2010

Mapping Online Privacy

Jacqueline D. Lipton
University of Pittsburgh School of Law, jdl103@pitt.edu

Follow this and additional works at: https://scholarship.law.pitt.edu/fac_articles

Part of the Civil Rights and Discrimination Commons, Communications Law Commons, Constitutional Law Commons, International Law Commons, Internet Law Commons, Legal History Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
Jacqueline D. Lipton, Mapping Online Privacy, 104 Northwestern University Law Review 477 (2010). Available at: https://scholarship.law.pitt.edu/fac_articles/183

This Article is brought to you for free and open access by the Faculty Publications at Scholarship@PITT LAW. It has been accepted for inclusion in Articles by an authorized administrator of Scholarship@PITT LAW. For more information, please contact leers@pitt.edu, shephard@pitt.edu.
MAPPING ONLINE PRIVACY

Jacqueline D. Lipton*


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

* 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. Additionally, the author would like to thank participants at the Cyberlaw 2.0: Legal Challenges of an Evolving Internet, the 9th Annual CIPLIT Symposium at DePaul University College of Law, October 15–16, 2009. The author also greatly benefited from comments made at faculty colloquium presentations of earlier drafts of this article at Osgoode Hall Law School, York University, Toronto, on November 5, 2009, and at Akron Law School, Akron, Ohio, on November 18, 2009. 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, Professor Michael Birnbaum, Mr Ryan Calo, and Professor Matthew Sag. The editors of the Northwestern University Law Review and, in particular, Kevin King, Rami Fakhouri, Peter Julian, and Gautam Huded, did a magnificent job throughout the editing process, and the author thanks them gratefully for all of their hard work in this context. All errors and omissions are my own.
Justice Scalia here refers to a class exercise assigned by Professor Joel Reidenberg of Fordham Law School. Professor Reidenberg had previously 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. In early 2009, one of Professor Reidenberg’s students posted a news report on the class discussion board about comments regarding digital privacy made by Justice Scalia. The Justice had said: “Every single datum about my life is private? That’s silly.” This inspired Professor Reidenberg to select Justice Scalia, rather than himself, as the focus of the class exercise for the semester.

After searching the Internet, Professor Reidenberg’s students compiled a dossier about Justice Scalia from publicly available materials which included some information about his family, both in text and image formats. The dossier was not made public, although Justice Scalia was informed of its existence. To Professor Reidenberg, this was a “teachable” moment. To Justice Scalia, it was an exercise in poor professorial judgment. Did it alter either man’s views 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. The Justice publicly stood by his own previous remarks on privacy. Nevertheless, the exchange

---

3 Id.
4 Hill, supra note 1.
6 Hill, supra note 1; Posting of Daniel Solove, supra note 2.
7 Hill, supra note 1; Posting of Daniel Solove, supra note 2.
8 Posting of Daniel Solove, supra note 2; see also Cohen, supra note 5 (using the phrase “teaching moment” to describe “lessons learned from real life that help illuminate an academic subject”).
9 Hill, supra note 1 (“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.” (quoting Justice Scalia) (internal quotation marks omitted)).
10 Posting of Daniel Solove, supra note 2; see also Cohen, supra note 5 (“Mr. Reidenberg was speaking [at an academic conference] about the loss of ‘practical obscurity,’ that is, the idea that certain personal information may always have been publicly available—down at the courthouse, say—but in reality was very hard to discover and disseminate.”).
11 Hill, supra note 1 (“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.” (quoting Justice Scalia) (internal quotation marks omitted)).
Mapping Online Privacy

sparked a vibrant online debate about privacy in the age of the maturing Internet—a useful starting point for this discussion.

We are now in an age in which online communications are much broader in scope, speed, and nature than during the early days of the Internet. With participatory Web 2.0 technologies, many more people than ever before have opportunities to gather, collate, and disseminate information about others globally at the push of a button. Privacy laws and policies have been slow to adapt to these new technologies. Of course, an obvious 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. As such, if we want laws to reflect societal expectations of privacy, it is simply too early to identify any—or at least 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 in seeking to develop a conception of the outer boundaries of digital privacy law. Specifically, this Article posits 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 be helpful to pull back the lens and see if it is possible to create a larger-scale outline of privacy. This broader perspective may help to illuminate the constituent elements of a privacy incursion, and the

---

12 See, e.g., id.; Posting of Daniel Solove, supra note 2; see also Cohen, supra note 5 ("Professor Reidenberg's comments at the conference were picked up by a Web site, Above the Law, and the genie was out of the bottle, speeded on its way with the headline 'What Fordham Knows About Justice Scalia.'").

13 DAVID KESMODEL, THE DOMAIN GAME 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 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").

14 Of course, privacy law is problematic in the best of times because it is aimed at restricting truth-ful speech about individuals, often in the face of powerful speech protections such as the First Amendment. Even in jurisdictions with strong legal protections for personal privacy, the balance between privacy and speech is difficult for courts. See, e.g., Mosley v. News Group Newspapers, [2008] EWHC (QB) 1777, [8]–[15], [2008] All E.R. (D) 322 (Eng.) (describing balance between free speech and privacy under Articles 8 and 10 of the European Convention on Human Rights and Fundamental Freedoms).

15 For example, privacy law is generally a matter of state law in the United States. See MATTHEW BENDER & CO, PERSONAL INJURY: ACTIONS, DEFENSES, DAMAGES § 120.01[1] (2010) (listing the various state actions for privacy throughout the United States).
interrelationships between those elements. In this context, the Article identifies six discrete aspects of privacy relating to: (1) actors--relationships; (2) conduct; (3) motivations; (4) harms--remedies; (5) nature of information; and (6) format of information.

Taken together, these elements can describe, at a relatively high level of abstraction, any given privacy-threatening scenario. Examining such scenarios through this multifocal lens might enable us to gain a better sense of what properly belongs within each element, and of the interactions between them. This approach 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 that may not otherwise become apparent. Part I highlights the limitations of current privacy law and theory in the context of Web 2.0. Part II develops an outline of privacy for Web 2.0 based on the six aspects of privacy described above. The Article concludes with a brief discussion of the contributions and limitations of this mapping approach in developing clearer and more cohesive privacy laws and policies for the future.

I. 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

Web 2.0 involves more voices than previous Internet technologies. Blogs, wikis, online social networks, and massively multiplayer online
games\textsuperscript{21} allow more people to communicate more information than ever before, both about themselves and about others—sometimes deliberately, and sometimes incidentally.\textsuperscript{22} This proliferation of new technologies 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 of personal information to create large-scale, text-based digital dossiers about individuals.\textsuperscript{23} These concerns 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.\textsuperscript{24}

Web 2.0 raises new challenges for privacy. With more voices online, there is a wider scope for privacy invasion. With more recording technologies readily at hand—such as cell phone cameras and text messaging services like Twitter\textsuperscript{25}—there is a wider scope for incidental gathering of

\begin{footnotesize}
\textsuperscript{19} LOWE, \textit{supra} note 13, 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"); DON TAPSCOTT \& ANTHONY D WILLIAMS, \textit{WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING} 13 (2008) (defining a "wiki" as "software that enables users to edit the content of Web pages").

\textsuperscript{20} LOWE, \textit{supra} note 13, at 292 (describing "social networking" as "[w]ebsites that allow people to share ideas, information, and images and to form networks with friends, family, or other like-minded individuals"); SOLOVE, \textit{THE FUTURE OF REPUTATION, supra} note 17, at 26 (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).

\textsuperscript{21} JENKINS, \textit{supra} note 18, at 289 ("Massively Multiplayer Online Role-Playing Games, an emerging genre that brings together thousands of people interacting through avatars in a graphically rich fantasy environment.").

\textsuperscript{22} TAPSCOTT \& WILLIAMS, \textit{supra} note 19, at 242-43 (describing social interactions between geographically dispersed coworkers whilst playing the online game Battlefield 2).


