

## Mapping Online Privacy

Jacqueline D. Lipton \*

### *Abstract*

*Privacy scholars have recently outlined difficulties in applying existing concepts of personal privacy to the maturing Internet. With Web 2.0 technologies, more people have more opportunities to post information about themselves and others online, often with scant regard for individual privacy. Shifting notions of “reasonable expectations of privacy” in the context of blogs, wikis, and online social networks create challenges for privacy regulation. Courts and commentators struggle with Web 2.0 privacy incursions without the benefit of a clear regulatory framework. This article offers a map of privacy that might help delineate at least the outer boundaries of Web 2.0 privacy. The aim is to develop an umbrella under which individual aspects of privacy may be collected and examined, along with their relationships to each other. The key aspects of privacy identified are: (i) actors/relationships; (ii) privacy-threatening conduct; (iii) motivations; (iv) harms/remedies; (v) nature of private information; and, (vi) format of information. The author suggests that by examining these aspects of privacy, and their inter-relationships, we might gain a more comprehensive picture of online privacy. We might also gain a better idea of precisely where Web 2.0 technologies are putting pressure on the boundaries of traditional notions of privacy.*

### Table of Contents

I.	Introduction: The Professor, the Judge, and the Internet .....	
II.	The Maturing Internet and Limitations of Existing Privacy Models .....	
	A. Legal Models of Privacy .....	
	B. Privacy Theory .....	
	1. <i>Theories Defining the Nature of Privacy</i> .....	
	2. <i>Theories Categorizing Privacy Harms</i> .....	
	3. <i>Theories Proposing Specific Legal Reforms</i> .....	
III.	Mapping Privacy .....	
	A. Actors/Relationships .....	
	B. Conduct .....	
	C. Motivations .....	
	D. Harms/Remedies .....	

---

\* Professor of Law, Associate Dean for Faculty Development and Research, Co-Director, Center for Law, Technology and the Arts, Associate Director, Frederick K Cox International Law Center, Case Western Reserve University School of Law, 11075 East Boulevard, Cleveland, Ohio 44106, USA, Email: Jacqueline.Lipton@case.edu, Fax: (216) 368 2086. The author would like to thank Professor James Speta and Professor Olufunmilayo Arewa for including me in the “maturing Internet” discussions at Northwestern University, as well as other participants at the Maturing Internet Studies conference, Northwestern University School of Law, May 11, 2009, Chicago, Illinois. Particular thanks are due (again) to Professor Olufunmilayo Arewa, Professor James Speta, and also Professor Brett Frischmann, Professor Peter DiCola, Professor Bryan Pardo, Professor Danielle Keats Citron, Professor Patricia Sánchez Abril, and Professor Matthew Sag. All errors and omissions are my own.

- 1. Harms.....
- 2. Remedies .....
- E. Nature of Information .....
- F. Format of Information.....
- IV. Conclusions.....

**I. INTRODUCTION: THE PROFESSOR, THE JUDGE, AND THE INTERNET...**

*“It is not a rare phenomenon that what is legal may also be quite irresponsible. That appears in the First Amendment context all the time. What can be said often should not be said.”*

Justice Antonin Scalia<sup>1</sup>

Justice Scalia here refers to a class exercise assigned by Professor Joel Reidenberg of Fordham Law School.<sup>2</sup> Professor Reidenberg had historically assigned students in his privacy class the task of finding a specific esoteric piece of information about him online. His aim was to illustrate ways in which the public/private boundaries break down in the Internet age.<sup>3</sup> In early 2009, one of Professor Reidenberg’s students posted a news report on the class discussion board about comments on digital privacy made by Justice Scalia. The Judge had said: "Every single datum about my life is private? That's silly."<sup>4</sup> This inspired Professor Reidenberg to select Judge Scalia as the focus of the class exercise for the semester. The theme was still to illustrate the breaking down of public/private boundaries online. Professor Reidenberg had been thinking of experimenting with a more public figure and felt that Justice Scalia was a good choice.<sup>5</sup>

Students compiled a dossier about Justice Scalia from information publicly available online that included some information about his family, both in text and image formats.<sup>6</sup> The information collected was not made public, although Justice Scalia was

<sup>1</sup> Cited in Kashmir Hill, *Justice Scalia Responds to Fordham Privacy Invasion!*, Above The Law, April 29, 2009, available at [http://abovethelaw.com/2009/04/justice\\_scalia\\_responds\\_to\\_for.php](http://abovethelaw.com/2009/04/justice_scalia_responds_to_for.php) (last viewed on May 9, 2009).

<sup>2</sup> Daniel Solove, *Justice Scalia’s Dossier: Joel Reidenberg Responds*, Concurring Opinions, May 1, 2009, available at [http://www.concurringopinions.com/archives/2009/05/justice\\_scalias\\_3.html](http://www.concurringopinions.com/archives/2009/05/justice_scalias_3.html), last viewed on May 25, 2009; see also Noam Cohen, *Law Students Teach Scalia About Privacy and the Web*, The New York Times, May 17, 2009, full text available at [http://www.nytimes.com/2009/05/18/technology/internet/18link.html?\\_r=1](http://www.nytimes.com/2009/05/18/technology/internet/18link.html?_r=1), last viewed on May 25, 2009.

<sup>3</sup> *id.*

<sup>4</sup> Kashmir Hill, *Justice Scalia Responds to Fordham Privacy Invasion!*, Above The Law, April 29, 2009, available at [http://abovethelaw.com/2009/04/justice\\_scalia\\_responds\\_to\\_for.php](http://abovethelaw.com/2009/04/justice_scalia_responds_to_for.php), last viewed on May 9, 2009.

<sup>5</sup> Daniel Solove, *Justice Scalia’s Dossier: Joel Reidenberg Responds*, Concurring Opinions, May 1, 2009, available at [http://www.concurringopinions.com/archives/2009/05/justice\\_scalias\\_3.html](http://www.concurringopinions.com/archives/2009/05/justice_scalias_3.html), last viewed on May 25, 2009; see also Noam Cohen, *Law Students Teach Scalia About Privacy and the Web*, The New York Times, May 17, 2009, full text available at [http://www.nytimes.com/2009/05/18/technology/internet/18link.html?\\_r=1](http://www.nytimes.com/2009/05/18/technology/internet/18link.html?_r=1), last viewed on May 25, 2009.

<sup>6</sup> *id.*

informed of its existence.<sup>7</sup> To Professor Reidenberg, this was a “teachable moment”.<sup>8</sup> To Justice Scalia, it was an exercise in poor professorial judgment.<sup>9</sup> Did it alter the views of either man about online privacy? Probably not. At the end of the day, the professor felt that he had proved his point about the “over-transparency of personal information” online.<sup>10</sup> The Judge stood by his own previous remarks on privacy.<sup>11</sup> Nevertheless, the exchange sparked a vibrant online debate about privacy in the age of the maturing Internet<sup>12</sup> - a useful starting point for this discussion.

We are now in an age where online communications are much broader in scope, speed, and nature than the early days of the Internet. With participatory Web 2.0 technologies,<sup>13</sup> many more people than ever before have opportunities to gather, collate, and disseminate information about others, globally, and at the push of a button. Privacy laws and policies have been slow to adapt to these technologies.<sup>14</sup> Of course, an obvious

---

<sup>7</sup> Cited in Kashmir Hill, *Justice Scalia Responds to Fordham Privacy Invasion!*, Above The Law, April 29, 2009, available at [http://abovethelaw.com/2009/04/justice\\_scalia\\_responds\\_to\\_for.php](http://abovethelaw.com/2009/04/justice_scalia_responds_to_for.php), last viewed on May 9, 2009.

<sup>8</sup> Daniel Solove, *Justice Scalia's Dossier: Joel Reidenberg Responds*, Concurring Opinions, May 1, 2009, available at [http://www.concurringopinions.com/archives/2009/05/justice\\_scalias\\_3.html](http://www.concurringopinions.com/archives/2009/05/justice_scalias_3.html), last viewed on May 25, 2009; see also Noam Cohen, *Law Students Teach Scalia About Privacy and the Web*, The New York Times, May 17, 2009, full text available at [http://www.nytimes.com/2009/05/18/technology/internet/18link.html?\\_r=1](http://www.nytimes.com/2009/05/18/technology/internet/18link.html?_r=1), last viewed on May 25, 2009.

<sup>9</sup> Kashmir Hill, *Justice Scalia Responds to Fordham Privacy Invasion!*, Above The Law, April 29, 2009, available at [http://abovethelaw.com/2009/04/justice\\_scalia\\_responds\\_to\\_for.php](http://abovethelaw.com/2009/04/justice_scalia_responds_to_for.php), last viewed on May 9, 2009 (“Prof. Reidenberg's exercise is an example of perfectly legal, abominably poor judgment. Since he was not teaching a course in judgment, I presume he felt no responsibility to display any.”)

<sup>10</sup> Daniel Solove, *Justice Scalia's Dossier: Joel Reidenberg Responds*, Concurring Opinions, May 1, 2009, available at [http://www.concurringopinions.com/archives/2009/05/justice\\_scalias\\_3.html](http://www.concurringopinions.com/archives/2009/05/justice_scalias_3.html), last viewed on May 25, 2009; see also Noam Cohen, *Law Students Teach Scalia About Privacy and the Web*, The New York Times, May 17, 2009, full text available at [http://www.nytimes.com/2009/05/18/technology/internet/18link.html?\\_r=1](http://www.nytimes.com/2009/05/18/technology/internet/18link.html?_r=1), last viewed on May 25, 2009.

<sup>11</sup> Kashmir Hill, *Justice Scalia Responds to Fordham Privacy Invasion!*, Above The Law, April 29, 2009, available at [http://abovethelaw.com/2009/04/justice\\_scalia\\_responds\\_to\\_for.php](http://abovethelaw.com/2009/04/justice_scalia_responds_to_for.php), last viewed on May 9, 2009 (“I stand by my remark at the Institute of American and Talmudic Law conference that it is silly to think that every single datum about my life is private.”)

<sup>12</sup> Daniel Solove, *Justice Scalia's Dossier: Joel Reidenberg Responds*, Concurring Opinions, May 1, 2009, available at [http://www.concurringopinions.com/archives/2009/05/justice\\_scalias\\_3.html](http://www.concurringopinions.com/archives/2009/05/justice_scalias_3.html), last viewed on May 25, 2009; see also Noam Cohen, *Law Students Teach Scalia About Privacy and the Web*, The New York Times, May 17, 2009, full text available at [http://www.nytimes.com/2009/05/18/technology/internet/18link.html?\\_r=1](http://www.nytimes.com/2009/05/18/technology/internet/18link.html?_r=1), last viewed on May 25, 2009; Kashmir Hill, *Justice Scalia Responds to Fordham Privacy Invasion!*, Above The Law, April 29, 2009, available at [http://abovethelaw.com/2009/04/justice\\_scalia\\_responds\\_to\\_for.php](http://abovethelaw.com/2009/04/justice_scalia_responds_to_for.php), last viewed on May 9, 2009.

<sup>13</sup> DAVID KESMODEL, *THE DOMAIN GAME: HOW PEOPLE GET RICH FROM INTERNET DOMAIN NAMES*, 126 (2008) (“Web 2.0 was a buzz word used to describe a new wave of Web businesses that leveraged social networking, user-generated content, and other forms of collaboration and information-sharing on the Internet.”); JANET LOWE, *GOOGLE SPEAKS: SECRETS OF THE WORLD'S GREATEST BILLIONAIRE ENTREPRENEURS, SERGEY BRIN AND LARRY PAGE*, 294 (2009) (defining “Web 2.0” as “A term used to describe an evolving generation of a participatory Web. Web 2.0 describes the proliferation of interconnectivity and social interaction on the World Wide Web.”)

<sup>14</sup> Of course, privacy law is problematic at the best of times because it is aimed at restricting truthful speech about individuals often in the face of powerful speech protections such as the First Amendment in the United States. Even in jurisdictions with strong legal protections for personal privacy, the balance

reason for this lag is simple mechanics. It takes longer for laws to evolve than for digital technology to advance. This is particularly true of laws that involve basic human values, such as privacy and free speech. Additionally, technology advances globally while laws relating to cultural mores are usually local.<sup>15</sup> Further, if we want laws to reflect societal expectations of privacy, it is simply too early to identify any – or many - clear social norms in the context of Web 2.0. Without clearer identification of norms and values, legislators and judges will be at a loss to craft laws that reflect appropriate ideals.

This article looks at the online privacy question from a broader perspective than much of the previous literature. It develops a map of privacy at a higher level of abstraction than has been previously available. The thesis is that many lawmakers and commentators have struggled with privacy theory because they are too close to a particular situation or given set of privacy problems. Because privacy has historically encompassed wide-ranging areas of social, economic, and governmental interaction, it may help at this point to pull back the lens and see if it is possible to create a larger scale map of privacy. This may help to determine the outer boundaries of privacy, as well as the constituent elements of a privacy incursion, and the inter-relationships between those elements. In this context, the author identifies six discrete aspects of privacy relating to: (a) actors/relationships; (b) conduct; (c) motivations; (d) harms/remedies (e) nature of information; and, (f) format of information.

