “right to the free development of one’s personality” clause in Article 1 treats the right to privacy (*Privatsphäre*) as an integral part of a person’s general personality right (*allegemeines Persönlichkeitsrecht*).<sup>143</sup> From a German perspective, it is not possible to distinguish “privacy” from “personality.”<sup>144</sup> Other aspects of the general personality right are the individual sphere (*Individualsphäre*), which protects the personality and the freedom of self-determination, and the intimate sphere (*Intimsphäre*), which includes a person’s thoughts and emotions, their various forms of expression, and all other aspects that require secrecy by virtue of their nature.<sup>145</sup> The intimate sphere is absolutely protected and cannot be exposed to the public at all.<sup>146</sup>

A further statutory protection of privacy is found in the *Kunsturhebergesetz* (Act on the Author’s Rights in Respect of Artistic Works and Photography), which provides protection against the publication or dissemination of a person’s image.<sup>147</sup> Section 22 of the *Kunsturhebergesetz* states, “Images may only be disseminated or publicly be presented with the approval of the person shown.”<sup>148</sup> Approval is deemed to have been granted if the person shown in the image received consideration for the production of the image.<sup>149</sup> The statute does not

---

139. *Id.* at 79.

140. *Id.*

141. *Id.*

142. SABINE MICHALOWSKI & LORNA WOODS, GERMAN CONSTITUTIONAL LAW: THE PROTECTION OF CIVIL LIBERTIES 3–4 (1999). For the text of the Weimar Constitution, see HEINRICH OPPENHEIMER, THE CONSTITUTION OF THE GERMAN REPUBLIC, at 219–58 (1923).

143. Thomas R. Klötzel, *Privacy and Personality*, in INTERNATIONAL PRIVACY, PUBLICITY AND PERSONALITY LAWS 157, 157 (Michael Henry ed., 2001).

144. *Id.*

145. *Id.* at 158.

146. *Id.*

147. *Id.* at 159.

148. *Id.* at 165.

149. *Id.*

prohibit the taking of an image but only its dissemination and publication, although case law has recognized that the act of taking a picture itself can be considered a violation of the general personality right.<sup>150</sup> This statute covers any form of image of one or more persons.<sup>151</sup> It is necessary that the person shown can be recognized, but it is sufficient if the individual can be identified by a small number of people on the basis of certain elements such as appearance, haircut, clothing, and so forth.<sup>152</sup>

In Germany, only one case to date has been litigated regarding alleged privacy violations occasioned by the imagery aspect of Street View (as opposed to the surreptitious data-collection aspect). The plaintiff, identified only as a woman in Berlin, was the owner of a single-family house in a “quiet” neighborhood of other single-family houses.<sup>153</sup> She claimed that although photographs taken of a house from a public street are not “objectionable,” it would be an infringement upon her “personality” for a photograph to be taken of her property over a six-foot-tall hedge, which would show her dwelling and possibly her and her family.<sup>154</sup> Accordingly, she sought to have her house omitted from the Street View program.<sup>155</sup> The *Landgericht* (Court of Appeal of the State of Berlin) held, however, that she had no legal claim by which Google could be enjoined from photographing her house—which Google had not yet done—on account of injury to her “general personality right” (*allgemeinen Persönlichkeitsrechts*) under the *Grundgesetz*.<sup>156</sup> The court found the possibility too remote that Google would take images of her house showing a detailed glimpse into its private areas, especially because Google utilizes technology to render faces unrecognizable through blurring.<sup>157</sup> Moreover, the court found this possibility remote because in Germany, Google allows homeowners and renters to request that their buildings be hidden in Street View by a pixelated “curtain,” which would allow the plaintiff to “secure her rights more quickly and easily” than through an injunction.<sup>158</sup>

---

150. *Id.*

151. *Id.* at 166.

152. *Id.*

153. Landgericht [LGZ] [Court of Appeal of the State of Berlin] Sept. 13, 2010, 37 LGZ 363/10, available at <http://www.berlin.de/sen/justiz/gerichte/kg/presse/archiv/20110315.1545.335632.html>.

