September 2014

"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video

Jacqueline D. Lipton
Case Western Reserve University School of Law, jdl14@case.edu

"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video

Jacqueline D. Lipton*

Abstract

In January 2009, the Camera Phone Predator Alert bill was introduced into Congress. It raised serious concerns about privacy rights in the face of digital video technology. In so doing, it brought to light a worrying gap in current privacy regulation – the lack of rules relating to digital video privacy. To date, digital privacy regulation has focused on text records that contain personal data. Little attention has been paid to privacy in video files that may portray individuals in inappropriate contexts, or in an unflattering or embarrassing light. As digital video technology, including inexpensive cellphone cameras, is now becoming widespread in the hands of the public, the regulatory focus must shift. Once a small percentage of online content, digital video is now appearing at an exponential rate. This is largely due to the growth of online social networking platforms such as YouTube and Facebook. Sharing video online has become a global phenomenon, while the lack of effective privacy protection for these images has become a global problem. Digital video poses four distinct problems for privacy, arising from: de-contextualization, dissemination, aggregation, and permanency of video information. While video shares some of these attributes with text, its unique qualities necessitate a separate study of video privacy regulation. This article identifies a rationale for, and critiques suggested approaches to, digital video privacy. It argues that legal regulation, without more, is unlikely to provide necessary solutions. Instead, it advocates a new multi-modal approach consisting of a matrix of legal rules, social norms, system architecture, market forces, public education, and non-profit institutions.

---

* Professor of Law, 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. For helpful comments on earlier drafts of this article, the author would like to thank Professor Andrea Matwyshyn and participants at a panel on user-generated content and privacy at "Computers, Freedom and Privacy '08" at Yale University on May 21, 2008, as well as participants at the 8th Annual Intellectual Property Scholars' Conference at Stanford Law School on August 7-8, 2008, and participants in a Faculty Colloquium at Villanova Law School on October 10, 2008, and those at a Faculty Workshop at the University of Florida Levin College of Law on October 15, 2008. Additionally thanks are due to the following people for commenting on earlier drafts of this article – Professor A. Michael Froomkin, Professor Mark Lemley, Professor Patricia Sánchez Abril, Professor Ruth Gordon, Professor Doris DelTosto Brogan, Professor John Gotanda, Professor Marc Blitz, Professor Hannibal Travis, Professor Diane Zimmerman, Professor Daniel Sokol, Professor Lyrissa Lidsky, Professor Elizabeth Rowe, Professor Jon Mills, Professor Michelle Jacobs, Professor Juan Perea, Professor Charlene Luke, Professor B Jessie Hill, and Professor Christopher Slobogin. Thanks are also due to Josephina Manifold for her excellent research assistance. All mistakes and omissions are, of course, my own.

Table of Contents

I. INTRODUCTION

In my mind and in my car, we can't rewind we've gone too far.
Pictures came and broke your heart, put the blame on VTR.

- The Buggles, *"Video Killed the Radio Star"*[1]

Once upon a time, a passenger's dog defecated on the floor of a subway car in South Korea. While unremarkable in itself, this story quickly became an Internet sensation when the passenger refused to clean the mess, even after being offered a tissue by a fellow traveler.[2] Someone on the train, an anonymous face in the crowd, took photos of the woman with a cellphone camera. These images were promptly posted on a popular Korean blog. The aim was to shame the unrepentant and socially irresponsible dog owner.[3] Ultimately, the humiliation attached to this incident resulted in a firestorm of criticism that caused her to quit her job.[4] This story is one of a number of recent episodes illustrating how a person's privacy can be destroyed at the push of a button, using the simplest and most ubiquitous combination of digital technologies – the cellphone camera and the Internet.[5] Another salient example of this phenomenon involved "Star Wars kid" – a Canadian teenager who filmed himself playing with a golf ball retriever as if it was a light-saber from the *Star Wars* movies. His video was posted to the Internet without his authorization. It was then adopted by a variety of amateur video enthusiasts on services such as YouTube.[6] They created many popular, but extremely humiliating, mash-up videos[7] of the youth.[8] The young man ended up dropping out of school. He also required psychiatric care, including a period of institutionalization at a children's psychiatric facility.[9]

---

[1] The Buggles, "Video Killed the Radio Star" (song lyrics), available at http://www.lyricsondemand.com/onehitwonders/videokilledtheradiostarlyrics.html, last viewed on May 14, 2008.