These elements taken together can describe, at a relatively high level of abstraction, any given privacy-threatening scenario. Examining such scenarios in this way might enable us to gain a better sense of what properly belongs within each element, and of the interactions between them. This approach to privacy will not create a perfect picture of privacy and is certainly not the only way a privacy landscape could be mapped for Web 2.0. However, despite the high level of abstraction and broad scope of this approach, it allows us to identify recurring themes and patterns in Web 2.0 privacy incursions that may not otherwise become apparent.<sup>16</sup> Part II highlights the limitations of current privacy law and theory in the context of Web 2.0. Part III develops a map of privacy for Web 2.0 based on the six aspects of privacy described above. Part IV concludes with a brief discussion of the contributions and limitations of this mapping technique in developing clearer and more cohesive privacy laws and policies for the future.

---

between privacy and speech is difficult for courts: see, for example, discussion in *Mosley v News Group Newspapers Ltd*, [2008] EWHC 1777 (QB), para 8-15 (describing balance between free speech and privacy under Articles 8 and 10 of the European Convention on Human Rights and Fundamental Freedoms).

<sup>15</sup> By way of example, privacy law is a matter of state law in the United States.

<sup>16</sup> This is similar to the approach taken by Professor James Grimmelman recently in his attempt to map a law of Internet search engines: James Grimmelman, *The Structure of Search Engine Law*, 93 IOWA L REV 1, 15 (2007) (“The set of laws potentially applicable to search may seem bewilderingly large. It has, however, a recurring deep structure that becomes evident if we focus on four concepts: the actors involved, the information flows among them, the interests that they bring to search, and the legal theories that they use to vindicate their interests.”)

## II. THE MATURING INTERNET AND LIMITATIONS OF EXISTING PRIVACY MODELS

### A. LEGAL MODELS OF PRIVACY

*“New technologies do not just enhance freedom but also alter the matrix of freedom and control in new and challenging ways.”*

Professor Daniel Solove<sup>17</sup>

Web 2.0 involves more voices than previous Internet technologies. With blogs,<sup>18</sup> wikis,<sup>19</sup> online social networks,<sup>20</sup> and massively multi-player online games,<sup>21</sup> more people are able to communicate more information both about themselves and about others – sometimes deliberately and sometimes incidentally to some other form of interaction.<sup>22</sup> This raises a whole host of privacy concerns differing in nature and scope from what has gone before. Earlier Internet privacy concerns related predominantly to the aggregation and availability of large-scale text-based digital dossiers about individuals.<sup>23</sup> These were addressed, to the extent they were addressed at all, by laws aimed at regulating the aggregation and use of such dossiers by governments and corporate entities.<sup>24</sup>

---

<sup>17</sup> DANIEL SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET*, 205 (2007) [hereinafter, *THE FUTURE OF REPUTATION*].

<sup>18</sup> JOHN PALFREY and URS GASSER, *BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES*, 27 (2008) (describing a “blog” as “a very simple Web page with a mix of text and photos”); HENRY JENKINS, *CONVERGENCE CULTURE: WHERE OLD AND NEW MEDIA COLLIDE*, 320 (2006) (describing “blogging” as “the term initially referred to a technological platform that allowed easy and rapid updating of Web content. Increasingly, it has come to refer to a mode of publication of grassroots origin that responds to information circulated either by other bloggers or by the mainstream media.”); JANET LOWE, *GOOGLE SPEAKS: SECRETS OF THE WORLD’S GREATEST BILLIONAIRE ENTREPRENEURS*, SERGEY BRIN AND LARRY PAGE, 288 (2009) (defining “blog” as “Short for *Web log*, or a string of journal entries posted on a Web page.”).

<sup>19</sup> DON TAPSCOTT and ANTHONY D WILLIAMS, *WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING*, 13 (2008) (defining a “wiki” as “software that enables users to edit the content of Web pages.”); LOWE, *GOOGLE SPEAKS*, *supra* note \_\_\_, at 294 (defining “wikis” as “A collection of Web pages that enables anyone who accesses them to contribute or modify content, using a simplified computer language.”)

<sup>20</sup> SOLOVE, *THE FUTURE OF REPUTATION*, *supra* note \_\_\_, at 26 (2007) (describing the concept underlying social networking sites as enabling networks of friends and acquaintances to digitally link their profiles, share personal information and communicate with each other) [hereinafter, *THE FUTURE OF REPUTATION*]; LOWE, *GOOGLE SPEAKS*, *supra* note \_\_\_, at 292 (describing “social networking” as “Websites that allow people to share ideas, information, and images and to form networks with friends, family, or other like-minded individuals.”)

<sup>21</sup> JENKINS, *supra* note \_\_\_, at 329 (“Massively multiplayer online role-playing games, an emerging genre that brings together thousands of people interacting through avatars in a graphically rich fantasy environment.”)

<sup>22</sup> TAPSCOTT and WILLIAMS, *supra* note \_\_\_, AT 242-243 (describing social interactions between geographically dispersed coworkers whilst playing the online game *Battlefield 2*).

<sup>23</sup> DANIEL SOLOVE, *THE DIGITAL PERSON*, 1-7 (2004) (describing the problem of “digital dossiers” online) [hereinafter, *THE DIGITAL PERSON*].

<sup>24</sup> See, for example, discussion of the European Union Data Protection Directive in Part II.A *infra*.

Web 2.0 raises new challenges for privacy. With more voices online, there is more scope for privacy invasion. With more recording technologies easily at hand – such as cellphone cameras and text messaging services like Twitter<sup>25</sup> – there is more scope for incidental gathering of details of people’s private lives that can be uploaded and disseminated globally at the push of a button. Because of these developments, the boundaries between the public and private spheres are breaking down,<sup>26</sup> or at least becoming more difficult to discern. Thus, any privacy-protecting laws that are premised on now-dated conceptions of a “reasonable expectation of privacy”<sup>27</sup> are becoming more difficult to apply.<sup>28</sup>

One of the most comprehensive privacy regulations implemented in the early days of the Internet was the European Union Data Protection Directive.<sup>29</sup> Although broadly conceived to regulate as much privacy-threatening behavior as possible, it was drafted predominantly through a Web 1.0 lens. The Directive’s main area of operation is with respect to: “the processing of personal data wholly or partly by automatic means, and ... the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system”.<sup>30</sup> While the Directive’s definitions of “personal data”<sup>31</sup> and “processing”<sup>32</sup> are broad, the implication is that the

---

<sup>25</sup> Twitter is a digital messaging service that describes itself as: “Twitter is a service for friends, family, and co-workers to communicate and stay connected through the exchange of quick, frequent answers to one simple question: What are you doing?” (see [twitter.com](http://twitter.com), last viewed on June 15, 2009). “Twitter” is described in Wikipedia.org as: “[A] free social networking and micro-blogging service that enables its users to send and read other users’ updates known as *tweets*. Tweets are text-based posts of up to 140 characters in length which are displayed on the user’s profile page and delivered to other users who have subscribed to them (known as *followers*).” (see <http://en.wikipedia.org/wiki/Twitter>, last viewed on May 25, 2009). Twitter is technically both an information gathering and dissemination technology as the recording and distribution of a “tweet” both gathers and distributes information about something or someone almost simultaneously.

<sup>26</sup> Daniel Solove, *Justice Scalia’s Dossier: Joel Reidenberg Responds*, Concurring Opinions, May 1, 2009, available at [http://www.concurringopinions.com/archives/2009/05/justice\\_scalias\\_3.html](http://www.concurringopinions.com/archives/2009/05/justice_scalias_3.html), last viewed on May 25, 2009.

<sup>27</sup> The “reasonable expectation of privacy” doctrine is derived originally from the Fourth Amendment of the United States Constitution. See discussion in DANIEL SOLOVE, MARC ROTENBERG and PAUL SCHWARTZ, *INFORMATION PRIVACY LAW*, 33-34 (2 ed, 2006) [hereinafter, *INFORMATION PRIVACY LAW*].

<sup>28</sup> RESTATEMENT (SECOND) OF TORTS § 652D cmt. c (related to the public disclosure of private facts tort). See also Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1, 18 (2007) (“In deciding privacy tort claims, courts are charged with determining whether there was a reasonable expectation of privacy in the space in question.”)

<sup>29</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

<sup>30</sup> Data Protection Directive, Art. 3(1).

<sup>31</sup> Data Protection Directive, Art. 2(a) (“personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”).

<sup>32</sup> Data Protection Directive, Art. 2(b) (“processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use,

drafters were contemplating large scale text-based digital filing systems typically compiled by governmental and private institutions.<sup>33</sup>

A “filing system” is defined in the Directive as: “any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis”.<sup>34</sup> Although this could cover, say, an online social networking service like Facebook, the more natural fit for such a conception is a digital database containing text-based records. Of course this is not to say that the Directive could not, or does not, apply to Web 2.0 technologies. It simply evidences the fact that the drafters of the Directive were contemplating the future of the Internet in terms of the then prevailing Web 1.0 technologies. Applying the Directive’s terms to Web 2.0 technologies could be problematic in practice, depending on the circumstances. For example, is an online multi-player game a “structured set of personal data which are accessible according to specific criteria”? Probably not. An online multi-player game, like *Second Life*,<sup>35</sup> may in fact contain personal facts about an individual – particularly if the individual’s identity associated with his or her Avatar<sup>36</sup> is known to others. However, is the information *accessible according to specific criteria* as contemplated by the Directive? This is likely not the case.

While a database containing personal information is usually searchable via keyword, the same will not be true of many multi-player games, or social networking sites. Some of these sites will be searchable by criteria that might identify data about an individual. However, the application of the Directive in the Web 2.0 context could well be more problematic and piecemeal than its original application to text-based digital databases. This is because new online technologies are not mere aggregated dossiers of personal data, but are virtual worlds that contain both personal and other information in a variety of formats. While text-based data is easily keyword searchable, other forms of data such as audio and video files are not easily searchable unless they are effectively tagged.<sup>37</sup> Newer Web 2.0 technologies that contain data in these varied formats may not easily be characterized as forums in which information is *accessible according to specific criteria* for the purposes of the Directive.

---

disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”).

<sup>33</sup> See Data Protection Directive, Art. 2(d) and (e) which respectively define “controller” and “processor” of data terms of “a natural or legal person, public authority, agency or any other body”.

<sup>34</sup> Data Protection Directive, Art. 2(c).

<sup>35</sup> PALFREY and GASSER, *supra* note \_\_\_, at 28-29 (describing *Second Life* a promising and popular virtual world).

<sup>36</sup> *id.*, at 20 (describing avatars as fake personas online that enable an individual to try out a new identity).

<sup>37</sup> *id.*, at 62 (tagging a non-text file allows it to be more easily searchable via the text in the tag); LOWE, GOOGLE SPEAKS, *supra* note \_\_\_, at 292 (defining “tagging” as “Naming an image, file, or something on the Internet. It needs a name before you can search for it.”)

The Directive has, in fact, been applied fairly broadly to online activities to date. A good example is the case of *Re Bodil Lindqvist*,<sup>38</sup> in which the European Court of Justice held that the posting on a publicly available website of gossipy text relating to private individuals by a peer who worked in a church with them was an infringement of the Directive.<sup>39</sup> Furthermore, the court held that the disclosure of the personal information was not excused by the “purely personal activities” exception in the Directive.<sup>40</sup> Nevertheless, the holding was limited to text based information disclosed to the world at large on a publicly available website. It is not clear how private information disclosed in closed online networks – like Facebook or Second Life – would fare under this reasoning.<sup>41</sup> It was clearly significant to the *Bodil Lindqvist* court that the information was publicly available to an indefinite number of people on a generally accessible website.<sup>42</sup> Additionally, as the *Bodil Lindqvist* holding dealt with data in a text format, it is not clear how the reasoning might extend to information in audio, video, or other formats which may be less easily searchable than text records.

The European Union has some of the strongest legal privacy protections in the world.<sup>43</sup> If European Union laws are potentially limited in the face of Web 2.0 technologies, how might American laws fare? The United States has never been particularly focused on protecting individual privacy. To the extent that American law has dealt with privacy, the protections have largely been restricted to government intrusions into privacy.<sup>44</sup> There has not been much of an attempt to protect individual privacy against others, outside the limited development of the four privacy torts.<sup>45</sup> There are a variety of explanations as to why the United States has not developed stronger privacy protections. Privacy law has typically taken a back seat to the First Amendment.<sup>46</sup> While there is an express constitutional guarantee of free speech and of a

<sup>38</sup> ECJ, Luxembourg, November 6, 2003, full text available at: <http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET>, last viewed on December 16, 2008.

<sup>39</sup> *id.*

<sup>40</sup> Art. 3(2) provides that: “This Directive shall not apply to the processing of personal data ... by a natural person in the course of a purely personal or household activity.”

<sup>41</sup> Of course, distinctions between open and closed networks should not be overstated, as it is relatively easy for information disclosed in a closed network to go viral and become publicly accessible.

<sup>42</sup> *Re Bodil Lindqvist*, at ¶ 47 (ECJ, Luxembourg, November 6, 2003, full text available at: <http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET>, last viewed on December 16, 2008).

<sup>43</sup> SOLOVE, ROTENBERG, and SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note \_\_\_\_, at 839 (describing the European Union’s “omnibus” approach to protecting privacy).

<sup>44</sup> *id.*, at 207 (noting the particular tension between privacy and the government’s law enforcement activities).