154. Kammergericht [OLGZ] [Supreme Court of the State of Berlin] Oct. 25, 2010, 10 OLGZ 127/10, available at <http://www.berlin.de/sen/justiz/gerichte/kg/presse/archiv/20110315.1545.335632.html> (“Die Antragstellerin geht zutreffend davon aus, dass Aufnahmen eines Hauses von offener Straße aus nicht zu beanstanden sind. Etwas anderes gilt nur, soweit Aufnahmen unter Überwindung einer Umfriedung angefertigt werden und/oder die Wohnung zeigen, weil dies eine Persönlichkeitsrechtverletzung darstellen kann.”).

155. *Id.*

156. 37 LGZ 363, at 6.

157. *Id.* at 3, 5.

158. *Id.* at 5 (“Damit kann der Betroffene, jedenfalls was die wesentlichen möglichen

The court did, however, state that the plaintiff's rights might be implicated if she or her family actually were to be photographed on the street or in their neighborhood, as this might constitute infringement of section 22 of the *Kunsturhebergesetz*.<sup>159</sup> However, the court stated that while it was "theoretically conceivable that [the plaintiff and her family] would be in the street at the moment the photograph was taken," such an event is only a "bare possibility" and "not particularly likely" because the vehicle would pass by while taking photographs for "only a few seconds."<sup>160</sup> The court considered the possibility of personal photographs or otherwise impermissible images being disseminated on Street View to be small, and the harm that such images would cause the plaintiff to be less severe than the *actual* publication of improper photos.<sup>161</sup> Thus, the plaintiff was not entitled to a temporary restraining order or preliminary injunction.<sup>162</sup>

The *Kammergericht* (Supreme Court of the State of Berlin) upheld this decision on October 25, 2010.<sup>163</sup> Both of these rulings came just a few months before Street View was launched in Germany.<sup>164</sup> It was therefore unclear whether the plaintiff's house was even going to be shown in Street View or what additional, personal aspects of her property or private life would be shown on that service. As a result, the *Landgericht* and the *Kammergericht* demonstrated skepticism about the privacy risks that Street View posed and found that the only harm to the plaintiff was purely speculative. Indeed, there could not have been any harm before the images of German cities were made public, because whatever damage might have been done to the plaintiff or others would have arisen only when millions of Internet users could view them in private moments.

As the complaints to Privacy International showed, the harm came to persons captured by Street View only after the images were taken and then made available to anyone in the world with an Internet

---

Verletzungshandlungen betrifft, seine Rechte auf andere Weise einfacher und schneller durchsetzen.").

159. *Id.* at 4.

160. *Id.* at 5.

161. *Id.* at 6.

162. *Id.*

163. Kammergericht [OLGZ] [Supreme Court of the State of Berlin] Oct. 25, 2010, 10 OLGZ 127/10, available at <http://www.berlin.de/sen/justiz/gerichte/kg/presse/archiv/20110315.1545.335632.html>.

164. These rulings, however, were not made public until Berlin's city government issued a press release on March 15, 2011, with the first media reports about the ruling coming one week after that. Press Release, Kammergericht [Supreme Court of Berlin], *Aufnahmen Eines Hauses für Google Street View von der Offenen Straße aus Nicht zu Beanstanden* (Mar. 15, 2011), available at <http://www.berlin.de/sen/justiz/gerichte/kg/presse/archiv/20110315.1545.335632.html>; see also Jeremy Kirk, *Berlin Court Rules Street View Doesn't Invade Privacy*, PC WORLD (Mar. 22, 2011, 7:40 AM), [http://www.pcworld.com/businesscenter/article/222805/berlin\\_court\\_rules\\_street\\_view\\_doesnt\\_invade\\_privacy.html](http://www.pcworld.com/businesscenter/article/222805/berlin_court_rules_street_view_doesnt_invade_privacy.html).

connection—especially those who knew the people photographed. Had the courts had the opportunity to witness Street View in operation, they would have been able to see some of the images circulated in the press in the days after its launch. These included a completely nude man in the trunk of his car, which was parked in the driveway of his house in Mannheim;<sup>165</sup> a prostitute searching for customers on a street in Cologne;<sup>166</sup> a prostitute in a Nuremburg brothel standing in a window at the same level as the car-mounted camera and wearing only underwear and a wristwatch;<sup>167</sup> and a truck driver in Munich urinating by the side of the road, with the truck’s license plate blurred but not the man’s face.<sup>168</sup> While the existence of images like these might not have led to a different outcomes in the cases just discussed, the courts’ analyses of how the service functions likely would have been different. Specifically, it would have been difficult for the courts to say that the fact that Google’s photos are taken from several meters above a car’s roof, and from the street as opposed to the sidewalk, makes these photos less likely to infringe on someone’s privacy. In fact, the cameras’ position is what has enabled the photos described above to be so intrusive.<sup>169</sup>