\textsuperscript{24} See, e.g., discussion of the European Union Data Protection Directive in notes 60–62 infra. The European Union Data Protection Directive specifically contemplates that problems may arise in applying its text-based provisions to more complex digital file formats. European Union Data Protection Directive 95/46, art. 33, 1995 O.J. (L 281) (EC), \textit{available at} http://aspe.hhs.gov/DATACNCL/eudirect.htm [hereinafter Data Protection Directive] ("The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.").

\textsuperscript{25} Twitter is a digital messaging service that describes itself as "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?" Twitter.com, \textit{What is Twitter?}, http://web.archive.org/web/20080724155350/http://twitter.com/ (last visited May 26, 2010). Twitter is described in Wikipedia.org as "a social networking and microblogging service that enables its users to send and read messages known as tweets. Tweets are text-based posts of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers who are known as followers." Wikipedia, \textit{Twitter}, http://en.wikipedia.org/wiki/Twitter (last visited May 26, 2010). 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. A further example of
\end{footnotesize}
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, or at least becoming more difficult to discern. Thus, any privacy laws premised on now-dated conceptions of a “reasonable expectation of privacy” are becoming more difficult to apply.

One of the most comprehensive privacy regulations implemented in the early days of the Internet was the European Union Data Protection Directive. 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.” While the Directive’s definitions of “personal data” and “processing” are broad, the implication is that the drafters were contemplating large scale text-based digital filing systems typically compiled by governmental and private institutions.

A “personal data filing system” is defined in the Directive as “any structured set of personal data which are accessible according to specific fast and easy digital recording technologies is found in the context of Facebook quizzes. See Ani L. Schwartz, Facebook: Protect My Privacy, SOCIAL ENTREPRENEURSHIP, Sept. 16, 2009, http://socialentrepreneurship.change.org/actions/view/facebook_protect_my_privacy (describing threats to privacy posed by Facebook quizzes).

26 Posting of Daniel Solove, supra note 2.

27 DANIEL SOLOVE, MARC ROTENBERG & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 33–34 (2d ed. 2006) [hereinafter SOLOVE ET AL., INFORMATION PRIVACY LAW] (noting that the “reasonable expectation of privacy” doctrine is derived originally from the Fourth Amendment of the U.S. Constitution).

28 Patricia Sánchez Abril, Recasting Privacy Torts in a Spaceless World, 21 HARV. J.L. & TECH. 1, 18 (2007) [hereinafter Sánchez Abril, Recasting Privacy Torts] (“In deciding privacy tort claims, courts are charged with determining whether there was a reasonable expectation of privacy in the space in question.”); see also RESTATEMENT (SECOND) OF TORTS § 652D cmt. c (1977) (discussing the tort of public disclosure of private facts and how the rule applies only against “unreasonable publicity, of a kind highly offensive to the ordinary reasonable man”).


30 Id. at art. 3(1).

31 Id. at 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.”).

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

33 See id. at art. 2(d) & (e) (defining, respectively, “controller” and “processor” of data terms as “a natural or legal person, public authority, agency or any other body”).

482
criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.” Although this definition could theoretically encompass an online social networking service like Facebook, the more natural fit 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 multiplayer game a “structured set of personal data which are accessible according to specific criteria”? Probably not. An online multiplayer game, like Second Life, may in fact contain personal facts about an individual—particularly if the individual’s identity associated with his or her avatar 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 keywords, the same will not be true of many multiplayer 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. New online technologies are not mere aggregated dossiers of personal data, but are virtual worlds which contain personal information in a variety of formats. While text-based data is easily searchable by keywords, other forms of data—such as audio and video files—are not easily searchable unless

34 Id. at art. 2(c).
36 For example, in a recent case of cyberbullying, a court struggled to apply computer trespass provisions of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2006), to conduct involving the creation of a fictitious persona on the Web 2.0 social networking service MySpace to harass and bully a teenage girl, Megan Meier, ultimately culminating in her suicide. Initially, the court held that the provisions of the CFAA would cover conduct of a MySpace user that contravened MySpace’s posted terms of service as the basis of violating the CFAA’s felony provision, id. § 1030(c)(2)(B)(ii), but the court later held that using CFAA’s misdemeanor provisions to enforce online terms of use would make the statute void for vagueness. United States v Drew, 259 F.R.D. 449, 451, 464 (C.D. Cal. 2009).
37 PALFREY & GASSER, supra note 18, at 28–29 (describing Second Life as a promising and popular virtual world where users can tailor the appearance of their avatars including skin color and the shape of their nose).
38 Id. at 20 (describing avatars as fake personas online which enable an individual to try out a new identity).
they are effectively tagged.\textsuperscript{39} Thus, newer Web 2.0 technologies that contain data in these varied formats may not be easily characterized as forums in which information is \textit{accessible according to specific criteria} for the purposes of the Directive.

The Directive has been applied fairly broadly to online activities. A good example is the case of \textit{In re Bodil Lindqvist}.\textsuperscript{40} In this case, 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.\textsuperscript{41} Furthermore, the court held that the disclosure of the personal information was not excused by the "purely personal activities" exception in the Directive.\textsuperscript{42} Nevertheless, the holding was limited to text-based information disclosed to the world at large on a publicly available website.\textsuperscript{43} It is not clear how private information disclosed in closed online networks—like Facebook or Second Life—would fare under this reasoning.\textsuperscript{44} It was clearly significant to the \textit{Bodil Lindqvist} court that the information was publicly available to an indefinite number of people on a generally accessible website.\textsuperscript{45} Additionally, as the \textit{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.\textsuperscript{46}

If European Union laws are potentially of limited application in the face of Web 2.0 technologies, how might American laws fare? After all, the European Union has some of the strongest legal privacy protections in the world.\textsuperscript{47} By contrast, the United States has never been particularly focused on protecting individual privacy. To the extent that American law

\textsuperscript{39} \textit{Id.} at 62 (tagging a nontext file allows it to be more easily searchable via the text in the tag); LOWE, supra note 13, at 292 (defining "tagging" as "[n]aming an image, file, or something on the Internet. It needs a name before you can search for it.").


\textsuperscript{41} \textit{Id.} ¶¶ 1–6.

\textsuperscript{42} Data Protection Directive, supra note 24, at 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.").

\textsuperscript{43} Data Protection Working Party, supra note 35, § 3.1.2 (noting that where an online social network member extends dissemination of information beyond selected friends to the public at large, she may become a "data controller" for the purposes of the Directive, and be subject to all of its restrictions on processing personal information).

\textsuperscript{44} 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.

\textsuperscript{45} Lindqvist, 2003 E.C.R. I-12971, ¶ 47.

\textsuperscript{46} For a more detailed discussion on how the Directive might apply to these kinds of file formats, see Jacqueline D. Lipton, Digital Multi-Media and the Limits of Privacy Law, 42 CASE W. RES. J. INT’L L. 551 (2010).

\textsuperscript{47} SOLOVE ET AL., INFORMATION PRIVACY LAW, supra note 27, at 869 (describing the European Union’s "omnibus" approach to protecting privacy).
has dealt with privacy at all, the protections have largely been restricted to government intrusions into privacy. Setting aside the limited development of the four privacy torts, there has not been much of an effort to protect individual privacy against private intrusions.