<sup>45</sup> Restatement (Second) of Torts, §§ 652A-E (1997).

<sup>46</sup> SOLOVE, ROTENBERG, and SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note \_\_\_\_, at 132 (“The privacy torts exist in an uneasy tension with the First Amendment.”); Diane Leenheer Zimmerman, *Is There a Right to Have Something to Say? One View of the Public Domain*, 73 FORDHAM L REV 297, 348-9 (2004) (“[F]rom the birth of the common law right of privacy, courts recognized that there is a downside to granting individuals control over how others can use information about them. It significantly strips others of the wherewithal to form their own ideas, utilize their own observations, and communicate about these things with friends, colleagues, and fellow citizens. The fear of this unconstitutional consequence is why broad newsworthiness rules have cabined the tort almost to the point of annihilation. This strongly

free press in the United States, there is no express constitutional guarantee of a right to privacy. Limited privacy rights have been implied into certain sections of the Constitution,<sup>47</sup> but obviously this is less extensive than the constitutional protections for free speech. This comparison is important because privacy rights are in constant tension with rights to free expression, particularly as regards truthful speech.<sup>48</sup> While false speech can generally be proscribed by the laws of defamation on the basis that one's reputation deserves protection even in the face of free speech guarantees, the idea of limiting truthful speech has been more problematic.<sup>49</sup>

Other explanations for the lack of privacy protections in the United States include the fact that American tort law in particular tends to focus on identifying and compensating harms that can be economically quantified. It is difficult to quantify many privacy harms in purely in this way. There may also be a sense that privacy harms are problematic because often an individual victim of a privacy incursion has been complicit in her own misfortune.<sup>50</sup> It is possible to argue, at least in the pre-Internet world, that individuals have historically held the power to control the spread of their personal information in large measure. Thus, if they have been careless about this information, they deserve what they get. In the real world, individuals can use physical structures like doors, walls, windows, safes, and locked filing cabinets to shut out the public and keep the private sphere private. Where a person fails to take advantage of these physical means of keeping sensitive information literally behind closed doors, the individual should not be regarded as having a reasonable expectation of privacy that the law should protect.

---

suggests that the ability to use speech goods is a necessary element of what the First Amendment protects, and that, as a result, it is very risky to allow individuals to “own” or control use of their life stories.”); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN L REV 1049 (2000) (suggesting that tortious approaches to protecting privacy cannot be reconciled with the First Amendment, but that contractual approaches may avoid this criticism).

<sup>47</sup> SOLOVE, ROTENBERG, and SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note \_\_\_, at 33 -34.

<sup>48</sup> *id.*, at 132 (“The privacy torts exist in an uneasy tension with the First Amendment.”); Diane Leenheer Zimmerman, *Is There a Right to Have Something to Say? One View of the Public Domain*, 73 FORDHAM L REV 297, 348-9 (2004) (“[F]rom the birth of the common law right of privacy, courts recognized that there is a downside to granting individuals control over how others can use information about them. It significantly strips others of the wherewithal to form their own ideas, utilize their own observations, and communicate about these things with friends, colleagues, and fellow citizens. The fear of this unconstitutional consequence is why broad newsworthiness rules have cabined the tort almost to the point of annihilation. This strongly suggests that the ability to use speech goods is a necessary element of what the First Amendment protects, and that, as a result, it is very risky to allow individuals to “own” or control use of their life stories.”); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN L REV 1049 (2000) (suggesting that tortious approaches to protecting privacy cannot be reconciled with the First Amendment, but that contractual approaches may avoid this criticism); SOLOVE, THE FUTURE OF REPUTATION, *supra* note \_\_\_, at 160 (“There is no easy solution to how to balance free speech with privacy and reputation .... Balancing free speech with privacy and reputation is a complicated and delicate task. Too much weight on either side of the scale will have detrimental consequences. The law still has a distance to go toward establishing a good balance.”)

<sup>49</sup> *id.*

<sup>50</sup> *Mosley v News Group Newspapers Ltd*, [2008] EWHC 1777 (QB), para. 225-6 (noting appropriateness of taking plaintiff's own conduct into account in ascertaining privacy harm).

Much of this reasoning breaks down online. Even in the Web 1.0 world, we witnessed the unprecedented ability of governments and corporations to gather and collate private data about individuals. Those individuals lost control of much of their personal information as a result. Online businesses could easily gather information about consumer spending habits as a result of using available technological means such as cookies<sup>51</sup> to track online purchases. Governments could require individuals to submit to the recording of sensitive information in centralized databases for various public policy programs.<sup>52</sup> Courts generally found these computer-enabled dealings with personal information to be acceptable, or at least not to infringe privacy rights.<sup>53</sup> This kind of conduct was precisely the type of activity at which the European Union Data Protection Directive was aimed. The Directive sought to limit the situations in which such information could be gathered and processed without a data subject's consent.<sup>54</sup> It also attempted to build in controls to ensure access to,<sup>55</sup> and accuracy of,<sup>56</sup> any data so processed.

There was no commensurate push in the United States to develop a comprehensive data protection law. Even in the early days of the Internet, American plaintiffs were forced to frame their claims in terms of piecemeal provisions of various statutes,<sup>57</sup> as well as potentially the common law privacy torts.<sup>58</sup> In the world of Web 2.0, existing laws are even more troublesome. Web 2.0 breaks down the barriers between the public and private spheres in a much more pronounced way than Web 1.0 technologies. As private individuals are participating more in gathering and communicating information about themselves and others online, the boundary between public and private - to the extent that it was ever particularly clear - potentially breaks down altogether.

Even within closed networks like Facebook, participating individuals lose the nuances of control they had over personal information in the past. For example, while the physical world accommodates gradations of relationships of friendship and trust – which may impact on what is and is not disclosed to another person – online social networks are binary. Either one is a “friend” or one isn't.<sup>59</sup> Additionally, it is very

---

<sup>51</sup> *In re Doubleclick Privacy Litigation*, 154 F. Supp. 2d 497, 502-3 (2001) (“Cookies are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner.”)

<sup>52</sup> *Whalen v Roe*, 429 U.S. 589 (1977) (upholding validating of legislation requiring government to retain records of prescriptions of certain controlled medications).

<sup>53</sup> *id.*; *In re Doubleclick Privacy Litigation*, 154 F. Supp. 2d 497 (2001); *Dwyer v American Express*, 273 Ill. App. 3d 742 (1995).

<sup>54</sup> Data Protection Directive, Art 6.

<sup>55</sup> *id.*, Art 12.

<sup>56</sup> *id.*, Art 6(1)(d).

<sup>57</sup> Such as the Electronic Communications Privacy Act, 18 U.S.C. § 2510 and the Computer Fraud and Abuse Act, 18 U.S.C. §1030.

<sup>58</sup> Restatement (Second) of Torts, §§ 652A-E (1997).

<sup>59</sup> SOLOVE, THE FUTURE OF REPUTATION, *supra* note \_\_, at 202 (“social network sites often have a very loose concept of “friend.” The sites divide a person’s social universe into “friends” and everybody else.”)

difficult to refuse to accept a request to “friend” someone, and almost impossible to “unfriend”<sup>60</sup> them once they have been “friended”. This all adds up to a loss of control over personal information in Web 2.0 forums. Current privacy laws have little to say about such problems and, moreover, are internationally disharmonized in an increasingly globalized society.

## B. PRIVACY THEORY

Privacy scholars have struggled to develop theories of privacy for Web 2.0 that make sense, and that can be translated into useful laws and policies. Some excellent work has been done in recent years in this area. A body of literature has started to emerge that attempts to delineate the policies underlying privacy regulation in the digital age. While some scholars have focused on defining the nature of privacy rights,<sup>61</sup> others have attempted to categorize privacy-threatening conduct,<sup>62</sup> and still others have talked more specifically about practical legal reforms that might better protect online privacy.<sup>63</sup> This Part briefly surveys current theoretical approaches and identifies their limitations with respect to delineating the outer boundaries of privacy for Web 2.0. The current theories themselves are not problematic *per se*. However, there is, as yet, no attempt to map the boundaries of privacy at a higher level of abstraction in order to get a better overall picture of where Web 2.0 technologies challenge existing conceptions of privacy.

### 1. Theories Defining the Nature of Privacy

With respect to the first group of privacy theories – those seeking to define the nature of privacy rights – much of the relevant literature predates the Internet. Theorists have struggled with the nature of privacy since the earliest times in human history. Indeed, the seminal article on privacy in the United States appeared in the *Harvard Law Review* circa 1890.<sup>64</sup> That article itself cited even earlier conceptions of privacy.<sup>65</sup> Like any theory, existing conceptions of privacy have their shortcomings, a number of which

---

<sup>60</sup> CORY DOCTOROW, *CONTENT*, 183 (2008) (“It’s socially awkward to refuse to add someone to your friends list – but *removing* someone from your friends list is practically a declaration of war.”)

<sup>61</sup> See, for example, JON L. MILLS, *PRIVACY: THE LOST RIGHT*, 13-15 (2008) (formula for defining privacy rights).

<sup>62</sup> DANIEL SOLOVE, *UNDERSTANDING PRIVACY*, 105 (2008) (“My taxonomy’s categories are not based upon any overarching principle. We do not need overarching principles to understand and recognize problems .... If we focus on the problems, we can better understand and address them. I aim to shift the approach to a bottom-up focus on problems that are all related to each other, yet not in exactly the same way....”). [hereinafter, *UNDERSTANDING PRIVACY*].

<sup>63</sup> See, for example, Professor Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 *HARVARD JOURNAL OF LAW AND TECHNOLOGY* 1 (2007); Professor Sánchez Abril, *A (My)Space of One’s Own: On Privacy and Online Social Networks*, 6 *NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY* (2007); Professor Sánchez Abril and Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient’s Bill of Rights*, 6 *NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY* 244 (2008).

<sup>64</sup> Samuel D. Warren and Louis Brandeis, *The Right to Privacy*, 4 *HARVARD LAW REVIEW* 193 (1890).

<sup>65</sup> THOMAS COOLEY, *COOLEY ON TORTS*, 29 (1888).

relate generally to their notion of a privacy right, but some of which are more specific to their application to the Internet age.

One of the leading new privacy theorists, Professor Daniel Solove, has recently catalogued and critiqued the main pre-Internet privacy theories.<sup>66</sup> His list includes: (a) Samuel Warren and Louis Brandeis's famous conception of privacy as the "right to be let alone";<sup>67</sup> (b) the concept of privacy as a right to limit access to the self;<sup>68</sup> (c) privacy conceived as secrecy;<sup>69</sup> (d) privacy as control over personal information;<sup>70</sup> (e) privacy as an aspect of personhood;<sup>71</sup> and, (f) privacy as control over intimate relationships.<sup>72</sup> Having identified and critiqued existing theories, Professor Solove argues that each of these theories "fail on their own terms"<sup>73</sup>, inasmuch as they do not "achieve the goal of finding the common denominator"<sup>74</sup> upon which they are premised. He then goes on to suggest that privacy theory needs to be reconceptualised by being refocused away from the idea of a common denominator.<sup>75</sup> In particular, he suggests that "the quest for a common denominator is a search for the holy grail"<sup>76</sup> and that privacy discourse may be better served by developing "a new way to understand privacy".<sup>77</sup> This article is intended as a new step in the direction advocated by Solove.

Existing theories on the nature of a privacy right are extremely useful in grappling with policy justifications behind the creation of any laws aimed at protecting personal privacy. They help to explain whether we should be focusing on ideas of economics or human dignity, or something else. Despite the lack of a common denominator, they give some guidance to our underlying theoretical conceptions of privacy. However, apart from the lack of a common denominator, the other shortcoming of most of these theoretical models is that they do not – and probably cannot – give a sense of the outer boundaries of privacy. Whether they focus on property, dignity, or relationships of confidence, they are trying to get to the inner kernel of a privacy right, not to its outer boundaries. The aim of outlining a map of privacy is to identify these outer boundaries. The idea of this article is to develop a framework within which to pinpoint precisely where traditional notions of privacy are being pushed beyond their historical bounds, and to attempt to gain a picture of how far those boundaries might realistically be pushed. Thus, traditional privacy theories will likely continue to develop an internal justification for privacy rights, while work such as this article aims to contain those theories within a meaningful set of boundaries to prevent their becoming unwieldy "catch alls" for increasingly amorphous harms arising out of Internet conduct.

---

<sup>66</sup> DANIEL SOLOVE, UNDERSTANDING PRIVACY, 12-38 (2008).  
<sup>67</sup> *id.*, 15-18; Warren and Brandeis, *The Right to Privacy*, *supra* note \_\_\_\_.  
<sup>68</sup> DANIEL SOLOVE, UNDERSTANDING PRIVACY, 18-21 (2008).  
<sup>69</sup> *id.*, at 21-24.  
<sup>70</sup> *id.*, at 24-29.  
<sup>71</sup> *id.*, at 29-34.  
<sup>72</sup> *id.*, at 34-37.  
<sup>73</sup> *id.*, at 38.  
<sup>74</sup> *id.*, at 38.  
<sup>75</sup> *id.*, at 38-39.  
<sup>76</sup> *id.*, at 38.  
<sup>77</sup> *id.*, at 39.