Because the *Landgericht* and the *Kammergericht* ruled only narrowly that the plaintiff was not entitled to “preventative” relief,<sup>170</sup> it remains to be seen how a German court would consider allegations of actual harm brought by people whose images were actually distributed via Street View. For the time being, at least in Germany, the mere filming from the street of publicly viewable *buildings* does not violate German privacy laws. Nevertheless, Google in Germany recently acknowledged that it does not intend to expand Street View beyond the twenty cities currently available, nor will it take steps to update the imagery it currently has in Germany.<sup>171</sup> While Google gave no official reason for stopping further Street View activities in Germany, one press source stated that it “cannot be ruled out” that the “massive protests . . . have contributed” to this decision, including the 244,000 requests Google received from people who wanted their houses pixelated out of Google’s maps.<sup>172</sup>

---

165. Huch, *Was Hat den Google da Gefilmt?*, BILD ZEITUNG (Ger.) (Nov. 20, 2010), <http://www.bild.de/BILD/news/leserreporter/aktuell/nachrichten/2010/11/19/google-street-view-fehler/ungepixelte-menschen.html>.

166. *Id.*

167. *Id.*

168. *Id.*

169. Landgericht [LGZ] [Court of Appeal of the State of Berlin] Sept. 13, 2010, 37 LGZ 363/10 5, available at <http://www.berlin.de/sen/justiz/gerichte/kg/presse/archiv/20110315.1545.335632.html>.

170. *Id.* at 3.

171. Christian Fenselau, *Keine Neuen Deutschen Städte in Google Street View*, T-ONLINE BLOG (Mar. 23, 2011, 2:08 PM), [http://computer.t-online.de/google-street-view-keine-neuen-staedte-in-deutschland/id\\_45187128/index?news](http://computer.t-online.de/google-street-view-keine-neuen-staedte-in-deutschland/id_45187128/index?news).

172. *Id.*

Google thus far has prevailed in litigation regarding the image-taking and image-distribution aspects of Street View both in the U.S. and in Germany. The limited scope of these decisions, however, means that German and U.S. courts have yet to consider the issue of whether images of a person, either on her own property or in the wider public, can compromise a person's identity and thus violate her expectations of privacy once disseminated via Street View. In light of the statutory language of the *Kunsturhebergesetz*, it is at least conceivable that a German court could find that the distribution of images of persons in public violates this law, especially in those cases where a person's face was not pixelated or where a person's identity could be discerned from other aspects of her physical appearance.

#### IV. AN INTERNATIONAL APPROACH TO PROTECTING PRIVACY RIGHTS

There is a strong correlation between the degree of political and economic freedom in a given country and whether images of that country appear on Street View.<sup>173</sup> A nation selected for inclusion in Street View tends to be a multiparty democracy with a great amount of political and press freedom.<sup>174</sup> Nearly all countries in which Google has operated its vehicles may be categorized as either a "full democracy" (with a flourishing political culture and fully independent press) or a "flawed democracy" (with free and fair elections but with some weaknesses, although this category also includes democracies such as France.)<sup>175</sup> Only two countries—Hong Kong and Singapore—may be categorized as having "hybrid" political systems (that is, lacking free elections or an uncurbed press.)<sup>176</sup> However, both of these nations enjoy a vast degree of economic freedom, ranking by one measure first and second in the world, respectively.<sup>177</sup> No "authoritarian" countries (systems with little political pluralism and a curtailed press) currently appear on Street View.<sup>178</sup>

It is difficult, therefore, to imagine a politically or economically open society flatly prohibiting an entity like Google from creating maps of its territory and enhancing those maps with detailed, visual, street-level data to enhance their utility. The large degree of openness in such countries, with their attendant press freedoms, appears to be

---

173. A list of countries that currently appear on Street View may be found at *Streetview Landing Page Prototype*, GOOGLE, [http://gmaps-samples.googlecode.com/svn/trunk/streetview\\_landing/streetview-map.html](http://gmaps-samples.googlecode.com/svn/trunk/streetview_landing/streetview-map.html) (last visited Feb. 14, 2012).