There are a variety of explanations as to why the United States has not developed stronger privacy protections. First, privacy law has typically taken a backseat to the First Amendment. While there is an express constitutional guarantee of free speech and a free press in the United States, there is no such guarantee of a right to privacy. Limited privacy rights have been read into certain sections of the Constitution, 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 with regard to truthful speech. 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

---

48 Id. at 207 (noting the particular tension between privacy and the government's law enforcement activities).
51 SOLOVE ET AL., INFORMATION PRIVACY LAW, supra note 27, at 132 ("The privacy torts exist in an uneasy tension with the First Amendment."); 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, 1051-55 (2000) (suggesting that tortious approaches to protecting privacy cannot be reconciled with the First Amendment, but that contractual approaches may avoid this criticism); Diane Leenheer Zimmerman, Is There a Right to Have Something to Say? One View of the Public Domain, 73 FORDHAM L. REV. 297, 348-49 (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." (footnotes omitted)).
52 SOLOVE ET AL., INFORMATION PRIVACY LAW, supra note 27, at 33 ("Although the United States Constitution does not specifically mention privacy, it has a number of provisions that protect privacy, and it has been interpreted as providing a right to privacy. In some instances, the First Amendment serves to safeguard privacy . . . . The Third Amendment protects the privacy of the home by preventing the government from requiring soldiers to reside in people's homes . . . . The Fourth Amendment provides that people have the right 'to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . .'").
53 Id. at 132 ("The privacy torts exist in an uneasy tension with the First Amendment."); SOLOVE, THE FUTURE OF REPUTATION, supra note 17, 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."); Volokh, supra note 51, at 1049; Zimmerman, supra note 51, at 348-49.
free speech guarantees—the idea of limiting truthful speech has been more problematic.54

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.55 It is difficult to quantify many privacy harms in this way. There may also be a sense that compensating privacy harms is problematic because often victims of privacy incursions may be complicit in their own misfortune.56 It is possible to argue that, at least in the pre-Internet world, individuals were, by and large, able to control the dissemination of their personal information. Thus, if they were careless about this information, they deserved what they got. In the offline 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 protection, it may be argued that she should not be regarded as having an expectation of privacy that the law should protect.

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 by using technological means such as cookies57 to track online purchases. Governments could require individuals to submit to the recording of sensitive information in centralized databases for various public policy programs.58 In the United States, courts generally found these computer-enabled dealings with personal information to be acceptable, or at least not violative of privacy rights.59 In contrast, such infringements were 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 con-

54 Sánchez Abril, (My)Space, supra note 49, at 79 (“The torts of defamation—libel and slander—do not apply if the information published was true or opinion, however harrowing. Thus, if the disclosure is true but nonetheless embarrassing, or meant for other audiences, these dignitary torts are inapplicable.” (footnote omitted)).
55 See infra note 188 and accompanying text.
57 In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502–03 (S.D.N.Y. 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.”).
sent. It also attempted to build in controls to ensure a subject's access to, and the accuracy of, 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, as well as potentially the common law privacy torts.

In the world of Web 2.0, existing laws are even more troublesome. Web 2.0 technologies break down the barriers between the public and private spheres in a much more pronounced way than their predecessors. 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 often lose the nuanced control they had over personal information in the past. For example, while the physical world accommodates gradations of relationships of friendship and trust—which certainly affects what is and is not disclosed to another person—some online social networks are binary. Either one is a "friend" or one isn't. Additionally, it is very difficult to refuse to accept a request to "friend" someone, and almost unbearable to "unfriend" them once they have been "friended." The temptation is often great online to "friend" large numbers of people who one has not actually met in the physical world. While some online social networks at least allow gradations of friendship that enable people to be careful about precisely what information is released to their online friends and acquaintances, often the users of these services are careless with their information, or that of others, in practice. 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.

---

60 Data Protection Directive, supra note 24, at art. 7 (setting out the data subject's consent as necessary for processing personal data unless the processing can be justified by necessity relating to performance of a contract, compliance with a legal obligation of the data controller, and so on).

61 Id. at art. 12 (requiring that data controllers provide access to personal information of data subjects).

62 Id. at art. 6(1)(d) (requiring accuracy of data processed by data controllers).


64 Restatement (Second) of Torts §§ 652A-E (1977).

65 Solove, The Future of Reputation, supra note 17, at 202 ("[S]ocial network sites often have a very loose concept of 'friend.' The sites divide a person's social universe into 'friends' and everybody else.").

66 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.").

67 See Data Protection Working Party, supra note 35, § 3.1.1 ("Typically, access to data (profile data, postings, stories . . .) contributed by a user [of an online social networking service] is limited to self-selected contacts. In some cases however, users may acquire a high number of third party contacts, some of whom he may not actually know.").
B. Privacy Theory

Privacy scholars have struggled to develop theories of privacy for Web 2.0 that make sense and can be translated into useful laws and policies. Some excellent work has been done in this area in recent years, and 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, others have attempted to categorize privacy-threatening conduct, and still others have talked more specifically about practical legal reforms that might better protect online privacy. This section briefly surveys current theoretical approaches and identifies their limitations with respect to delineating the outer boundaries of privacy. The current theories themselves are not problematic per se. However, there is, as yet, no attempt to outline the contours 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. This is a particularly important exercise in an era where there are increasing calls for legislatures to take actions more appropriately tailored to protecting privacy on a global scale in light of Web 2.0 developments.

A look at privacy from its outer boundaries may help to inform legislators faced with this daunting task. This approach may help law and policy makers identify the scope of Web 2.0 challenges for privacy and may illuminate areas that require the most immediate action.

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 long struggled with the nature of privacy. Indeed, the seminal article on privacy in the United States appeared in the *Harvard Law Review* in 1890.

---


69 See, e.g., 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.”).


71 See, e.g., NEIL ROBINSON, HANS GRAUX, MAARTEN BOTTERMANY & LORENZO VALERI, REVIEW OF THE EUROPEAN UNION DATA PROTECTION DIRECTIVE, at vii (May 2009), available at http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf ("Overall, we found that as we move toward a globally networked society, the [Data Protection] Directive as it stands will not suffice in the long term. While the widely applauded principles of the Directive will remain as a useful front-end, they will need to be supported by a harms-based back-end in order to cope with the growing challenge of globalisation and international data flows.”).

That article itself cited even earlier conceptions of privacy.\textsuperscript{73} As with any theory, existing conceptions of privacy have their shortcomings, a number of which relate generally to their notion of a privacy right, but some of which arise specifically out of their application to the Internet age.

One of today's leading privacy theorists, Professor Daniel Solove, has recently catalogued and critiqued the main pre-Internet privacy theories.\textsuperscript{74} His list includes: (1) Samuel Warren and Louis Brandeis's famous conception of privacy as the "right to be let alone";\textsuperscript{75} (2) the concept of privacy as a right to limit access to the self;\textsuperscript{76} (3) privacy conceived as secrecy;\textsuperscript{77} (4) privacy as control over personal information;\textsuperscript{78} (5) privacy as an aspect of personhood;\textsuperscript{79} and (6) privacy as control over intimate relationships.\textsuperscript{80} Having identified and critiqued existing theories, Professor Solove argues that each of these theories "fail on their own terms"\textsuperscript{81} because they do not "achieve the goal of finding the common denominator"\textsuperscript{82} upon which they are premised. He then goes on to suggest that privacy theory needs to be reconceptualized by avoiding the idea of a common denominator.\textsuperscript{83} In particular, he suggests that "the quest for a common denominator is a search for the holy grail"\textsuperscript{84} and that privacy discourse may be better served by developing "a new way to understand privacy."\textsuperscript{85} This Article, by mapping the outer boundaries and limitations of privacy law rather than searching for an internal logic, takes a step in the new direction advocated by Professor Solove.

Existing theories on the nature of a privacy right are extremely useful in a number of ways. They aid 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, 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 limits of privacy. Whether they focus on property, dignity, or relationships of confidence, they are trying to

\textsuperscript{73} Id. at 195 n.4 (citing \textit{THOMAS COOLEY, COOLEY ON TORTS} 29 (2d ed. 1888)).
\textsuperscript{74} SOLOVE, \textit{UNDERSTANDING PRIVACY}, supra note 69, at 12–38.
\textsuperscript{75} Id. at 15–18; Warren & Brandeis, supra note 72, at 194 (quoting \textit{THOMAS M. COOLEY, COOLEY ON TORTS} 29 (2d ed. 1888)).
\textsuperscript{76} SOLOVE, \textit{UNDERSTANDING PRIVACY}, supra note 69, at 18–21.
\textsuperscript{77} Id. at 21–24.
\textsuperscript{78} Id. at 24–29.
\textsuperscript{79} Id. at 29–34.
\textsuperscript{80} Id. at 34–37.
\textsuperscript{81} Id. at 38.
\textsuperscript{82} Id.
\textsuperscript{83} Id. at 38–39.
\textsuperscript{84} Id. at 38.
\textsuperscript{85} Id. at 39.
get to the inner kernel of a privacy right, not to its outer boundaries. Outer boundaries are also important, particularly for law and policy makers tasked with creating rules and regulations that appropriately address Web 2.0 privacy concerns. Any new approach to regulation must be sufficiently flexible to address specific harms without being too narrowly focused on individual privacy scenarios. A consideration of the outer boundaries of privacy assists legislators and other policy makers by creating some guidance as to how broadly any new law or policy should reach. It augments current approaches that focus on the inner boundaries of privacy regulation, such as Professor Solove's approach of identifying specific privacy harms and addressing them on a case-by-case basis as part of a related puzzle of digital age privacy problems.  