## 2. Theories Categorizing Privacy Harms

Professor Solove's most significant contribution to privacy discourse to date has been his innovative approach to conceptualizing privacy.<sup>78</sup> In this context, he developed a taxonomy of privacy<sup>79</sup> within which he has gathered a series of categories of conduct that implicate privacy harms. He has identified the relationships between these categories in terms of "family resemblances".<sup>80</sup> He advocates this approach over an attempt to discern a single underlying common denominator to unify privacy. He goes on to construct a theory of privacy that takes a bottom-up approach, drawing generalities from specific experiences.<sup>81</sup> Rather than being "rigid and controlling",<sup>82</sup> he advocates a framework that is "flexible and open ended"<sup>83</sup> and that draws from the similarities between different classes of conduct.<sup>84</sup>

Solove's taxonomy of privacy is organized into four categories of privacy-threatening conduct, each of which is subdivided into more specific instances of that class.<sup>85</sup> The categories are: (a) information collection; (b) information processing; (c) information dissemination; and, (d) invasion.<sup>86</sup> Collection contains sub-categories of conduct relating to surveillance<sup>87</sup> and interrogation.<sup>88</sup> Processing contemplates aggregation,<sup>89</sup> identification,<sup>90</sup> insecurity,<sup>91</sup> secondary use,<sup>92</sup> and exclusion.<sup>93</sup>

---

<sup>78</sup>78 Of course, Professor Solove is not the first scholar to attempt a categorization of privacy harms. In 1960, Dean William Prosser pioneered this approach in his seminal article that became the basis for the privacy torts in the Restatement (Second) of Torts, §§ 652A-E (1997). See William Prosser, *Privacy*, 48 CALIFORNIA LAW REVIEW 383 (1960). In this article, Dean Prosser developed four distinct categories of privacy harm which developed into the current privacy torts. They are: (a) intrusion into the plaintiff's seclusion; (b) public disclosure of private facts; (c) publicity which places the plaintiff in a false light; and, (d) misappropriation of the plaintiff's name or likeness. Professor Solove's theories are described here in preference to Dean Prosser's largely because Professor Solove's taxonomy is more readily applicable to the Internet age, while Dean Prosser's categorization scheme has caused some practical problems when applied to online conduct. These limitations have been recognized in recent scholarship: See Patricia Sánchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY (2007); Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1 (2007).

<sup>79</sup> DANIEL SOLOVE, UNDERSTANDING PRIVACY, 105 (2008) ("My taxonomy's categories are not based upon any overarching principle. We do not need overarching principles to understand and recognize problems .... If we focus on the problems, we can better understand and address them. I aim to shift the approach to a bottom-up focus on problems that are all related to each other, yet not in exactly the same way....").

<sup>80</sup> *id.*, at 40.

<sup>81</sup> *id.*, at 46-7.

<sup>82</sup> *id.*, at 49.

<sup>83</sup> *id.*, at 49.

<sup>84</sup> *id.*, at 49.

<sup>85</sup> *id.*, at 103-4.

<sup>86</sup> *id.*, at 103.

<sup>87</sup> *id.*, at 106-112.

<sup>88</sup> *id.*, at 112-117.

<sup>89</sup> *id.*, at 117-121.

<sup>90</sup> *id.*, at 121-126.

<sup>91</sup> *id.*, at 126-129.

Dissemination contemplates breach of confidentiality,<sup>94</sup> disclosure,<sup>95</sup> exposure,<sup>96</sup> increased accessibility of information,<sup>97</sup> blackmail,<sup>98</sup> appropriation,<sup>99</sup> and distortion of information.<sup>100</sup> Invasion includes intrusion<sup>101</sup> and decisional interference.<sup>102</sup>

This familial relationship conception of privacy has been a useful organizing force in recent privacy discourse. It helps with the amorphous nature of privacy to take a bottom-up approach and describe the kinds of conduct usually associated with privacy incursions, as well as categorizing the conduct into discrete areas or themes. The one limitation of this approach is its focus predominantly on *conduct*. This is not a criticism of the theory, but rather an observation that its focus is on one salient aspect of privacy. Of course, this is not news to Professor Solove who has suggested other approaches to privacy, notably the idea of premising much new privacy discourse on the nature of relationships between members of society in generating expectations of privacy. In recent privacy scholarship, Solove and co-author, Professor Neil Richards, make comparisons with recent British privacy law<sup>103</sup> that historically draws on relationships of confidence for its theoretical justification.

The approach suggested in this article mirrors Solove's taxonomy in that it takes a bottom-up approach to privacy, drawing generalities from specifics. It also looks at relationships between different aspects of a privacy, but in this context the aspects are not classes of conduct, but rather elements of a privacy incursion that involve people, motivations, harms, remedies, and the kinds of information in question in a given scenario. The idea is to pull the lens further out than Solove does, to map the outer boundaries of privacy for the Internet age. Even though the framework proposed here is at a relatively high level of abstraction it is nevertheless a "bottom up" pragmatic approach. It draws its structure from current practical controversies about online privacy, and then builds generalities about the potential boundaries of online privacy based on those specifics.

### 3. Theories Proposing Specific Legal Reforms

---

<sup>92</sup> *id.*, at 129-133.

<sup>93</sup> *id.*, at 133-136.

<sup>94</sup> *id.*, at 136-140.

<sup>95</sup> *id.*, at 140-146.

<sup>96</sup> *id.*, at 146-149.

<sup>97</sup> *id.*, at 149-151.

<sup>98</sup> *id.*, at 151-154.

<sup>99</sup> *id.*, at 154-158.

<sup>100</sup> *id.*, at 158-161.

<sup>101</sup> *id.*, at 161-165.

<sup>102</sup> *id.*, at 165-170.

<sup>103</sup> Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN L REV 1049 (2000) (suggesting that tortious approaches to protecting privacy cannot be reconciled with the First Amendment, but that contractual approaches may avoid this criticism); See also Andrew McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L REV 887, 927 (2006); Neil Richards and Daniel Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 THE GEORGETOWN LAW JOURNAL 123 (2007).

The final set of privacy theories arises from recent literature that takes what might be described as a doctrinal approach to specific online privacy problems. Some of the leaders in this field in recent years have been Professor Avner Levin and Professor Sánchez Abril. They base their suggestions for law reform on detailed empirical work about the privacy expectations of the Web 2.0 generation.<sup>104</sup> Professor Sánchez Abril has further identified the breakdown of traditional notions of public versus private spaces online, and has noted that American privacy law is overly premised on notions of private physical spaces.<sup>105</sup> She has made a number of specific suggestions for reworking tort law in the digital age to take account of the shift to the digital world, with a particular focus on online social networking.<sup>106</sup>

Two of her more interesting suggestions involve reworking the public disclosure tort<sup>107</sup> for the world of online social networks,<sup>108</sup> and using contractual means to better protect sensitive health information disclosed and aggregated in digital forums.<sup>109</sup> The kinds of approaches to online privacy advocated by Professor Sánchez Abril are appealing in that they provide immediate, concrete, and well-reasoned solutions to specific privacy problems. Again, Professor Sánchez Abril, like Professor Solove, is taking a bottom-up, pragmatic approach to online privacy problems. Again, the limitations of her theories are that they only consider discrete pieces of the overall privacy matrix, albeit some extremely important pieces. Thus, the development of an umbrella approach to privacy may help to tease out connections between some of the specific practical puzzles identified in her work, and the work of others in a similar vein.

### III. MAPPING PRIVACY

The aim of the privacy map is to provide some useful guidance about the scope of online privacy problems in the Web 2.0 age while retaining sufficient flexibility to encapsulate new and evolving issues. Although the map takes a broad picture of privacy at a relatively high level of abstraction, it is nevertheless a bottom-up approach because it

---

<sup>104</sup> Avner Levin and Patricia Sánchez Abril, Two Notions of Privacy Online, 11 VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW \_\_ (forthcoming, 2009).

<sup>105</sup> Professor Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1, 3 (2007) (“Traditionally, privacy has been inextricably linked to physical space.”)

<sup>106</sup> *id.*; Professor Sánchez Abril, *A (My)Space of One’s Own: On Privacy and Online Social Networks*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY (2007); Professor Sánchez Abril and Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient’s Bill of Rights*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 244 (2008).

<sup>107</sup> Restatement (Second) of Torts, § 652D (“One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that: (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.”)

<sup>108</sup> Professor Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1, 28 (2007).

<sup>109</sup> Professor Sánchez Abril and Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient’s Bill of Rights*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 244 (2008).

draws from specific instances of privacy to develop more general abstractions. This approach may illuminate latent connections between what appear to be disparate types of privacy incursions. It should also help to identify gaps and inconsistencies in current privacy laws and policies, and to develop better privacy laws and policies for the future.

This article advocates the identification and development of six dimensions of privacy: (a) actors/relationships; (b) conduct; (c) motivations; (d) harms/remedies; (e) nature of information; and, (e) format of information. All of these elements are present in every privacy incursion, so in a sense they form a familial set of attributes that can be used to generate a privacy framework. The following discussion describes in more detail the issues that may be encapsulated within each of these dimensions, as well as ways in which the consideration of each dimension as part of a general privacy matrix may help in developing future privacy policy.

While this discussion as so far focused on drawbacks of existing laws - notably American tort laws - in the privacy context, it is important to recognize that the answer to Web 2.0 privacy problems is unlikely to be purely, or even predominantly, within the realm of legal discourse.<sup>110</sup> It is likely that other modes of regulation will provide more useful answers to online privacy problems than legal solutions.<sup>111</sup> Thus the identification and development of social norms, technological solutions, and market practices may do a better job of protecting online privacy than legal rules.<sup>112</sup> Of course, legal rules work in a variety of ways. They do not only constrain behavior by punishing infringers. They also serve communicative functions that reinforce desired behaviors. It is important to recognize this fact when considering the role of law in the overall online privacy matrix. While it is beyond the scope of this article to suggest specific legal and other solutions to the privacy problems identified here, much of that work is currently being done by scholars in the privacy field.<sup>113</sup>

## A. ACTORS/RELATIONSHIPS

The first dimension of privacy may be described as *actors/relationships*. It encapsulates all those involved in a privacy incursion – complainants, defendants, and third parties. It also incorporates the *relationships* between those actors. Obviously, any conduct that involves privacy involves actors. However, pre-Internet discourse was

---

<sup>110</sup> Lawrence Lessig, *The Architecture of Privacy*, 1 VANDERBILT J ENT L & PRAC 56 (1999); Jacqueline Lipton, “*We, the Paparazzi*”: *Developing a Privacy Paradigm for Digital Video*, forthcoming IOWA L REV, 2009.

<sup>111</sup> Jacqueline Lipton, “*We, the Paparazzi*”: *Developing a Privacy Paradigm for Digital Video*, forthcoming IOWA L REV, 2009.

<sup>112</sup> Lawrence Lessig, *The Architecture of Privacy*, 1 VANDERBILT J ENT L & PRAC 56 (1999); Jacqueline Lipton, “*We, the Paparazzi*”: *Developing a Privacy Paradigm for Digital Video*, forthcoming IOWA L REV, 2009.

<sup>113</sup> *id.*, McClurg, *supra* note \_\_\_\_, Grimmelman, *supra* note \_\_\_\_, Professor Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1 (2007); Professor Sánchez Abril, *A (My)Space of One’s Own: On Privacy and Online Social Networks*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY (2007); Professor Sánchez Abril and Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient’s Bill of Rights*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 244 (2008).

concerned largely with relationships between governments and individuals as the key actors in a privacy-threatening scenario.<sup>114</sup> To some extent, traditional discourse also involved relationships between the press and private individuals.<sup>115</sup> These concerns have definitely become more pronounced as increasingly intrusive recording devices such as telephoto camera lenses and long range microphones have become more prominent in the hands of the press. Of course, such advanced technology also raises concerns about uses that governments may make of such technologies.<sup>116</sup> Note that at this point of the inquiry we are not yet talking about the *activities* that governments and the press undertake with this technology. That comes in the next dimension. We are simply identifying the actors in a privacy incursion, their relationships to each other, and, importantly, how those relationships may be changing in a Web 2.0 society.

Even before the development of Web 2.0 technologies, Web 1.0 had exacerbated pre-digital privacy concerns. In the early days of the Internet, individuals became increasingly concerned about the use of digital information processing technologies by both governments and private institutions.<sup>117</sup> As noted earlier, the European Union Data Protection Directive was largely aimed at remedying some of these problems.<sup>118</sup> Again, the focus was on governmental and corporate uses of individuals' personal data, rather than with purely social or familial relationships.<sup>119</sup> Web 2.0 dramatically expands the kinds of relationships that may be implicated in privacy incursions. With the rise of Web 2.0 participatory technologies, individuals may be increasingly concerned about peer-to-peer privacy problems in settings such as wikis, blogs, social networks, and even online games. Thus, it is important to add to the *actors* dimension of privacy a whole new class of social relationships that were not particularly significant in previous privacy discourse.<sup>120</sup>

Another important issue raised by Web 2.0 relates to the need to define the relationships between actors. A number of commentators have pointed out that notions of friendship and acquaintance work very differently in Web 2.0 contexts than they have in the past.<sup>121</sup> Online networking technologies involve binary concepts of friendship: that

<sup>114</sup> *Mosley v News Group Newspapers*, [2008] EWHC 1777 (QB), at para 9 (noting that modern privacy values are now as much applicable between private actors as they historically were between individuals and public authorities).