174. For a ranking of countries by degree of political freedom, see ECONOMIST INTELLIGENCE UNIT, *DEMOCRACY INDEX 2010: DEMOCRACY IN RETREAT* 3–8 (Nov. 2010).

175. *Id.* at 31.

176. *Id.*

177. HERITAGE FOUND. & WALL ST. J., *Executive Highlights, in 2011 INDEX OF ECONOMIC FREEDOM* 6 (2011), available at [http://www.heritage.org/index/PDF/2011/Index2011\\_ExecutiveHighlights.pdf](http://www.heritage.org/index/PDF/2011/Index2011_ExecutiveHighlights.pdf).

178. ECONOMIST INTELLIGENCE UNIT, *supra* note 174, at 32.

incompatible with government action that would obstruct the dissemination of the sort of information Google provides. Even a democratic nation with enormous security concerns, such as Israel, likely will soon appear on Street View despite misgivings that such photos might enable terrorist attacks.<sup>179</sup>

But to allow an entity like Google to operate freely cannot mean that it also should be allowed to provide its service absolutely unchecked. Legislatures and courts must consider the countervailing forces of political and economic liberty and the privacy interests of individuals in light of rapid changes in technology. Otherwise, lawmakers would be conceding the field of identity protection to a profit-driven organization that might not share the privacy concerns of the broader public.

The more that technology operates at a supranational level, allowing Internet users to access information from any place in the world, the more U.S. lawmaking bodies must consider legal standards of privacy protection being developed elsewhere. Failing to do so might diminish the ability of U.S. companies to make their services accessible to Internet users beyond the U.S., thus hindering companies' global reach even as they comply with domestic law. Congress should formulate vigorous identity protections in light of developments abroad, but which are based on our common law and constitutional precedents that respect the right to an inviolate personality or the right to be let alone. Such legislation would bring U.S. data-protection norms closer to those currently enforced or likely to prevail in other open, democratic societies, such as the recent European proposal for a "right to be forgotten."<sup>180</sup> It also would help to ensure that the U.S. technology sector retains the freedom to innovate—a freedom that has made services like Street View indispensable throughout the world—while offering consumer protections flexible enough to respond quickly to unanticipated challenges that new technologies may engender.

As the statements of Senators Kerry and McCain and the Department of Commerce's report on data privacy indicate, the primary concern of the U.S. government regarding Internet privacy is the security of personal data transmitted to third parties, regardless of whether third parties buy the information or obtain it for free. As discussed above, however, a photograph of a person is data about that person just as much as are an address or date of birth. Therefore, any data-protection legislation Congress proposes to empower consumers to control the flow

---

179. Jessica Guynn, *In Israel, Google Street View Is Seen as Possible Tool for Terrorists*, L.A. TIMES, Feb. 22, 2011, at 1; see also Chloe Albanesius, *Google Street View Coming to Israel "Soon," Officials Say*, PC MAG. (Feb. 22, 2011, 11:01 AM), <http://www.pcmag.com/article2/0,2817,2380709,00.asp>.

180. Matt Warman, *EU Proposes Online Right "to Be Forgotten,"* TELEGRAPH (London) (Nov. 5, 2010, 12:55 PM), <http://www.telegraph.co.uk/technology/internet/8112702/EU-proposes-online-right-to-be-forgotten.html>.

of information about them must also include the ability to control the transmission of an image of a person. The right to an inviolate personality ought to form the basis of consumers' ability to control personal data, both because this right is so deeply embedded in American jurisprudence and because traditional privacy torts are too limited to respond to technology's ever-improving ability to capture and disseminate personal information efficiently.

As a global entity producing data accessible anywhere in the world that has an unfettered Internet connection, Google must grapple with a patchwork of privacy regimes throughout the world. However, Google need not wait until Congress (or lawmaking bodies abroad) passes statutes or regulations protecting an individual's right to privacy before it takes steps to remedy the grave privacy concerns about Street View that have dogged it in the past. It could, for instance, implement technological solutions for assuring that Street View does not distribute even partial images of private individuals who may not wish to appear on the service.