2. Theories Categorizing Privacy Harms.—Professor Solove's most significant contribution to privacy discourse to date has been his innovative approach to conceptualizing privacy. He has developed a taxonomy of privacy, which includes categories of conduct that implicate privacy harms. He has identified the relationships between these categories in terms of "family-resemblances" and advocates this approach over an attempt to discern a single underlying common denominator to unify privacy. Professor Solove's theory of privacy takes a bottom-up approach, drawing generalities from specific experiences. Rather than being "rigid and controlling," he advocates a framework that is "flexible and open
Mapping Online Privacy

Professor 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. The categories are: “(1) information collection, (2) information processing, (3) information dissemination, and (4) invasion.”

Collection contains subcategories of conduct relating to surveillance and interrogation. Processing contemplates aggregation, identification, insecurity, secondary use, and exclusion. Dissemination contemplates breach of confidentiality, disclosure, exposure, increased accessibility of information, blackmail, appropriation, and distortion of information. Invasion includes intrusion and decisional interference.

This familial-relationship conception of privacy has been a useful organizational tool in recent privacy discourse. Given the amorphous nature of privacy, it is helpful to take a bottom-up approach and describe the kinds of conduct usually associated with privacy incursions and to categorize the conduct into discrete areas or themes. The one limitation of this approach is that it focuses predominantly on specific conduct. This is not a criticism of the theory, but rather an observation that its focus is only 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 of the new privacy discourse on the role of interpersonal relationships in generating expectations of privacy. In recent privacy scholarship, Professor Solove and coauthor Professor Neil Richards make comparisons with new

93 Id.
94 Id.
95 Id. at 103-04.
96 Id. at 103.
97 Id. at 106-12.
98 Id. at 112-17.
99 Id. at 117-21.
100 Id. at 121-26.
101 Id. at 126-29.
102 Id. at 129-33.
103 Id. at 133-36.
104 Id. at 136-40.
105 Id. at 140-46.
106 Id. at 146-49.
107 Id. at 149-51.
108 Id. at 151-54.
109 Id. at 154-58.
110 Id. at 158-61.
111 Id. at 161-65.
112 Id. at 165-70.
British privacy law, which draws on relationships of confidence for its theoretical justification.113

3. *Theories Proposing Specific Legal Reforms.*—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. Two particular leaders in this field in recent years have been Professor 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.114 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.115 She has made a number of specific suggestions for reworking tort law to take account of the shift to the digital world, with a particular focus on online social networking.116

Two of Professor Sánchez Abril’s more interesting suggestions involve reworking the public disclosure tort117 for the world of online social networks,118 and using contractual means to better protect sensitive health information disclosed and aggregated in digital forums.119 The 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. As such, Professor Sánchez Abril, like Professor Solove, takes a bottom-up, pragmatic approach to specific online privacy problems. Again, one limitation of her theories is that they only consider certain discrete—albeit extremely important—pieces of the overall privacy matrix. They give specific guidance as to how best to rework the inner boundaries of privacy for Web 2.0 technologies. Nevertheless, it may be a useful exercise to augment these approaches with an examination of the outer bounds of privacy. The development of an umbrella approach to privacy may help to tease out connections between some of the specific practical puzzles identified in the earlier privacy literature that focuses predominantly on identifying and remediing specific privacy harms.

115 See Sánchez Abril, *Recasting Privacy Torts*, supra note 28, at 3 (“Traditionally, privacy has been inextricably linked to physical space.”).
117 RESTATEMENT (SECOND) OF TORTS § 652D (1977) (“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.”).
119 Sánchez Abril & Cava, *supra* note 70, at 268.
II. MAPPING PRIVACY

This Part suggests an outline for sketching the outer boundaries of privacy. Such an approach could help pinpoint more precisely where traditional notions of privacy are being pushed beyond their historical bounds and aid in determining 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.

The approach suggested here mirrors Professor Solove's taxonomy in the sense that it takes a bottom-up approach to privacy, drawing generalities from specifics. It also looks at relationships between different aspects of privacy, but in this context the aspects are not classes of conduct. Rather, they are 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 widen the lens further than Professor Solove does, in order 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. 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: (1) actors and relationships; (2) conduct; (3) motivations; (4) harms and remedies; (5) nature of information; and (6) 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 has so far focused on drawbacks of existing law—notably American tort law—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. It is likely that other informal modes of regulation will provide more useful an-

---

120 See Lawrence Lessig, The Architecture of Privacy, 1 VAND. J. ENT. L. & PRAC. 56, 62–64 (1999); Jacqueline D. Lipton, "We, the Paparazzi": Developing a Privacy Paradigm for Digital Video, 95 IOWA L. REV. 919 (2010).
answers to online privacy problems than legal solutions.\textsuperscript{121} Thus the identification and development of social norms, technological solutions, and market practices may do more to protect online privacy than new legal rules.\textsuperscript{122} Of course, legal rules work in a variety of ways. They not only constrain behavior by punishing infringers, but also serve communicative functions that reinforce desired behaviors. In fact, the review of the Data Protection Directive conducted in the European Union in 2009 emphasized the importance of legislators working together with business representatives, civil society representatives, and nongovernmental organizations in order to better address global privacy concerns in the Web 2.0 era.\textsuperscript{123}

\textbf{A. Actors and Relationships}

The first dimension of privacy may be described as \textit{actors and relationships}. It encapsulates all those involved in a privacy incursion—complainants, defendants, and third parties. It also incorporates the \textit{relationships} between those actors. Pre-Internet discourse was concerned largely with relationships between governments and individuals as the key actors in a privacy-threatening scenario.\textsuperscript{124} To some extent, the traditional discourse also involved relationships between the press and private individuals.\textsuperscript{125} These concerns have 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, the development of such advanced technology also raises concerns about how governments may use these technologies.\textsuperscript{126}

Even before the advent of Web 2.0, Web 1.0 technologies exacerbated predigital 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.\textsuperscript{127} As noted

\textsuperscript{121} See Lipton, supra note 120.
\textsuperscript{122} See Lessig, supra note 120, at 62–64; Lipton, supra note 120.
\textsuperscript{123} See, e.g., ROBINSON ET AL., supra note 71, at 13 (“The Article 29 Working Party should expand liaisons with business representatives, civil society representatives and Non-Governmental Organisation communities.”).
\textsuperscript{124} See Mosley v. News Group Newspapers, [2008] EWHC (QB) 1777, [9], [2008] All E.R. (D) 322 (Eng.) (noting that modern privacy values are now as applicable between private actors as they historically were between individuals and public authorities).
\textsuperscript{125} See SOLOVE ET AL., INFORMATION PRIVACY LAW, supra note 27, at 75 (noting historical concerns about privacy with respect to the media).
\textsuperscript{126} See id. at 207 (“Throughout the twentieth century, technology provided the government significantly greater ability to probe into the private lives of individuals.”). 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.
\textsuperscript{127} See, e.g., Whalen v. Roe, 429 U.S. 589, 591 (1977) (dealing with government-imposed legislation to collect certain sensitive information about drug prescriptions in a digital database); In re Double-click Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001) (involving the use of cookies to
Mapping Online Privacy

earlier, the European Union Data Protection Directive was largely aimed at remedying some of these problems.128 Again, the focus was on governmental and corporate uses of individuals' personal data, rather than purely social or familial relationships.129 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: those between private individuals.130