<sup>115</sup> SOLOVE, ROTENBERG, and SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note \_\_\_\_, at 75 (noting historical concerns about privacy with respect to the media).

<sup>116</sup> *id.*, at 207 ("Throughout the twentieth century, technology provided the government significantly greater ability to probe into the private lives of individuals.")

<sup>117</sup> *Whalen v Roe*, 429 U.S. 589 (1977); *In re Doubleclick Privacy Litigation*, 154 F. Supp. 2d 497 (2001); *Dwyer v American Express*, 273 Ill. App. 3d 742 (1995).

<sup>118</sup> See discussion in Part II.A *supra*.

<sup>119</sup> Data Protection Directive, Art 3(2) ("This Directive shall not apply to the processing of personal data ... by a natural person in the course of a purely personal or household activity.")

<sup>120</sup> This was recognized by Judge Eady in *Mosley v News Group Newspapers Ltd*, [2008] EWHC 1777 (QB), at para 9 (acknowledging that modern privacy incursions are likely to involve disputes between private individuals).

<sup>121</sup> Grimmelman, *supra* note \_\_\_\_, at \_\_\_\_; Lipton, "We, the Paparazzi", *supra* note \_\_\_\_, at \_\_\_\_; Craig Wilson, *The Final Word: Sorry, Charlie, Imaginary Friends Come and Go*, June 9, 2009 (available at [http://www.usatoday.com/life/columnist/finalword/2009-06-09-final-word\\_N.htm](http://www.usatoday.com/life/columnist/finalword/2009-06-09-final-word_N.htm), last viewed on June 15,

is, a person is either your friend or not.<sup>122</sup> There is little latitude built in to current systems to distinguish between people you know and trust, and people you know less well and may not particularly trust with personal information. One journalist has recently referred to the multitude of contacts generated on Facebook as being akin to “imaginary friends”<sup>123</sup> – that is, friends who do not feature as real people in your life, much like the imaginary friends created in childhood for an artificial sense of company and companionship. Of course, technological capabilities could be developed in the future to accommodate more gradations of online friendship and to distinguish the “real” online friends from the imaginary.<sup>124</sup> However, for the present time, it is sufficient to appreciate that the concepts of actors and relationships may be different online than was previously the case, even in the age of Web 1.0.

Other new conceptions of actors and relationships necessitated by the age of Web 2.0 relate to new kinds of relationships individuals have with *businesses* and *governments*. In terms of relationships with businesses, individuals now engage in new contractual relationships with online service providers such as Facebook,<sup>125</sup> MySpace,<sup>126</sup> Second Life,<sup>127</sup> and Wikipedia.<sup>128</sup> These entities know that they will be dealing with private information on a daily basis. They generally adopt some form of privacy policy.<sup>129</sup> Individuals may also have their own expectations of privacy in the context of these relationships that may or may not conform with the terms of those policies. Again, these relationships between actors – this time usually individuals and corporate actors – are different from those that arose previously. Online social network providers obviously hold and deal with personal data, but in a very different context than most Web 1.0 businesses. These entities do not exist for the purpose of collating and processing individual information to engage in targeted marketing, unlike many Web 1.0 businesses before them. Thus, laws and norms from the Web 1.0 age about relationships involving private information may not fit the same mould as these new individual-corporate relationships. These kinds of relationships require closer examination in order to develop meaningful privacy boundaries.

Relationships between individuals and governments also change in the Web 2.0 world. In earlier times, government basically governed, and citizens were the governed. That was the nature of the relationship. If government collected or used personal information, there were certain accepted parameters, but it was always within the government-governed relationship. The advent of modern social networking technologies

---

2009) (noting that “friends” on social networking sites are very much like the imaginary friends of one’s childhood days).

<sup>122</sup> SOLOVE, *THE FUTURE OF REPUTATION*, *supra* note \_\_, at 202 (“social network sites often have a very loose concept of “friend.” The sites divide a person’s social universe into “friends” and everybody else.”)

<sup>123</sup> Wilson, *supra* note \_\_\_\_.

<sup>124</sup> Grimmelman, *supra* note \_\_, at \_\_\_\_.

<sup>125</sup> [www.facebook.com](http://www.facebook.com), last viewed on June 15, 2009.

<sup>126</sup> [www.myspace.com](http://www.myspace.com), last viewed on June 15, 2009.

<sup>127</sup> [www.secondlife.com](http://www.secondlife.com), last viewed on June 15, 2009.

<sup>128</sup> [www.wikipedia.org](http://www.wikipedia.org), last viewed on June 15, 2009.

<sup>129</sup> See discussion in Grimmelman, *supra* note \_\_, at \_\_\_\_; Lipton, “*We, the Paparazzi*”, *supra* note \_\_, at \_\_\_\_.

has changed this relationship in ways that have yet to be examined in terms of applicable norms and legal principles. In the 2008 presidential election in the United States, all major candidates established interactive presences on popular social networking sites, such as Facebook.<sup>130</sup> Although some use was made of early iterations of these technologies in the 2004 presidential election,<sup>131</sup> the timing of the 2008 election coincided more squarely with the rise of Web 2.0 and the ability of candidates to be truly interactive with their supporters.

President Obama, in particular, made unprecedented use of these technologies in his campaign,<sup>132</sup> and his use of Web 2.0 technologies has continued into his presidency.<sup>133</sup> As candidates become government officials, however, an interesting phenomenon is occurring with respect to their use of online social networks. In the campaign context, individuals were able to “friend” candidates on services like Facebook and to be involved in the campaigns and receive information in that context. However, once the candidates become the government, does this relationship with supporters change by necessity? Professor Danielle Citron has recently commented on the problems that arise when the government has in its hands personal information about private individuals that it may have obtained over a social networking site when a supporter “friended” a candidate. She raises some interesting questions about the relationship between the governed and the government when the relationships developed in the campaigning context are translated to the governing context:

“When we interact with Government on private social media sites like Facebook or YouTube, have we implicitly forsaken any privacy in those communications? Does the President and his helpers get to collect personal data we post on our Facebook profiles and scurry back to agency information systems for processing, say data mining programs looking for threats to critical infrastructure or data matching programs looking for dead beat dads? On the one hand, we gave up that information voluntarily: if we set our privacy settings on Facebook accordingly, we know that what we tell our friends is “out of the bag” so to speak. On the other hand, do we really expect that the President, as my friend, is going to take my data and use it for purposes other than what his Facebook page promotes: conversations with the President about public policy, not whether we pay child support or engage in antisocial activities?”<sup>134</sup>

---

<sup>130</sup> See discussion in *From Domain Names to Video Games: The Rise of the Internet in Presidential Politics*, 86 DENVER UNIVERSITY LAW REVIEW 693 (2009).

<sup>131</sup> *id.*

<sup>132</sup> *id.*

<sup>133</sup> Danielle Citron, *President Obama’s Facebook Friends: Web 2.0 Technologies and Privacy*, Concurring Opinions, (April 29, 2009), available at [http://www.concurringopinions.com/archives/2009/04/president\\_obama\\_2.html#more](http://www.concurringopinions.com/archives/2009/04/president_obama_2.html#more), last viewed on May 10, 2009. See also <http://www.whitehouse.gov/>, last viewed on June 15, 2009.

<sup>134</sup> Danielle Citron, *President Obama’s Facebook Friends: Web 2.0 Technologies and Privacy*, Concurring Opinions, (April 29, 2009), available at

Of course, the changing nature of the relationships between private individuals and successful candidates for office post-election also has positive aspects for a representative democracy. As Professor Citron acknowledges, online social networking technology can add an important level of transparency between government and private individuals.<sup>135</sup> Regardless of the pros and cons of this phenomenon, the implications for a large scale map of privacy are that we need to investigate ways in which relationships change in the Web 2.0 world between individuals and governments, and the impact this may have on our reasonable expectations of privacy vis-à-vis the government. Of course examining actors and relationships in isolation does not tell us a lot about what an overall map of privacy should look like. However, it does tell us that the actors involved in privacy-threatening conduct, and the relationships between them are dramatically changing in the digital age. This will impact on what can be considered a reasonable expectation of privacy in the Web 2.0 age.

## B. CONDUCT

The second aspect of the privacy map involves privacy-threatening *conduct*. This refers to the types of activities individual actors may engage in that threaten privacy in one way or another. This aspect does not require a tremendous amount of explication as it has been so comprehensively developed in Professor Solove's work.<sup>136</sup> The idea here is a categorization of the various different kinds of conduct that might infringe an individual's expectations of, or rights to, privacy. Professor Solove's taxonomy of privacy effectively achieves this, breaking down privacy-threatening conduct into four distinct categories: (a) information collection; (b) information processing; (c) information dissemination; and, (d) invasion.<sup>137</sup> These categories break down further into the sub-categories described above.<sup>138</sup>

It is important to recognize a distinction between activities that involve actual *intrusions* into an individual's private space – such as those contemplated in Professor Solove's fourth category – from those that involve *uses* of information. *Uses* of information include collection/aggregation, processing, and dissemination. In other words, at a meta-level, *uses* would encapsulate Professor Solove's first three categories – collection, processing, and dissemination. The reason that an overarching map of privacy should distinguish between invasion, on the one hand, and use, on the other, is that most current laws tend to fall on one or the other side of this broad division. There is a distinct

---

[http://www.concurringopinions.com/archives/2009/04/president\\_obama\\_2.html#more](http://www.concurringopinions.com/archives/2009/04/president_obama_2.html#more), last viewed on May 10, 2009.

<sup>135</sup> *id.* (“President Barak Obama has [6,239,925](#) Facebook friends. To be sure, this friendship has its privileges. FOPs can post questions on the economy and vote on others' submissions and questions. Have we awoken to a new era of participatory democracy where Web 2.0 technologies mediate conversations between the Executive Branch (and maybe the President himself as he reportedly reads selected public mail weekly) and the interested Facebook friendly public? Do these social media technologies tap public participation in ways that e-Rulemaking proponents envisioned but to date has not? Quite possibly.”)

<sup>136</sup> SOLOVE, UNDERSTANDING PRIVACY, *supra* note \_\_\_\_.

<sup>137</sup> *id.*, at 103.

<sup>138</sup> See discussion in Part II.B.2 *supra*.

group of laws concerned with *invading another's physical space* in order to gather information,<sup>139</sup> and another broad group of laws concerned with *unauthorized use* of that information.<sup>140</sup>

It is important to recognize that in the Web 2.0 context, the distinction even between these two broad categories of *gathering* and *use* of private information is breaking down. Typical conduct on social networks or blogs or wikis, for example, may involve simultaneously gathering and using information. For example, sending a “tweet” over Twitter about oneself or one’s friend may be regarded as gathering the information and broadcasting (ie using) it simultaneously. Thus, it is important to appreciate that *conduct* for the purposes of the privacy map can be examined at various levels of abstraction. The more detailed level evident in Professor Solove’s taxonomy will likely prove to be very useful in formulating specific laws for particular categories of privacy-threatening conduct. The higher levels of abstraction may be useful in thinking about ways in which categories of privacy-threatening conduct are beginning to break down or merge together in the Web 2.0 era.

Future privacy theorists may have to grapple with the question of whether to maintain a distinction between *invasion* and *use* of personal information if the two forms of conduct are realistically converging. In particular, future work in this area should probably focus more on the *use* side of the equation than was the case in the past. While many pre-Internet laws focused on privacy *invasions*,<sup>141</sup> the greatest harms in the present age often come from unauthorized uses of private information online.<sup>142</sup> This is because one of the key contributions of modern technologies is the ability to collate and broadcast large volumes of information globally at the push of a button. This challenges expectations of privacy in ways previously unimaginable. As Professor Sánchez Abril has noted, “In today’s legal and technological world, telling one can literally mean telling the world.”<sup>143</sup>

<sup>139</sup> See, for example, Cal. Civ. Code §1708.8 (aimed at curbing intrusive recordings of individuals in private spaces); Restatement (Second) of Torts, § 652B (“One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”)

<sup>140</sup> For example, Restatement (Second) of Torts, § 652C (“One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.”); §652D (“One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that: (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.”); §652E (“One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if: (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.”)

<sup>141</sup> See, for example, Cal. Civ. Code §1708.8 (aimed at curbing intrusive recordings of individuals in private spaces).

<sup>142</sup> See discussion in SOLOVE, THE FUTURE OF REPUTATION, *supra* note \_\_\_\_, at 1-4.

<sup>143</sup> Patricia Sánchez Abril, *A (My)Space of One’s Own: On Privacy and Online Social Networks*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 73, 80 (2007).

A graphic example of this fact arises from the fairly constant outcry over Google Street View, part of the popular global mapping service promulgated by the search engine Google.<sup>144</sup> Google creates its street views by using three dimensional video cameras mounted on vehicles that drive through the streets of cities and towns taking pictures to be used on the popular mapping service.<sup>145</sup> Many have complained that this practice is an infringement of individual privacy in the home.<sup>146</sup> However, Google representatives generally counter that they are not taking pictures of anything that cannot be observed from a public street so they are not infringing privacy rights.<sup>147</sup> The difference in opinion must be explained not with reference to the actual image gathering, but rather its global dissemination, along with the *permanence* of the information when stored online.