One approach to this solution is the three-dimensional imagery shown by the map service of Google's Chinese counterpart, Baidu.<sup>181</sup> Users of Baidu's maps have the ability to "swoop" over Chinese cities and view detailed digital representations of almost every building in a city, thereby allowing users to visualize a part of the city or a route between two points even if they cannot view it from a street-level perspective.<sup>182</sup> The result of such purely digital imagery, however, is that Baidu's monochromatic cityscapes are disconcertingly devoid of any people, cars, or activity. Accordingly, the advantages of actual street-level imagery for drivers or pedestrians navigating unfamiliar territory are lacking because the maps do not render a true-to-life depiction of the area.

But Google need not resort to such exclusively digital representations to ensure that people's identities are not compromised, particularly because doing so would negate a large part of the functionality of Google Maps. It could instead develop a technology to replace images of people with renderings of unreal persons, created by digital artists, similar to architectural renderings. Such a technology would eliminate the possibility that a person's identity could be divulged while also showing scenes that might even be more representative of that particular place,

---

181. See Baidu, <http://map.baidu.com/> (last visited Feb. 14, 2012).

182. It is not clear why Baidu elected to show only three-dimensional representations of China's cities; one concern may be to avoid running afoul of Article 120 of the General Principles of Civil Law of the People's Republic of China, which provides that "[i]f a citizen's right of personal name, portrait, reputation or honour is infringed upon, he shall have the right to demand that the infringement be stopped." See General Principles of Civil Law of the People's Republic of China (promulgated by the Nat'l People's Congress., Apr. 12, 1986, effective Jan. 1, 1987), available at <http://en.chinacourt.org/public/detail.php?id=2696>.

perhaps by varying the density of the crowds depending on the time of day or by showing animations of a journey between points on a map.<sup>183</sup> Google could thus sidestep the need to respond to inconsistent and unpredictable privacy regimes among different countries by digitally altering Street View's imagery to obviate any possibility of identifying any persons who happen to be caught at that fraction of a second that one of Google's cameras releases its shutter as it rolls down a public thoroughfare.

### CONCLUSION

The reach of Street View has expanded far beyond the initial concept seen in 2007, when Google added photographs of several U.S. cities to its maps. If anything, the "street" part of the name is becoming less and less accurate as Google makes available images taken from railways in the Swiss Alps<sup>184</sup> and even places with no paved roads like the Amazon River<sup>185</sup> and Antarctica.<sup>186</sup> Street View also has made available images from the inside of museums such as the Metropolitan Museum of Art in New York City, the National Gallery in London, and the Hermitage in Saint Petersburg, Russia.<sup>187</sup> Most recently, Google announced a service called Places that will show the interiors of businesses such as restaurants, hotels, and fitness clubs.<sup>188</sup> The more that Street View and related services achieve a panopticon-like level of coverage of the globe, the greater the likelihood that Google will capture and disseminate images of persons who are engaging in certain activities precisely because they had an expectation of privacy.

As images not only become more widely accessible over the Internet, but also attain a permanent digital presence through caching and archiving, the need to defend the right to an inviolate personality grows more imperative. Rather than allowing the "right to be let alone" to become something that a for-profit corporation may or may not choose to grant, government entities must vigorously safeguard that right for those who might wish to exercise it.

---

183. For an example of what digital simulations of persons and street life in an urban landscape might look like, including movements of pedestrians, see TRANSBAY TRANSIT CENTER, <http://transbaycenter.org/> (last visited Feb. 14, 2012), which depicts a mass-transit hub currently being constructed in downtown San Francisco that is slated for completion in 2018.

184. *Street View Hits the Stunning Swiss Alp Railways*, OFFICIAL GOOGLE BLOG (Oct. 20, 2011, 7:00 AM), <http://googleblog.blogspot.com/2011/10/street-view-hits-stunning-swiss-alps.html>.

185. Juan Forero, *Google Goes to the Amazon*, WASH. POST, Oct. 18, 2011, at A8.

186. Sam Biddle, *Google Street View Invades Antarctica*, GIZMODO (Sept. 30, 2010, 7:20 PM), <http://gizmodo.com/5652406/google-street-view-invades-antarctica>.

187. Nick Bilton, *Google Takes Street View into Art Museums*, N.Y. TIMES BITS (Feb. 2, 2011, 2:55 PM), <http://bits.blogs.nytimes.com/2011/02/01/google-takes-street-view-into-art-museums>.

188. Dan Smith, *Google Rolls Street View Indoors with Places*, WIRED UK (Oct. 31, 2011), <http://www.wired.co.uk/news/archive/2011-10/31/google-streetview-moves-indoors>.

\*\*\*