In this context, Web 2.0 potentially changes how the relationships between actors are defined. For example, questions arise as to whether it is appropriate to consider the large number of online contacts who a network user may never have met as "friends" or "peers." Lack of real personal ties with online friends may result in people being less careful about others' privacy when disseminating personal information about them. Additionally, one might consider whether in the Web 2.0 context, the dissemination of information online by private individuals on blogs and other platforms effectively turns these individuals into a new kind of amateur journalist.131 The journalism paradigm causes a number of potential difficulties in that amateur journalists are not governed by the codes of conduct to which professional journalists at least notionally subscribe. While it is possible that amateur journalists will develop online norms that may protect individual privacy, at least one commentator has doubted that it will be easy to regulate blogger conduct through norms.132

Other new conceptions of actors and relationships necessitated by the age of Web 2.0 relate to new kinds of relationships individuals have with

---

128 See supra notes 60-62.
129 Data Protection Directive, supra note 24, at 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.").
130 This was recognized by Judge Eady in Mosley v. News Group Newspapers, [2008] EWHC (QB) 1777, [9], [2008] All E.R. (D) 322 (Eng.) (acknowledging that some privacy incursions will involve disputes between private individuals).
132 Id. at 213 ("Developing norms that control amateur journalists' behavior may not be easy. These journalists by definition comprise a vast group of millions of diverse people rather than a well-defined profession. It may be difficult to find a set of principles that amateur journalists generally can agree on and internalize as norms. Moreover, the self-expression motives of amateur journalists suggest that they will tend to have libertarian views, or at least views incompatible with externally imposed order." (footnotes omitted)).
In terms of relationships with businesses, individuals now engage in new contractual relationships with online service providers such as Facebook, MySpace, Second Life, and Wikipedia. These entities know that they will be dealing with private information on a daily basis. They generally adopt some form of privacy policy. Individuals may also have their own expectations of privacy in the context of these relationships which may or may not conform with the terms of those policies. Other corporations, too, have new relationships with their customers online in the Web 2.0 age. Increasingly, corporations invite customers to become “fans” of particular products and services over networks such as Facebook. This is a new form of relationship between a business and its customers and its contours are not yet clear in terms of the information shared between the parties, and the appropriate boundaries of, for example, corporate use of customers’ information collected from an online fanbase.

All of these relationships between individuals and corporate actors are different from those that existed in the pre-Web 2.0 era. Online social network providers obviously hold and deal with personal data, but do so 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. Corporations that collect online “fans” also create new kinds of relationships with those people than was the case in the Web 1.0 era. The laws and norms developed for Web 1.0 about relationships involving private information between individuals and businesses may not be a good fit for these new individual–corporate relationships. These kinds of relationships require closer examination in order to develop meaningful privacy boundaries.

Relationships between individuals and governments have also changed in the Web 2.0 world. In earlier times, the relationship was basically a one-way street: with government governing and citizens being governed. 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 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

133 Facebook, http://www.facebook.com (last visited June 1, 2010).
137 See Lipton, supra note 120; see also Grimmelman, supra note 16, at 18–20 (discussing privacy of private user data held by search engines).
Mapping Online Privacy

popular social networking sites, such as Facebook. Although some use was made of early iterations of these technologies in the 2004 presidential election, the timing of the 2008 election coincided more squarely with the rise of Web 2.0 and the ability of candidates to truly interact with their supporters.

President Obama, in particular, made unprecedented use of these technologies in his campaign; his use of Web 2.0 technologies has continued into his presidency. 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 are able to "friend" candidates on services like Facebook and be involved in the campaigns and receive information in that context. However, once candidates are elected, this relationship changes. Does becoming part of the government necessitate this change? 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? Do 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?

Of course, the changing nature of the relationships between private individuals and successful candidates for office postelection also has positive aspects for a representative democracy. As Professor Citron acknowledges,

140 Id. at 699.
141 Id.
142 Danielle Citron, President Obama's Facebook Friends: Web 2.0 Technologies and Privacy, CONCURRING OPINIONS, Apr. 29, 2009, http://www.concurringopinions.com/archives/2009/04/president_obama_2.html#more, [hereinafter Posting of Danielle Citron]; see also The White House Homepage, http://www.whitehouse.gov (last visited June 1, 2010) (providing visitors with text, photo, and video content related to presidential activities, as well as the opportunity to link to other social networking sites, including Facebook, Twitter, MySpace, and LinkedIn).
143 Posting of Danielle Citron, supra note 142.
online social networking technology can add an important level of transparency between government and private individuals. Regardless of the pros and cons of this phenomenon, it has implications for a large-scale map of privacy. We need to investigate ways in which relationships change in the Web 2.0 world, 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. These changes will affect what can be considered a reasonable expectation of privacy in the Web 2.0 age.

Future law and policy makers considering the boundaries of appropriate privacy regulation will need to pay close attention to the nature of the relationships between the parties. As described here, these relationships are significantly changing in the Web 2.0 environment, and the changes in the nature of online relationships will implicate the kinds of privacy harms that may occur and the kinds of remedies that may be appropriate. Online friends may need to be encouraged, through laws and other regulatory modalities, to become attuned to the global harms that careless disclosures might cause. The potential for widespread harm in social relationships is more significant online than ever before. Additionally, laws may need to be developed to regulate the more journalistic impulses of private individuals who are not governed by professional journalism’s codes of conduct. All of this is putting to one side the significant challenges that Web 2.0 poses for the application of privacy laws to governments and corporations that now deal with private information in the context of very different relationships than has been the case in the past.

B. Conduct

The second dimension of the privacy map is privacy-threatening conduct. This refers to the types of activities individual actors may engage in that threaten privacy in one way or another. This dimension does not require a tremendous amount of explication, as it has been comprehensively developed in Professor Solove’s work. The idea here is to create a categorization of the various different kinds of conduct that might infringe an

\footnote{144} Id. ("President Bara[c]k 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.").

\footnote{145} See Ribstein, supra note 131, at 213 (noting practical difficulties of regulating the conduct of amateur journalists in the blogosphere).

\footnote{146} See SOLOVE, UNDERSTANDING PRIVACY, supra note 69.
individual's expectations of, or rights to, privacy. Professor Solove's tax-
onomy of privacy effectively achieves this, breaking privacy-threatening
conduct into four distinct categories: "(1) information collection, (2) infor-
mation processing, (3) information dissemination, and (4) invasion." These categories break down further into the subcategories described
above.\(^\text{148}\)

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—and those that involve uses of information. Uses of information include collection or 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 overarching map of privacy should distinguish between invasion and use because most current laws tend to fall on one side or the other of this broad division. There is a distinct group of laws concerned with invading another's physical space in order to gather information,\(^\text{149}\) and another broad group of laws concerned with the unauthorized use of that information.\(^\text{150}\)

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,\(^\text{151}\) the greatest harms in the present age often come from unauthorized uses of private information online.\(^\text{152}\) This chang-

\(^{147}\) Id. at 103.

\(^{148}\) See supra notes 97–112.

\(^{149}\) See, e.g., CAL. CIV. CODE § 1708.8 (West 2009) (aimed at curbing intrusive recordings of individuals in private spaces); RESTATEMENT (SECOND) OF TORTS § 652B (1977) ("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.").

\(^{150}\) See, e.g., 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."); id. § 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."); id. § 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 in which the other would be placed.").

\(^{151}\) See, e.g., CAL. CIV. CODE § 1708.8 (aimed at curbing intrusive recordings of individuals in private spaces).

ing focus results from one of the key contributions of modern technologies: the ability to collate and broadcast large volumes of information globally with the push of a button. In effect, many of the barriers which once protected information against invasion have now fallen. This technological shift 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.”

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. Google creates its street views by using omnidirectional cameras mounted on vehicles that drive through the streets of cities and towns, taking pictures to be used on the popular mapping service. Many have complained that this practice is an infringement of individual privacy in the home. However, Google representatives generally counter that because they are not taking pictures of anything that cannot be observed from a public street, they are not infringing privacy rights.