While Google is undoubtedly correct that it is only gathering information that anyone could legally gather in a public place, what distinguishes Google's conduct is its subsequent use and ongoing availability of the information. Today's technology enables dissemination and storage of those images on a scope and scale never before imaginable. While before there was a fair amount of practical obscurity<sup>148</sup> of information gathered in a public place, today the potential for immediate global dissemination of that information is unparalleled by anything that occurred in the past. Once the information is available online, it is impossible to put the genie back in the bottle. An image subject can never be sure how many people have accessed and stored the image in question. Even dissemination of images taken in public places by media conglomerates in the past had less of a broad reach, and less of a quality of permanence, than information posted on Google Maps.

---

<sup>144</sup> Google's website boasts that Street View enables users to "explore neighborhoods at street level – virtually" (see [http://maps.google.com/help/maps/streetview/index.html#utm\\_campaign=en&utm\\_source=en-ha-na-us-google-svn&utm\\_medium=ha&utm\\_term=google%20street%20view](http://maps.google.com/help/maps/streetview/index.html#utm_campaign=en&utm_source=en-ha-na-us-google-svn&utm_medium=ha&utm_term=google%20street%20view), last viewed on June 15, 2009).

<sup>145</sup> LOWE, GOOGLE SPEAKS, *supra* note \_\_\_, at 193-194 (describing the mechanics of Google Street View).

<sup>146</sup> *id.*, at 193 ("Some people became alarmed when they realized Google Street View cameras could zoom in so closely that in one case, people could be seen inside the house. Aaron and Christine Boring, an American couple, unsuccessfully sued Google for \$25,000 for showing their house on Google Street View."); 194 ("The small northern German town of Molfsee – not at all happy at the prospect of becoming part of Street View – anticipated the arrival of Google's fleet of dark-colored Opel Astras with cameras on top. The photography vehicles already had shown up in other parts of Germany, snapping photographs for Google Street View. The 5,000 citizens of Molfsee took fast action, getting the local council to pass a road traffic act that would require Google to get a permit for the picture-taking. Local politicians then refused to issue the permit. Other parts of Germany were considering similar ordinances."); 195 ("In Japan, a group of lawyers and professors asked Google to suspend its Street View service there. "We strongly suspect that what Google has been doing deeply violates a basic right that humans have," said Yasuhiko Tajima, a professor of constitutional law at Sophia University and head of The Campaign Against Surveillance Society. "It is necessary to warn society that an IT giant is openly violating privacy rights, which are important rights that the citizens have, through this service.")

<sup>147</sup> LOWE, GOOGLE SPEAKS, *supra* note \_\_\_, at 194 (noting Google's response to a claim of privacy infringement with respect to its Google Street View service: "It usually is not against the law to photograph a house from the street, as long as the photographer does not trespass on private property.")

<sup>148</sup> MILLS, *supra* note \_\_\_, at 56 ("The upshot of technology and the increased supply and demand for information is a massive amount of information that is easily accessible. That which was lost in "practical obscurity" is available online and instantly.")

### C. MOTIVATIONS

Another important and perhaps less well understood dimension of online privacy relates to *motivations* of actors involved in privacy threatening conduct. There is also the associated question of the relevance of motive to the availability and nature of legal remedies. Clearly, some motivations for privacy incursions are laudable - or at least necessary or tolerable - in a democratic society. Incursions by the press into individual privacy in matters of public interest may be one obvious example.<sup>149</sup> In countries like the United States, this kind of motivation generally attracts legal and constitutional protection under the First Amendment. Of course, in the United States and other jurisdictions, there is always a fine line between distinguishing what is truly in the public interest from what may simply be interesting to the public.<sup>150</sup> Thus, a potential defendant's motivations may be relevant here.

For example, it is possible that a journalist's motivations in producing an article that is titillating but short on true public interest might be taken into account by a court in determining whether or not the conduct should be protected. This has been the case in recent British privacy litigation where a new free speech right<sup>151</sup> must now effectively be balanced against a new privacy right.<sup>152</sup> In *Mosley v News Group*,<sup>153</sup> the court spent a significant amount of time examining a journalist's motivations and conduct in developing a story that invaded the complainant's privacy and caused him much humiliation and embarrassment.<sup>154</sup> This inquiry was framed as being an important part of the public interest determination.<sup>155</sup>

Some motivations for privacy incursions may fall short of being in the public interest, but may be innocent or, at most, careless. Much social discourse is likely to fall within this context. This may have particular resonance for online social networks where there is much gossipy conduct, a large amount of which is thoughtless or at least without a malevolent intent, even if it ultimately harms, humiliates, or embarrasses someone. Again, disclosures of personal information thus motivated will often be protected by the First Amendment, providing that the information disclosed is not false. Commentators

---

<sup>149</sup> LOWE, GOOGLE SPEAKS, *supra* note \_\_\_\_, at 194-5 (“While Google software apparently blurs license plate numbers and faces [on Street View] so as to make them unrecognizable, and anyone who appears in a picture can request that the picture be removed, those safeguards do not seem to be enough for many people. Street View easily can provide other damaging information, and, especially when combined with buildings viewed from above by satellite, could be quite useful to stalkers or anyone with criminal intent.”)

<sup>150</sup> *Mosley v News Group Newspapers, Ltd*, [2008] EWHC 1777 (QB), para 31 (“It has repeatedly and rightly been said that what engages the interest of the public may not be material which engages the public interest.”)

<sup>151</sup> European Convention on Human Rights and Fundamental Freedoms, Art 10, imported into British law under the Human Rights Act, Eng. (1998).

<sup>152</sup> European Convention on Human Rights and Fundamental Freedoms, Art 8, imported into British law under the Human Rights Act, Eng. (1998)

<sup>153</sup> [2008] EWHC 1777 (QB).

<sup>154</sup> *id*, at paras 79-97 (judge analyzing conduct of journalist with respect to participants in erotic party).

<sup>155</sup> *id*, paras 153-171.

have begun to raise questions about these kinds of disclosures. Questions include the extent to which an information subject may have been the author of her own doom by failing to take reasonable steps to maintain the privacy of sensitive information.<sup>156</sup>

Counter to that, some have queried whether the First Amendment should play a significant role in protecting the ability of individuals to speak in a harmful, embarrassing, or gossipy way about each other online.<sup>157</sup> In other words, where the social value of the disclosure is minimal, and the privacy harm to an individual is potentially significant, should the First Amendment really trump the individual's privacy interests in these kinds of scenarios? Of course, this line of reasoning raises the question whether the right to free speech should include a right of privacy, rather than being juxtaposed against it.<sup>158</sup> Alternatively, it raises the question of whether shifting the balance, and allowing privacy to trump free speech in social or gossipy contexts, would create a culture of censorship contrary to the goals of the First Amendment.<sup>159</sup>

Another obvious motivation for behaviors that impinge on individual privacy is financial profit. This has traditionally been an easier inquiry for courts and legislatures. However a privacy right may be defined, there seems to be some general unease with the notion that a person or institution may make an uninvited and unauthorized profit from the private details of another's life – whether those details are conceived in terms of an aspect of personhood, a property right, or a dignitary right. Legislatures and courts have developed actions aimed at this kind of conduct in the past. They include: (a) the misappropriation tort in the United States;<sup>160</sup> (b) the right of publicity in the United States;<sup>161</sup> (c) American statutes aimed predominantly at curbing unauthorized newsgathering activities of the paparazzi;<sup>162</sup> (d) breach of confidence actions in the United Kingdom;<sup>163</sup> and, more recently, (e) privacy rights in the United Kingdom and throughout Europe established under Article 8 of the European Convention on Human Rights and Fundamental Freedoms.

It seems clear that an actor's motivations are properly regarded as an integral part of a broad privacy map. Motivations can have a significant impact on the ways in which courts, legislatures, and society analyze privacy-threatening conduct. Commentators

---

<sup>156</sup> Jacqueline Lipton, *Privacy Rights vs Architects of Our Own Doom*, May 10, 2009, Concurring Opinions (available at <http://www.concurringopinions.com/archives/2009/05/privacy-rights-vs-architects-of-our-own-doom.html>, last viewed on June 15, 2009).

<sup>157</sup> Jacqueline Lipton, "We, the Paparazzi", *supra* note \_\_\_\_, at \_\_\_\_.

<sup>158</sup> SOLOVE, *THE FUTURE OF REPUTATION*, *supra* note \_\_\_\_, at 130 (noting that both privacy and free speech are aspects of individual autonomy and need not be juxtaposed against each other in an "either or" balance).

<sup>159</sup> *id.*, at 126-127 (discussion of view that free speech is incompatible with privacy).

<sup>160</sup> Restatement (Second) of Torts, § 652C ("One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.")

<sup>161</sup> GILSON ON TRADEMARKS, at § 2.16[1] ("The right of publicity ... is the right of an individual to control the commercial use of his or her name, likeness, signature, or other personal characteristics."). See also MILLS, *supra* note \_\_\_\_, at 173-177 (discussing technical differences between the privacy misappropriation tort and the right of publicity tort).

<sup>162</sup> Cal. Civ. Code §1708.8 (aimed at curbing intrusive recordings of individuals in private spaces).

<sup>163</sup> See discussion in Richards and Solove, *supra* note \_\_\_\_.

have noted that courts are prepared to take a defendant's motivations into account when ascertaining whether a legally actionable privacy incursion has taken place.<sup>164</sup> Of course, public interest motivations will likely be protected by the First Amendment at least in the United States, while commercial motivations are generally less protected. However, the growing category of purely gossip or social motivations is less clear-cut. This category will need to garner more attention in the future by law and policy-makers as such conduct increases exponentially in the Web 2.0 age.

## D. HARMS/REMEDIES

### 1. Harms

What are the possible *harms* that may result from privacy-intrusive conduct? And what *remedies* are appropriate to redress those harms? Potential privacy harms are many and varied, and some are more readily cognizable as legally actionable than others. This may well have to change in the Web 2.0 age. Privacy harms in the online world can include: shame, embarrassment, ridicule, humiliation, economic loss, or perhaps even some damage to the person by way of physical<sup>165</sup> or psychological harm.<sup>166</sup> These are obviously harms to the person as opposed to harms to society at large. Nevertheless, privacy incursions may also cause more general societal harms in the sense of creating a culture of unease where people feel insecure about their personal information.<sup>167</sup>

The most readily remedied privacy harms in the pre-Web 2.0 era related to economic loss compensable by way of damages.<sup>168</sup> This may be a result of the misappropriation of an individual's private persona, as with the misappropriation privacy tort,<sup>169</sup> the right of publicity,<sup>170</sup> or identity theft.<sup>171</sup> Alternatively, some compensatory

---

<sup>164</sup> Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1, 36 (2007) ("Evidence of outrageous, intentional, and systematic campaigns to harass, discredit, or embarrass have been widely held to indicate invasions of privacy".)

<sup>165</sup> JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET AND HOW TO STOP IT*, 211 (2008) ("The famed "Bus Uncle" of Hong Kong upbraided a fellow bus passenger who politely asked him to speak more quietly on his mobile phone. The mobile phone user learned an important lesson in etiquette when a third person captured the argument and then uploaded it to the Internet, where 1.3 million people have viewed one version of the exchange .... Weeks after the video was posted, the Bus Uncle was beaten up in a targeted attack at the restaurant where he worked.")

<sup>166</sup> Wired News Report, *Star Wars Kid Files Lawsuit*, July 24, 2003, WIRED, available at <http://www.wired.com/culture/lifestyle/news/2003/07/59757>, last viewed on July 23, 2008 ("Ghyslain was so teased about the video, he dropped out of school and finished the semester at a children's psychiatric ward, according to a lawsuit filed in the Raza's hometown of Trois-Rivières, Quebec.")

<sup>167</sup> SOLOVE, *THE DIGITAL PERSON*, *supra* note \_\_\_\_, at 97 ("[T]he invasion conception's focus on privacy invasions as harms to specific individuals often overlooks the fact that certain privacy problems are structural – they affect not only particular individuals but society as a whole.")

<sup>168</sup> SOLOVE, *THE FUTURE OF REPUTATION*, *supra* note \_\_\_\_, at 122 (noting that while litigation is primarily about economic damages, many litigants bring claims for other reasons, such as to vindicate their reputation or seek an apology).

<sup>169</sup> Restatement (Second) of Torts, § 652C ("One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.")

<sup>170</sup> GILSON ON TRADEMARKS, at § 2.16[1] ("The right of publicity ... is the right of an individual to control the commercial use of his or her name, likeness, signature, or other personal characteristics."). See

damages might be paid for breaches of confidence involving personal information where an unauthorized profit has been made in breach of an obligation of confidence. In recent years, the breach of confidence action in the United Kingdom has been expanded to encapsulate relationships between plaintiffs and defendants where there are no clear express or implied *ex ante* agreements of confidentiality between the parties.<sup>172</sup>

Courts and legislatures have been slow to compensate plaintiffs for non-monetary harms resulting from a privacy incursion.<sup>173</sup> This may be because it is too difficult for courts to quantify such harms.<sup>174</sup> Alternatively, it may be because courts are wary of putting a high price on truthful speech for fear of chilling expression and creating a culture of censorship. Another explanation for the lack of judicial recognition of non-monetary privacy harms relates to the dearth of privacy actions brought before courts. Individuals who have faced shame, humiliation, or embarrassment as a result of the public dissemination of truthful information may have a variety of practical reasons for declining to bring a legal action, even if a cause of action is technically available. Many individual plaintiffs may not have the financial wherewithal or the time to litigate to protect their privacy.<sup>175</sup> More worrying, the private individual would have to relive the shame and embarrassment of the damaging information being entered into the public record during the course of court proceedings.<sup>176</sup> On top of this, the bringing of a privacy-based action is effectively an admission by the plaintiff that the information in question is true.