This difference in opinion must be explained not with reference to the supposed invasion—the actual image gathering—but rather the use: the permanent global dissemination of the images, along with the permanence

154 Google’s website boasts that Street View enables users to “[e]xplore the world at street level.” Google Maps, http://maps.google.com/help/maps/streetview/ (last visited June 1, 2010); see also Kara Rowland, Invasive New Technologies Alarming Parents, WASH. TIMES, July 28, 2008, at B3 (“The image available is the same as what one would see walking down a public street.”).
155 See LOWE, supra note 13, at 193–94 (describing the mechanics of Google Street View and the opposition it has produced).
156 See, e.g., 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.”); id. at 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 enacting similar ordinances.”); id. at 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 Yasuhiro 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.’”); Lora Pabst, North Oaks Tells Google Maps: Keep Out, STAR TRIBUNE, May 31, 2008, at 1A (“North Oaks’ unique situation, in which the roads are privately owned by the residents and the city enforces a trespassing ordinance, may have made it the first city in the country to request that the online search engine remove images from Google Maps.”).
157 LOWE, supra note 13, 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”).
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 the 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 of information gathered in a public place, today the potential for immediate global dissemination of that information is unprecedented. Once information is available online, it is impossible to put the genie back in the bottle. The subject of an image 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 a narrower reach, and less permanence, than information posted on Google Street View.

The changing nature of privacy-threatening conduct in the Web 2.0 age suggests that we now need to think about privacy very differently than we have in the past. This will again be a daunting task for legislators and other policy makers, such as judges and those who develop privacy-enhancing technologies. One question we might ask in this context is whether the traditional idea of "reasonable expectations of privacy" makes sense at all in the Web 2.0 age where technologies and new privacy-threatening practices are developing at an exponential rate. We may not have time to develop expectations of privacy that are reasonable before the new wave of privacy-threatening technologies develops and overtakes those expectations. This might militate against relying purely on law as the paradigmatic mode of privacy regulation in the future as it is likely that legislative developments will move too slowly to be of much use in the face of fast-paced technological change.

C. Motivations

Another important and perhaps less understood dimension of online privacy relates to motivations of actors involved in privacy-threatening

---

158 SOLOVE, THE FUTURE OF REPUTATION, supra note 17, at 4 ("Information that was once scattered, forgettable, and localized is becoming permanent and searchable.").
160 MILLS, supra note 68, 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.").
161 ROBINSON ET AL., supra note 71, at 16–19 (noting the challenges that fast-paced technology poses and suggesting the need for a multimodal approach to protecting privacy in the Web 2.0 age, involving the development of norms and technologies to enhance privacy along with clarification and better implementation of the EU Data Protection Directive).
conduct.\textsuperscript{162} 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.\textsuperscript{163} In countries like the United States, this kind of motivation generally attracts legal and constitutional protection under the First Amendment. Of course, there is always a fine line between distinguishing what is truly in the public interest from what may simply be interesting to the public.\textsuperscript{164}

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 in which a new free speech right\textsuperscript{165} must now effectively be balanced against a new privacy right.\textsuperscript{166} In Mosley v. News Group, 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.\textsuperscript{167} This inquiry was framed as being an important part of the public interest determination.\textsuperscript{168}

Some motivations for privacy incursions may fall short of being in the public interest but may be innocent or, at most, careless. A good deal of social discourse is likely to fall within this context, particularly in the context of online social networks which facilitate gossipy conduct, much of which is thoughtless or at least without malevolent intent, even if it ulti-

\textsuperscript{162} 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 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. See Sánchez Abril, Recasting Privacy Torts, supra note 28, at 36 (“Evidence of outrageous, intentional, and systematic campaigns to harass, discredit, or embarrass have been widely held to indicate invasions of privacy.” (footnote omitted)).

\textsuperscript{163} Google Street View is another example. Lowe, supra note 13, at 194–95 (“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.”).

\textsuperscript{164} Mosley v. News Group Newspapers, [2008] EWHC (QB) 1777, [31], [2008] All E.R. (D) 322 (Eng.) (“It has been repeatedly and rightly said that what engages the interest of the public may not be material which engages the public interest.”).


\textsuperscript{166} Id. at art. 8.

\textsuperscript{167} [2008] EWHC (QB) 1777, [79]–[97] (analyzing the motivation of a journalist’s conduct with respect to participants in erotic party).

\textsuperscript{168} Id. at [153]–[71] (analyzing whether the journalist lived up to the standard of “responsible journalism”).
mapping Online privacy approximately harms or humiliates someone. Again, disclosures of personal information thus motivated will often be protected by the First Amendment, providing that the information disclosed is not false. On the other hand, 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. 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? 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. 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.

Another obvious motivation for behaviors that impinge on individual privacy is financial profit, which 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: (1) the misappropriation tort in the United States; (2) the right of publicity in the United States; (3) American statutes aimed predominantly at curbing unauthorized newsgathering activities of the paparazzi; (4) breach of confidence actions in the United Kingdom; and, more recently, (5) privacy rights in the United Kingdom and throughout Europe established under Article 8 of the European Convention on Human Rights and Fundamental Freedoms.

169 See, e.g., Lipton, supra note 120.
170 Danielle Keats Citron, Cyber Civil Rights, 89 B.U. L. Rev. 61, 101 (2009) (noting that unbridled freedom of expression can cause greater harms than humiliation or embarrassment and that verbal online attacks can generate the fear of physical violence, exclusion and subordination).
171 SOLOVE, THE FUTURE OF REPUTATION, supra note 17, at 130 (noting that both privacy and free speech are aspects of individual autonomy and need not be juxtaposed against each other).
172 ld. at 126–27 (discussing the view that free speech is incompatible with privacy).
173 See RESTATEMENT (SECOND) OF TORTS § 652C (1977) (“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.”).
174 See ANNE GILSON LALONDE ET AL., I GILSON ON TRADEMARKS § 2B.01 (2009) (“The right of publicity is the right of [an individual] to control the commercial use of his or her name, visual likeness, signature symbol, or other personal characteristics.”); see also MILLS, supra note 68, at 173–77 (discussing technical differences between the privacy misappropriation tort and the right of publicity tort).
175 E.g., CAL. CIV. CODE § 1708.8 (West 2009) (aimed at curbing intrusive recordings of individuals in private spaces).
176 See discussion in Richards & Solove, supra note 113, at 158–73.
177 See European Convention on Human Rights, supra note 165, art. 8.
Legislators and policy makers will face some difficult choices related to the nature of the relationship between the parties to a privacy incursion. For example, the question arises whether careless and damaging disclosures of personal information between online peers should be excused, or should garner a lower level of remedy, because we need to develop a notion of "reasonable expectations of privacy" between peers that puts a greater onus on individuals to keep personal information secret even from their online friends to avoid such harms. On the other hand, should the onus be on private individuals to protect information of others that they happen to know through virtual relationships with those people? Privacy regulators will face myriad difficult choices going forward in trying to ascertain the types of relationships, and classes of conduct within those relationships, that merit legal redress to the extent that they involve careless privacy incursions. Additionally, as individuals increasingly become amateur journalists, questions will arise as to how best to balance privacy rights against freedom of expression outside the context of professional journalism. The privacy map outlined in this Article may be useful in drawing out some of the connections between relationships, conduct, motivations, and harms that will be important in ascertaining the scope of future privacy regulations in the Web 2.0 context.

D. Harms and 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 uncertain legal landscape may well have to develop more discernable features in the Web 2.0 age. Privacy harms in the online world can include shame, embarrassment, ridicule, humiliation, economic loss, or perhaps even more serious damage to the person by way of physical or psychological harm.\(^{181}\)

\(^{178}\) Ribstein, \textit{supra} note 131, at 187 (noting the trend towards private individuals becoming amateur journalists in the blogging context).

\(^{179}\) Data Protection Working Party, \textit{supra} note 35, § 3.1.2 (contemplating the need to balance rights to privacy and free expression between users of online social networks).

\(^{180}\) JONATHAN ZITTRAIN, \textit{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." (footnotes omitted)).