As noted by Judge Eady in the *Mosley* case, unlike a defamation suit which can have a restorative nature by publicly disclaiming the information in question and by imposing a monetary penalty for the disclosure, a privacy action emphasizes the truth of the information.<sup>177</sup> The judge also noted the difficulties inherent in attempting to quantify a loss of privacy. Such losses cannot really be compared meaningfully with any losses suffered as a result of a physical injury or even a defamation claim.<sup>178</sup> There is also again the question about the extent to which a judge should take into account a plaintiff's own complicity in the privacy harm. There is very little guidance for judges as to what are realistic precautions for an individual to be expected to take with respect to

---

also MILLS, *supra* note \_\_\_, at 173-177 (discussing technical differences between the privacy misappropriation tort and the right of publicity tort).

<sup>171</sup> See discussion in SOLOVE, ROTENBERG, and SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note \_\_\_, at 696-700.

<sup>172</sup> See discussion in Richards and Solove, *supra* note \_\_\_.

<sup>173</sup> Although this may be gradually changing at least in some jurisdictions. See, for example, *Mosley v News Group Newspapers Ltd*, [2008] EWHC 1777 (QB) (£60,000 damages awarded in breach of privacy action in the United Kingdom).

<sup>174</sup> *id.*, at para 231 (“it has to be accepted that an infringement of privacy cannot ever be effectively compensated by a monetary award. Judges cannot achieve what is, in the nature of things, impossible.”)

<sup>175</sup> *Mosley v News Group Newspapers Ltd*, [2008] EWHC 1777 (QB), para 230 (“Claimants with the degree of resolve (and financial resources) of Mr Max Mosley are likely to be few and far between.”)

<sup>176</sup> SOLOVE, THE FUTURE OF REPUTATION, *supra* note \_\_\_, at 120-121 (difficulties of plaintiffs in privacy actions having to be publicly identified on the court record).

<sup>177</sup> *Mosley v News Group Newspapers Ltd*, [2008] EWHC 1777 (QB), para 214 (distinguishing between damages for defamation and damages for infringement of privacy rights).

<sup>178</sup> *id.*

the protection of her own sensitive data. In *Mosley*, for example, the judge considered whether the plaintiff should have been expected to have been more careful with information about his sexual proclivities after he had been warned by friends that someone may be watching him.<sup>179</sup>

Extra-legal remedies may be equally problematic in practice. For example, private companies that provide services to protect individual reputations online, such as Reputation Defender,<sup>180</sup> may have perverse economic incentives when it comes to protecting individual privacy and reputation.<sup>181</sup> These services make money out of victims of online defamation and privacy incursions. If they were too effective in their stated aims of protecting individual reputations online, they could ultimately put themselves out of business. Thus, they arguably have a vested interest in the continuing culture of lack of respect between individuals about each others' online reputations.<sup>182</sup> It may be that the development of new market forces to combat online reputational and privacy harms could alleviate some of these perceived problems. The establishment of a *pro bono* reputation defense service would be an obvious example. Such a service could be funded by public or private donations or by the government. Pro bono law and technology clinics may be developed to this end.

The *harm* dimension of the privacy map is important because the ultimate goal of any law, policy, or practice aimed at protecting privacy in the age of the maturing Internet will have to deal with actual harms suffered by individuals online. In particular, in the world of social networking, and blogs, courts and legislatures will have to be sensitive to the likelihood that many of the harms suffered are not of the traditional economic nature which is usually the focus of our legal system. This may suggest that, with respect to the *harm* dimension of privacy, more thought needs to be given not only to the *nature* of harms that might be legally compensable, but also to the *ways* in which those harms are redressed.

To alleviate some of the perceived problems with reliance on public judicial proceedings, perhaps some form of closed trial could be established for certain types of privacy claims that relate to sensitive personal information. Alternatively, there may be other forms of dispute resolution, such as private mechanisms established by governments or private organizations. Some of the organizations that support blogs, wikis, and online social networks may think about setting up a dispute resolution arm for privacy claims. And there is of course the option mentioned above with respect to other market solutions – like new forms of reputation defence service being set up that do not

---

<sup>179</sup> *id.*, at para 225-226.

<sup>180</sup> See discussion in SOLOVE, THE FUTURE OF REPUTATION, *supra* note \_\_\_\_, at 192 (describing Reputation Defender as “a company that helps people find and remove harmful information about themselves online.”)

<sup>181</sup> See discussion in Ann Bartow, *Virtual Women*, forthcoming HARVARD JOURNAL OF LAW AND GENDER, 2009 (discussing the problem that Reputation Defender benefits from online harassment of women because they make money from cleaning up women's reputations online and have done some marketing directed at helping women who are subject to harassment online).

<sup>182</sup> *id.*

have economic incentives based on the volume of privacy-threatening and reputation-damaging conduct online.

## 2. Remedies

The harm question is inextricably linked with the question of an appropriate *remedy* – which is why the two are treated together here in this first cut of a privacy map, even though future work might do well to separate them. Obviously, compensatory damages have a useful remedial aspect, but they are also difficult to quantify in practice, and may lead to concerns about chilling speech. If the plaintiff’s real concern is with shame or embarrassment, and perhaps associated psychological harm, monetary damages may not in fact be an appropriate remedy. A plaintiff may rather seek some form of takedown remedy<sup>183</sup> directed at the most salient websites hosting relevant information. Of course, this would not be a perfect remedy because of the permanent and viral nature of information online.<sup>184</sup> At least it would be a statement that a privacy right had been infringed and would serve a somewhat remedial function as well as a communicative function to the online community about appropriate conduct with respect to privacy. It would probably have less of a chilling effect on speech than a damages award or criminal fine.

Alternatively - or additionally - a plaintiff may seek an apology from the person at the root of the privacy breach. That may be the person who originally gathered the private information or who first disseminated it online - to the extent that they are not the same person. An apology would be remedial and would signal the bounds of appropriate online behavior without attempting to put a monetary price on speech. Both the takedown and public apology options may be more appropriate than monetary remedies for yet another reason. The imposition of a financial penalty on an individual speaker for infringing someone’s privacy may be pretty useless in practice. If the individual defendant is impecunious, she knows that she can get away with the speech without paying the price.

Over the Internet, there may also be significant problems asserting jurisdiction over a foreign defendant in order to bring a privacy claim and impose a monetary remedy – a problem that may not be so pronounced with some private online dispute resolution mechanisms or reputation defense services. With respect to a deep-pocketed corporate defendant, a monetary penalty could also be relatively useless in practice because the penalty would have to be very high for it to make an impact on, say, a major media corporation. Presumably, damages for breach of privacy should be less than for defamation – because the sanction against the dissemination of false information should be more stringent than the sanction for disclosure of truthful information.<sup>185</sup> Thus, courts

---

<sup>183</sup> This could be modeled on the notice and takedown provisions in the Copyright Act – 17 U.S.C. § 512; see also discussion in Lipton, “*We, the Paparazzi*”, *supra* note \_\_\_\_, at \_\_\_\_.

<sup>184</sup> See discussion in Lipton, “*We, the Paparazzi*”, *supra* note \_\_\_\_, at \_\_\_\_.

<sup>185</sup> See discussion in *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), paras 212-215 (comparing damages for privacy and defamation claims).

may be limited in terms of the ability to make effective orders for privacy damages against both individual and corporate defendants.

The consideration of harms and remedies as distinct elements of an overall map of online privacy is useful in suggesting some future directions in which laws and policies could be developed to better meet the privacy-protecting needs of online communities. It may ultimately be a good idea to separate out *harms* and *remedies* into separate subcategories of a privacy map as noted above. However, for present purposes they have been considered together to make clearer the links between them, and to emphasize the fact that currently available remedies are not a particularly good fit for the kinds of harms currently arising in the Web 2.0 world. Of course, as noted above, it may be the case that the law in general is not the mainstay of privacy protection in the future. Private services relating to dispute resolution and reputation protection may be a better remedial fit for the needs of the Web 2.0 generation. One of the advantages of the privacy map is that the distinct harms arising in this generation, and the nature of appropriate remedies becomes more obvious when considered in the context of such an over-arching snapshot of digital privacy.

## E. NATURE OF INFORMATION

While the previous aspects of the privacy map have related predominantly to the active part of a privacy incursion in terms of actors, conduct, motivations, and harms, the last two aspects relate to the focal point of many privacy inquiries – the nature and format of the information in question. These two aspects of information are distinct from each other, even though they are related. Inquiries about the *nature* of information refer to the substance or content of the information, while inquiries about the *format* of information deal with differences in the digital file formats in which information is gathered and disseminated online. With regard to format, there are clear qualitative differences between the impact of different file formats – such as text, audio, video, and multi-media formats – on an audience.<sup>186</sup> These differences are discussed in the next section.

To date different legal systems have taken varying approaches to questions involving the *nature* of private information. The European Union Data Protection Directive takes a broad view of the nature and scope of personal information that should be protected from privacy-threatening conduct. The Directive defines personal data as:

---

<sup>186</sup> JON MILLS, *PRIVACY: THE LOST RIGHT*, 35-37 (2008) (noting the importance of recognizing that information available through different modes of communication - such as text, audio tape, still images, and video recordings – have different impacts on privacy); 238 (“courts may be more inclined to protect against intrusive images than intrusive words”); 263 (describing British courts’ readiness to extend privacy protections to photographs, but not to textual descriptions of particular misconduct); JOHN PALFREY and URS GASSER, *BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES*, 43 (2008) (“Photographs are no longer just tangible items to be mailed to friends and family – they are computer bytes easily spread across the Internet. These friends, too, upload the pictures to their own photo-sharing sites ...”); *Mosley v News Group Newspapers*, [2008] EWHC 1777 QB, at paras 16-23 (noting qualitative difference between video and text information in the privacy context); *Campbell v MGN*, [2004] UKHL 22, at paras 155-156 (noting qualitatively greater privacy harm that could occur as a result of dissemination of video images as compared with a textual account of the information in the journalist’s story).

“any information relating to an identified or identifiable natural person”.<sup>187</sup> Further, it singles out certain classes of information for additional protections over and above the general provisions of the Directive on data processing.<sup>188</sup> In this vein, Article 8 provides that: “Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”<sup>189</sup> Thus, the Directive attempts to be as future-proof as possible by broadly conceiving protections for personal information generally, and overlaying those basic protections with additional protections for particularly sensitive information.

American law paints a different picture of privacy with respect to the nature of information protected. American law comprises a series of piecemeal statutes that relate to specific protections for discrete classes of information – such as financial<sup>190</sup> or health information.<sup>191</sup> The downside of this approach in the age of Web 2.0 technologies is that it is less future-proof than the European Union approach because the classes of data protected are so limited. This has advantages and disadvantages. The obvious advantage is that the laws do not pose the risk of catching conduct not originally contemplated by the drafters – and perhaps chilling speech in the process. The disadvantage is that these laws are not intended to and will not automatically cover new privacy threats as they arise in various new online forums, such as online social networks.

In developing a map of online privacy, it is important for law and policy makers to consider the question as to what kinds of information require protection, and how that protection should be achieved in practice.<sup>192</sup> Some information has generally been regarded as more sensitive than other information in nature – including certain health<sup>193</sup>

---

<sup>187</sup> Art 2(a).

<sup>188</sup> Art 8.

<sup>189</sup> Art 8(1).

<sup>190</sup> See, for example, Fair Credit Reporting Act, Pub L No 90-321.

<sup>191</sup> See, for example, Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d-6(a)).

<sup>192</sup> An example of a court being particularly sensitive to the nature of personal information disclosed in public arose in the British House of Lords case of *Campbell v MGN Limited*, [2004] UKHL 22. This case involved a newspaper publishing a story about supermodel Naomi Campbell and her battle against drug addiction. In the case, the information in question was divided into five different substantive elements relating to the story and the judges were mindful of addressing each part of the substance individually in its application of the British breach of confidence action to the facts of the case. See *Campbell v MGN Limited*, [2004] UKHL 22, at para 23 (describing the five different substantive aspects of the information in question as: “(a) the fact of Miss Campbell’s drug addiction; (2) the fact that she was receiving treatment; (3) the fact that she was receiving treatment at Narcotics Anonymous; (4) the details of the treatment – how long she had been attending meetings, how often she went, how she was treated within the sessions themselves, the extent of her commitment, and the nature of her entrance on the specific occasion [photographed by the press photographer]; and (5) the visual portrayal of her leaving a specific meeting with other addicts.”)

<sup>193</sup> See, for example, *Re Bodil Lindqvist* (ECJ, Luxembourg, November 6, 2003, full text available at: <http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET>, last viewed on December 16, 2008) (involving information about a broken ankle as a health condition deserving of privacy); *Campbell v MGN Limited*, [2004] UKHL 22 (involving information about a supermodel’s drug addiction).

and financial information.<sup>194</sup> Nevertheless, even innocuous-seeming personal details can become greatly damaging if aggregated and disseminated online. This was certainly the case for “Dog Poop Girl”,<sup>195</sup> “Star Wars Kid”,<sup>196</sup> and “Bus Uncle”.<sup>197</sup> The nature of the information in all three cases was fairly innocuous, but led to serious harms in practice. In the Dog Poop Girl scenario, a Korean woman allowed her dog to poop on a subway train, and did not clean up the mess. This information - photographed and posted online – was aggregated with information about her identity, contact details, and workplace.<sup>198</sup> Ultimately, this led to a campaign of personal harassment that ultimately forced her to leave her job.<sup>199</sup>

The Star Wars kid scenario involved the unauthorized dissemination, and remixing, of a video of a young Canadian boy playing with a golf ball retriever as if it were a light sabre from the popular *Star Wars* movies.<sup>200</sup> Again, the information itself was innocuous in nature, but its dissemination and the resultant public humiliation caused the youth to require serious psychiatric treatment and to drop out of school.<sup>201</sup> Bus Uncle

---

<sup>194</sup> Balanced against this, courts in a number of jurisdictions have gone to great lengths to identify classes of information that are more important to disclose to the public despite the potential disclosure of private information that may be associated with that information: *Campbell v MGN*, [2004] UKHL 22, at para 148 (“There are undoubtedly different types of speech, just as there are different types of private information, some of which are more deserving of protection in a democratic society than others. Top of the list is political speech. The free exchange of information and ideas on matters relevant to the organisation [sic] of the economic, social and political life of the country is crucial to any democracy. Without this, it can scarcely be called a democracy at all. This includes revealing information about public figures, especially those in elective office, which would otherwise be private but is relevant to their participation in public life. Intellectual and educational speech and expression are also important in a democracy, not least because they enable the development of individuals’ potential to play a full part in society and in our democratic life. Artistic speech and expression is important for similar reasons, in fostering both individual originality and creativity and the free-thinking and dynamic society we so much value. No doubt there are other kinds of speech and expression for which similar claims can be made.”)

<sup>195</sup> JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET AND HOW TO STOP IT*, 211 (2008) (describing incident where woman refused to clean up her dog’s mess on a subway car in Korea and her life was subsequently ruined when photographs of the incident and additional information about her were posted online).

<sup>196</sup> Wired News Report, *Star Wars Kid Files Lawsuit*, July 24, 2003, WIRED, available at <http://www.wired.com/culture/lifestyle/news/2003/07/59757>, last viewed on July 23, 2008 (“Ghyslain was so teased about the video, he dropped out of school and finished the semester at a children's psychiatric ward, according to a lawsuit filed in the Raza's hometown of Trois-Rivières, Quebec.”); ZITTRAIN, *supra* note \_\_\_, at 212 (“The student who made the [Star Wars kid] video has been reported to have been traumatized by its circulation...”)

<sup>197</sup> ZITTRAIN, *supra* note \_\_\_, at 211 (“The famed “Bus Uncle” of Hong Kong upbraided a fellow bus passenger who politely asked him to speak more quietly on his mobile phone. The mobile phone user learned an important lesson in etiquette when a third person captured the argument and then uploaded it to the Internet, where 1.3 million people have viewed one version of the exchange .... Weeks after the video was posted, the Bus Uncle was beaten up in a targeted attack at the restaurant where he worked.”)

<sup>198</sup> SOLOVE, *THE FUTURE OF REPUTATION*, *supra* note \_\_\_, at 1-2.

<sup>199</sup> ZITTRAIN, *supra* note \_\_\_, at 211.

<sup>200</sup> SOLOVE, *THE FUTURE OF REPUTATION*, *supra* note \_\_\_, at 44-48.

<sup>201</sup> Wired News Report, *Star Wars Kid Files Lawsuit*, July 24, 2003, WIRED, available at <http://www.wired.com/culture/lifestyle/news/2003/07/59757>, last viewed on July 23, 2008 (“Ghyslain was so teased about the video, he dropped out of school and finished the semester at a children's psychiatric ward, according to a lawsuit filed in the Raza's hometown of Trois-Rivières, Quebec.”); ZITTRAIN, *supra*

incurred serious physical injury as a result of information spread on the Internet about his talking too loudly on a cellphone on a bus and ignoring requests from other passengers to be quiet.<sup>202</sup> Again, the information itself was fairly innocuous, but its online use led to great harm.

Pre-Web 2.0 conceptions of privacy do not generally cover innocuous information of this kind. Thus, questions about the *nature* of information to be protected in the digital age should be incorporated into a privacy framework along with a recognition that the boundaries of protected information may well need to be broader than previously contemplated. Of course, many privacy incursions involving innocuous information do not lend themselves to particularly grave injuries requiring legal or other redress. However, as the above examples illustrate, some disclosures of even innocuous information can be particularly harmful. Distinguishing between these two types of situations – innocuous information causing harm and innocuous information that does not cause harm – may require detailed thought in future privacy policy. The privacy map suggested here may help to ascertain relationships between nature of information, resultant harm, and appropriate remedy when attempting to make draw such distinctions in the future.

## F. FORMAT OF INFORMATION

The final aspect of the privacy map is the idea of the digital file *format* of the information in question. This is an important area of privacy that has received little attention in privacy discourse to date. The reason to factor in *format* is that privacy harms can differ significantly depending on the format of the information. The impact of information released in some forms can be very different from the impact of information released in other formats.<sup>203</sup> For example, a textual description of a car accident can have less of an emotional impact on the recipients of that information than a visual depiction of the car accident. This situation arose in a recent case of a young woman who was horrifically mutilated and killed in a car accident. Photographs of the accident scene were leaked by the police and disseminated over the Internet with various macabre captions added, much to the dismay of the young woman's family.<sup>204</sup> The impact of the

---

note \_\_\_, at 212 (“The student who made the [Star Wars kid] video has been reported to have been traumatized by its circulation...”)

<sup>202</sup> ZITTRAIN, *supra* note \_\_\_, at 211.

<sup>203</sup> JON MILLS, *PRIVACY: THE LOST RIGHT*, 35-37 (2008) (noting the importance of recognizing that information available through different modes of communication - such as text, audio tape, still images, and video recordings - have different impacts on privacy); 238 (“courts may be more inclined to protect against intrusive images than intrusive words”); 263 (describing British courts’ readiness to extend privacy protections to photographs, but not to textual descriptions of particular misconduct); JOHN PALFREY and URS GASSER, *BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES*, 43 (2008) (“Photographs are no longer just tangible items to be mailed to friends and family - they are computer bytes easily spread across the Internet. These friends, too, upload the pictures to their own photo-sharing sites ...”); *Campbell v MGN*, [2004] UKHL 22, at para 72 (“The publication of a photograph cannot necessarily be justified by saying that one would be entitled to publish a verbal description of the scene...”)

<sup>204</sup> Daniel Solove, *Family Privacy Rights in Death-Scene Images of the Deceased*, April 27, 2009, Concurring Opinions (available at [http://www.concurringopinions.com/archives/2009/04/family\\_privacy.html](http://www.concurringopinions.com/archives/2009/04/family_privacy.html), last viewed on June 16, 2009).

pictures was much more powerful and caused much more emotional harm to the family than a text-based description of the accident standing alone.<sup>205</sup>

Other situations have arisen involving differing impacts of the same information in different formats. With respect to a media corporation's request to access and broadcast audio tapes of the final moments in the Space Shuttle Challenger before its explosion, the court noted that releasing an audio tape could lead to much greater emotional distress to the families of those killed than simply releasing the transcripts (which NASA had been prepared to do).<sup>206</sup> In the recent *Mosley* litigation in Britain, the court was also mindful that the defendant newspaper could have run its story about the plaintiff's sexual proclivities in text format without having to resort to publishing splashy photographs of the people involved, and without having to post videos of the plaintiff's activities online.<sup>207</sup> In this case, the court ultimately found that even the text based publication infringed the plaintiff's privacy rights.<sup>208</sup> However, the judge took pains to distinguish between the different levels of harm that may be caused by the release of different file formats relating to the same information.<sup>209</sup>

The same impulse was evident in British House of Lords decision involving supermodel Naomi Campbell and a published story about her battle with drug addiction.<sup>210</sup> Several of the judges made comments about the fact that the story could have been published without photographs of Ms Campbell entering or leaving a Narcotics Anonymous meeting.<sup>211</sup> The addition of the photograph was not necessary for the story. Even the dissenting judges on this point noted that photographs are qualitatively different from text in the information they convey to the recipient.<sup>212</sup>

Today, more and more sophisticated recording technology is in the hands of the government, the press, private corporations, and private individuals. People can quickly,

<sup>205</sup> *id.*

<sup>206</sup> *New York Times v NASA*, 782 F.Supp 628 (1991).

<sup>207</sup> *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), para 16 ("Sometimes there may be a good case for revealing the fact of wrongdoing to the general public; it will not necessarily follow that photographs of "every gory detail" also need to be published to achieve the public interest objective.")

<sup>208</sup> *id.*, at para 134 ("In light of the strict criteria I am required to apply, in the modern climate, I could not hold that any of the visual images, whether published in the newspaper or on the website, can be justified in the public interest. Nor can it be said in this case that even the information conveyed in the verbal descriptions would qualify.")

<sup>209</sup> *id.*, at para 21 ("it should not be assumed that, even if the subject-matter of the meeting on 28 March was of public interest, the showing of the film or the pictures was a reasonable method of conveying that information. In effect, it is a question of proportionality."). See also discussion in *Campbell v MGN*, [2004] UKHL 22, at para 60 ("The relatively anodyne nature of the additional details is in my opinion important and distinguishes this case from cases in which (for example) there is a public interest in the disclosure of the existence of a sexual relationship (say, between a politician and someone whom she has appointed to public office) but the addition of salacious details or intimate photographs is disproportionate and unacceptable. The latter, even if accompanying a legitimate disclosure of a sexual relationship, would be too intrusive and demeaning.")

<sup>210</sup> *Campbell v MGN*, [2004] UKHL 22.

<sup>211</sup> *id.*, at paras 121-122; 155-156.

<sup>212</sup> *id.*, at para 31 ("In general photographs of people contain more information than textual description. That is why they are more vivid. That is why they are worth a thousand words.")

easily and cheaply create sophisticated multi-media files that may intrude into others' private lives.<sup>213</sup> While sometimes the disclosure of private information is in the public interest, the determination of whether the disclosure should be permitted or sanctioned must now take into account the format of the information as well as the nature of the information, and the motivations of the actors. It may be that in many cases, a textual description of an event would serve the public interest, but a graphical depiction is unnecessary and would cause disproportionate harm to innocent people. It is necessary for questions about the *format* of private information to play a significant role in the development of a map of privacy for the Web 2.0 environment.<sup>214</sup>

#### IV. CONCLUSIONS

The privacy map makes new contributions to digital privacy discourse, but also suffers from some limitations including the fact that the map in and of itself is not intended to provide specific solutions to Web 2.0 privacy problems. The aim is to create a framework within which such solutions might be more easily and cohesively developed. The idea of the map is to delineate some boundaries within which scholars, courts, and legislatures can work to identify in a more organized way some current and future challenges for privacy law. Although the framework presented here does not provide concrete solutions to privacy problems, it does illustrate how much broader the privacy matrix is today, and will be in the future, from what it has been in the past. It is also implicit in this discussion that the development of legal rules should not necessarily be the mainstay of future privacy law, although laws can provide remedies in some cases, and can certainly serve a communicative function about acceptable privacy norms.

In constructing the privacy map, the author agrees with Professor Solove that it is unnecessary to look for a common denominator to provide a unifying theoretical basis for all of privacy discourse. It may well be more useful at the present time to take a pragmatic bottom-up approach to Web 2.0 privacy problems. Professor Solove did this in the creation of his privacy taxonomy. His work enables scholars, courts, and legislatures to get a better picture of how different classes of privacy-threatening conduct relate to each other in the digital age in particular. The aim is similar for the privacy map presented here. The goal is to help organize future thought about privacy by drawing generalities from specific instances of privacy-threatening scenarios, albeit at a higher level of abstraction than Solove's approach.

Unlike other areas of law, the boundaries of privacy have historically been vague and unclear, and the relationships between different kinds of privacy-threatening conduct have been difficult to define. By grouping together categories of actors/relationships, conduct, motivations, harms/remedies, and investigations of the nature and the format of personal information, this framework allows a more comprehensive and cohesive approach to future privacy questions. It encourages courts and commentators not to lose sight of these aspects of a privacy incursion and the often subtle relationships between

---

<sup>213</sup> Solove, *The Future of Reputation*, *supra* note \_\_\_\_, at 45-46 (describing the multimedia versions created of the *Star Wars Kid* video and shared publicly over the Internet).

<sup>214</sup> See discussion in Lipton, "*We, the Paparazzi*", *supra* note \_\_\_\_.

them. Creating a framework that encourages all of the constituent elements of a privacy incursion to be examined in concert with each other may help to develop appropriate legal and social responses to today's privacy problems. At the end of the day, this approach may assist in the development of a more cohesive and comprehensive approach to privacy for the Web 2.0 generation, and whatever follows.