\(^{181}\) Id. at 212 ("The student who made the [Star Wars kid] video has been reported to have been traumatized by its circulation . . . ."); Wired News Report, \textit{Star Wars Kid Files Lawsuit}, WIRED, July 24, 2003, http://www.wired.com/culture/lifestyle/news/2003/07/59757 ("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.").
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.\textsuperscript{182}

The most readily remedied privacy harms in the pre-Web 2.0 era are related to economic loss compensable by way of damages.\textsuperscript{183} These damage-compensable harms may result from the misappropriation of an individual’s private persona, as with the misappropriation privacy tort,\textsuperscript{184} the right of publicity,\textsuperscript{185} or identity theft.\textsuperscript{186} Alternatively, some compensatory 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 express or implied ex ante agreements of confidentiality between the parties.\textsuperscript{187}

Courts and legislatures have been slow to compensate plaintiffs for nonmonetary harms resulting from a privacy incursion.\textsuperscript{188} This may be because it is too difficult for courts to quantify such harms.\textsuperscript{189} Alternatively, courts may be wary of putting a high price on truthful speech for fear of chilling expression and creating a culture of censorship. Still another explanation relates to the underenforcement of privacy rights. 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

\textsuperscript{182} SOLOVE, THE DIGITAL PERSON, supra note 23, at 97 (“The 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.”).
\textsuperscript{183} SOLOVE, THE FUTURE OF REPUTATION, supra note 17, at 122 (noting that while litigation is not always primarily about economic damages, rather many litigants bring claims for other reasons, such as to vindicate their reputation or seek an apology).
\textsuperscript{184} RESTATEMENT (SECOND) OF TORTS, § 652C (1977) (“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.”).
\textsuperscript{185} LALONDE ET AL., supra note 174, § 2B.01 (“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 68, at 173–77 (discussing technical differences between the privacy misappropriation tort and the right of publicity tort).
\textsuperscript{186} See SOLOVE ET AL., INFORMATION PRIVACY LAW, supra note 27, at 696–700.
\textsuperscript{187} See Richards & Solove, supra note 113, at 163–64.
\textsuperscript{188} This may be gradually changing at least in some jurisdictions. See, e.g., Mosley v. News Group Newspapers, [2008] EWHC (QB) 1777, [231], [2008] All E.R. (D) 322 (Eng.) (£60,000 damages awarded in breach of privacy action in the United Kingdom).
\textsuperscript{189} Id. at [231] (“[I]t 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.”).
wherewithal or the time to litigate to protect their privacy. More worrisome, 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. On top of this, bringing 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, a privacy action—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—emphasizes the truth of the information.

As alluded to earlier, there is also the question of 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 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 have been watching him.

Extralegal remedies may be equally problematic in practice. For example, private companies that provide online services to protect individuals’ reputations, such as ReputationDefender, may have perverse economic incentives when it comes to protecting individual privacy and reputation. These services make money from 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 furthering a culture that engenders a lack of respect between individuals for

190 Id. at [230] (“Claimants with the degree of resolve (and financial resources) of Mr. Max Mosley are likely to be few and far between.”); Keats Citron, supra note 170, at 90 (noting that in the analogous case of civil rights laws such as defamation, “because damages may be hard to prove and quantify, and because many plaintiffs cannot afford to litigate based on principle alone, the high cost of litigation often deters the filing of general tort suits”).

191 SOLOVE, THE FUTURE OF REPUTATION, supra note 17, at 120–21 (noting the difficulties of plaintiffs in privacy actions having to be publicly identified on court records).

192 Mosley, [2008] EWHC (QB) 1777, at [214] (distinguishing between damages for defamation and damages for infringement of privacy rights). Judge Eady also noted the difficulties inherent in attempting to quantify a loss of privacy. Id. at [215]–[16]. Such losses cannot really be compared meaningfully with any losses suffered as a result of a physical injury or even a defamation claim. Id.

193 Id. at [225]–[26].

194 See SOLOVE, THE FUTURE OF REPUTATION, supra note 17, at 192 (describing ReputationDefender as “a company that helps people find and remove harmful information about themselves online”).

195 See Ann Bartow, Internet Defamation as Profit Center: The Monetization of Online Harassment, 32 HARV. J. L. & GENDER 383, 419 (2009) (“The greater the quantity of sexual harassment toward affluent victims that appears on the Internet, the wealthier reputation defense services [like Reputation Defender] can become. Substantial widespread online personal misery equals success for these companies. The sexual-harassment-based component of the ReputationDefender business model partly depends on a long-term flourishing of frightening misogyny that the legal system will not address.”).
each others' online reputations. 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 is 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 that is usually the focus of our legal system. This increased emphasis on noneconomic harms 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 possible 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 consider setting up dispute resolution services for privacy claims. And finally, there are the market solutions mentioned above, such as new forms of reputation defense services which do not 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 privacy outline, 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 directed at the most salient websites

196 Id.
197 This could be modeled on the notice and takedown provisions in the Digital Millennium Copyright Act, 17 U.S.C. § 512 (2006); see also Lipton, supra note 120 ("Peer photographs are usually taken with the consent of the image subject and in a non-intrusive fashion. In many cases, the subject has no objection to the taking of the picture, but may later be concerned about viral online dissemination. Laws that regulate intrusive image-capturing are therefore not much help when the subject's concern is with online dissemination." (footnotes omitted)).
hosting relevant information. Of course, this would not be a perfect remedy because of the permanent and viral nature of information online. 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 quite useless in practice if the individual defendant is unable to pay. This is another area in which the Web 2.0 era raises new dynamics when contrasted with Web 1.0 activities. The entities most likely to violate privacy in the Web 1.0 age were governments and corporations with deeper pockets to pay damages. In the age of Web 2.0 technologies, those threatening privacy are more likely to be private individuals without the financial wherewithal to pay large damage awards.

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

Delineating remediable harms has been a challenge for law and policy makers since the early days of the Internet. Even early Web 1.0 cases involving the data aggregation practices of governments and corporations were problematic under existing privacy laws in terms of identifying and remedying specific harms, particularly when the harms were not easily

198 See Lipton, supra note 120.
quantifiable in economic terms.\textsuperscript{200} Web 2.0 raises new challenges, particularly if future privacy regulators attempt to delineate bad faith privacy incursions from careless but relatively innocent privacy incursions. This is where the need for examining relationships between actors, and motivations behind privacy breaches, becomes important in the Web 2.0 privacy context. If bad faith conduct is to be punished more strenuously than innocent but careless conduct, it will be necessary for future regulators to carefully consider the entire context of a given privacy breach in terms of the actors involved and the motivations for their conduct, as well as taking a broader view of the nature of the potential harms and possible remedies.

\textit{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 \textit{nature} and \textit{format} of the information in question. These two aspects of information are distinct from each other, even though they are related. Inquiries about the \textit{nature} of information refer to the substance or content of the information, while inquiries about the \textit{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 multimedia formats—on an audience.\textsuperscript{201} These differences are discussed in the next section.

To date, different legal systems have taken varying approaches to questions involving the \textit{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 "any information relating to an identified or identifiable natural person."\textsuperscript{202} Further, it singles out certain classes of information for additional protections over and above the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{200} See supra note 127 and accompanying text.
\item \textsuperscript{201} Mosley, [2008] EWHC (QB) 1777, at [19] (noting qualitative difference between video and text information in the privacy context); Campbell v. MGN Ltd., [2004] UKHL 22, [72], [155]-[56], [2004] 2 A.C. 457 (appeal taken from Eng.) (U.K.) ("The publication of a photograph cannot necessarily be justified by saying that one would be entitled to publish a verbal description of the scene . . . ."); MILLS, supra note 68, at 35-37 (2008) (noting the importance of recognizing that information available through different modes of communication—such as text, audioclip, still images, and video recordings—have different impacts on privacy); id. at 238 ([C]ourts may be more inclined to protect against intrusive images than intrusive words."); id. at 263 (describing the British court’s readiness to extend privacy protections to photographs, but not to textual descriptions of particular misconduct); PALFREY & GASSER, supra note 18, at 43 ("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 . . . .").
\item \textsuperscript{202} Data Protection Directive, supra note 24, at art. 2(a).
\end{itemize}
\end{footnotesize}
general provisions of the Directive on data processing. 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.” 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.

With respect to the nature of information protected, American law approaches privacy very differently. Specifically, American law consists of a series of piecemeal statutes that provide specific protections for discrete classes of information—such as financial or health information. The downside of this approach in the Web 2.0 era is that it is less future-proof than the European Union approach; the classes of data protected are limited. The obvious advantage, on the other hand, 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.

In mapping an outline for Web 2.0 privacy, it is important for law and policy makers to consider what kinds of information require protection and how that protection should be achieved in practice. Some types of information have generally been regarded as more sensitive than others, including certain health and financial data. Nevertheless, even innocuous-

---

203 Id. at art. 8.
204 Id. at art. 8(1).
207 Even the European Union approach is now suffering under the pressures of Web 2.0 technologies. See Robinson et al., supra note 71, at vii (“Overall, we found that as we move toward a globally networked society, the Directive as it stands will not suffice in the long term.”).
208 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 Ltd., [2004] UKHL 22, [2004] 2 A.C. 457 (appeal taken from Eng.) (U.K.). 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 id. at [23] (describing the five different substantive aspects of the information in question as: “(1) 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”).
209 See, e.g., Case C-101/01, Criminal Proceedings Against Bodil Lindqvist, 2003 E.C.R. I-12971, ¶¶ 49–51 (involving information about a broken ankle as a health condition deserving of privacy); Campbell, [2004] UKHL 22 (involving information about a supermodel’s drug addiction).
210 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
seeming personal details can become greatly damaging if aggregated and disseminated online. This was certainly the case for "Dog Poop Girl," "Star Wars Kid," and "Bus Uncle." 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 defecate on a subway train and did not clean up the mess. The event was photographed and posted online along with information about her identity, contact details, and workplace. This led to a campaign of personal harassment that ultimately forced the woman to leave her job.

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 "lightsaber" from the popular Star Wars movies. Again, the information itself was innocuous in nature, but its dissemination and the resulting public humiliation caused the youth to drop out of school and seek psychiatric treatment. Finally, the so-called "Bus Uncle" incurred serious physical injury as a result of an attack prompted by information spread on the Internet about his talking too loudly on a cell phone on a bus and ignoring requests from other passengers to be quiet. 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 private information that may be associated with that information. See, e.g., Campbell, [2004] UKHL 22, at [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 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.

211 ZITTRAIN, supra note 180, at 211 (describing incident where woman refused to clean up her dog's mess on a subway car in Korea and aftermath wherein she was targeted for harassment and forced to quit her job when photographs of the incident and additional information about her were posted online).

212 See supra note 181 and accompanying text.

213 See supra note 180 and accompanying text.

214 SOLOVE, THE FUTURE OF REPUTATION, supra note 17, at 1-2.

215 ZITTRAIN, supra note 180, at 211.

216 SOLOVE, THE FUTURE OF REPUTATION, supra note 17, at 44-48.

217 See supra note 212.

218 ZITTRAIN, supra note 180, at 211.
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 that does cause 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 draw such distinctions in the future.

It may be difficult ex ante to identify what particular information is likely to cause harm and what information is not. It seems that any information that shows an individual doing something embarrassing or that runs counter to social norms has the potential to cause harm if disseminated and remixed widely online. It may be that the size of the categories of information that have little to no potential to cause harm dramatically shrinks in the Web 2.0 age. The fact that even innocuous information can potentially cause great harm when globally disseminated and remixed—as in the cases of Star Wars Kid, Bus Uncle, and Dog Poop Girl—puts greater pressure on regulators to consider the other elements of the privacy map outlined here. Considering the nature of the information in isolation may not be a very productive exercise in the context of an attempt to ascertain likely harms and appropriate remedies for a privacy incursion. However, putting this element together with the other elements of the privacy map may provide a more useful picture of likely harms and appropriate remedies. In particular, the motivations of the actors may be relevant in this context.\textsuperscript{219}

\section*{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.\textsuperscript{220} 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 the recent case of a young woman, Nicole Catsouras, who was killed and horrifically mutilated in a car accident.\textsuperscript{221} Photographs of the accident scene were leaked by the police and disseminated over the Internet with various macabre captions

\begin{itemize}
\item \textsuperscript{219} Keats Citron, \textit{infra} note 170, at 125 (noting the importance of punishing mob behavior online which is in some ways analogous to punishing those who infringe on others' privacy with malicious motivations).
\item \textsuperscript{220} See \textit{infra} note 201 and accompanying text.
\item \textsuperscript{221} Keats Citron, \textit{infra} note 170, at 104–05 (describing the Catsouras incident).
\end{itemize}
added, much to the dismay of the young woman’s family.\textsuperscript{222} The impact of the pictures was much more powerful and emotionally harmful to the family than a text-based description of the accident, standing alone, could have been.\textsuperscript{223}

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, a federal district 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).\textsuperscript{224} In the recent \textit{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.\textsuperscript{225} In that case, the court ultimately found that even the text-based publication infringed the plaintiff’s privacy rights.\textsuperscript{226} 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.\textsuperscript{227}

The same impulse was evident in the British House of Lords decision involving a published story about supermodel Naomi Campbell’s battle with drug addiction.\textsuperscript{228} Several of the judges commented that the story could have been published without photographs of Campbell entering or leaving a Narcotics Anonymous meeting.\textsuperscript{229} The addition of the photograph was not necessary to the story. Even the judges dissenting on this point

\textsuperscript{222} Id.
\textsuperscript{223} Id.
\textsuperscript{225} \textit{Mosley v. News Group Newspapers}, [2008] EWHC (QB) 1777, [16], [2008] All E.R. (D) 322 (Eng.) ("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.").
\textsuperscript{226} Id. at [134] ("In the 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.").
\textsuperscript{227} Id. at [21] ("[I]t 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."); \textit{see also Campbell v. MGN Ltd.}, [2004] UKHL 22, [60] [2004] 2 A.C. 457 (appeal taken from Eng.) (U.K.) ("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 the sexual relationship, would be too intrusive and demeaning.").
\textsuperscript{228} \textit{Campbell}, [2004] UKHL 22.
\textsuperscript{229} Id. at [121], [155]–[56].
noted that photographs are qualitatively different from text in the information they convey to the recipient.\textsuperscript{230}

Today, more and more sophisticated recording technology is in the hands of the government, the press, private corporations, and private individuals. People can quickly, easily, and cheaply create sophisticated multimedia files capable of intruding into others' private lives.\textsuperscript{231} 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, while a graphical depiction would be 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 an outline of privacy for the Web 2.0 environment.\textsuperscript{232}

**CONCLUSION**

The aim of attempting to map an outline of privacy is to create a framework within which solutions to specific Web 2.0 privacy problems might be more easily and cohesively developed. The goal of the map is to delineate some boundaries within which scholars, courts, and legislatures can identify current and future challenges for privacy law in a more organized way. Although the framework presented here does not provide concrete solutions to privacy problems, it does illustrate how much the privacy matrix has broadened, and continues to broaden, since the advent of the Web 2.0 era. 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.

Part of the impetus behind the creation of an outline of the outer boundaries of privacy is that much recent work has focused instead on the specific individual privacy harms without considering how broadly any solutions might reach. An attempt to pull back the lens and take a more overarching view of privacy should help to ensure that some meaningful boundaries are imposed on future privacy regulation. The focus on the constituent elements of a privacy incursion—actors and relationships, conduct, motivations, harms and remedies, nature of information, and format of information—ensures that any regulatory actions taken can be linked to

\textsuperscript{230} Id. at [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.").

\textsuperscript{231} SOLOVE, THE FUTURE OF REPUTATION, supra note 17, at 45–46 (describing the multimedia versions created of the Star Wars Kid video and shared publicly over the Internet); Blackman, supra note 159, at 328–31 (discussing the acceleration of technologies which enhance the potential for intrusion).

\textsuperscript{232} See Lipton, supra note 120.
something relatively concrete in terms of the practical realities of a privacy-threatening situation. This approach encourages courts and commentators to focus on the constituent elements of any given privacy incursion and to attempt to tease out the often subtle relationships between them. 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.