[2] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT, 211 (2008).

[3] DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET, 1 (2007) [hereinafter, THE FUTURE OF REPUTATION].

[4] ZITTRAIN, *supra* note ___, at 211.

[5] *id*., at 99 ("One holder of a mobile phone camera can irrevocably compromise someone else's privacy …"). On camera phones in particular, see discussion in Alan Kato Ku, *Talk is Cheap, But a Picture is Worth a Thousand Words: Privacy Rights in the Era of Camera Phone Technology*, 45 SANTA CLARA L REV 679 (2005)

[6] See www.youtube.com, last viewed on September 29, 2008.

[7] Wikipedia currently defines a "mashup" as "a digital media file containing any or all of text, graphics, audio, video and animation drawn from pre-existing sources, to create a new derivative work": Wikipedia definition of "digital mashup", available at http://en.wikipedia.org/wiki/Mashup_(digital), last viewed on September 29, 2008.

[8] ZITTRAIN, *supra* note __, at 211 (discussion of "Star Wars kid" scenario); SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 43-48 (discussion of "Star Wars Kid" example of a video-based privacy invasion that harmed an individual's reputation and caused ongoing harm to him in the real world).

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

If these episodes are not enough to raise the specter of serious harm, consider the fate of "Bus Uncle" in Hong Kong. This man was physically assaulted in a targeted attack at the restaurant where he worked. The attack ensued after online posting of a video depicting him speaking loudly on his cellphone on a bus and ignoring requests of other passengers to be quiet.[10] Video privacy concerns have not gone unnoticed by Congress: for example, the Camera Phone Predator Alert bill,[11] introduced in January 2009, aims to allay fears about the exploitation of the public[12] through inappropriate and unauthorized cellphone photography.[13] The bill would require all cellphones to make an audible sound when taking a photograph to alert potential subjects that they may have been captured in a digital video file that could later be posted online.[14]

We are witnessing the emergence of a worrying new trend: peers[15] intruding into each other's privacy and anonymity with video and multi-media files in ways that harm the subjects of the digital files.[16] There is a mismatch between these harms and available legal remedies, notably those arising out of privacy and defamation law.[17] Even new laws

---

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

[11] H.R. 414 (111th Cong., 2009).

[12] In this respect, it focuses on children and adolescents: Camera Phone Predator Alert bill, H.R. 414 (111th Cong., 2009), § 2 ("Congress finds that children and adolescents have been exploited by photographs taken in dressing rooms and public places with the use of a camera phone.")

[13] See Priya Ganapati, *New Bill Asks For Cameraphones to Go Clickety Clack*, Wired Blog Network (Jan. 26, 2009) (available at http://blog.wired.com/gadgets/2009/01/new-bill-asks-f.html, last viewed on January 27, 2009).

[14] Camera Phone Predator Alert bill H.R. 414 (111th Cong., 2009), § 3(a) ("Beginning 1 year after the date of enactment of this Act, any mobile phone containing a digital camera that is manufactured for sale in the United States shall sound a tone or other sound audible within a reasonable radius of the phone whenever a photograph is taken with the camera in such phone. A mobile phone manufactured after such date shall not be equipped with a means of disabling or silencing such tone or sound.") In fact, such a law already exists in Japan: Ganapati, *supra* note ___ ("Japan already requires all cameraphones including the iPhone to make an audible noise when taking a photograph.")

[15] In this context I use the term "peers" in a broad sense, referring to members of society with equal access to each other via cellphone pictures and day-to-day interactions. Unless the context otherwise requires, the term is not intended to connate particularly close personal relationships.

[16] See also Andrew McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L REV 887, 927 (2006) ("[T]echnology has made it much easier for people to take embarrassing pictures of others, both with and without consent, and to widely disseminate them via the Internet."); 928 ("Digital cameras and camcorders are specifically designed to be connected to computers and to deliver pictures across worldwide networks in an instant."); ZITTRAIN, *supra* note ___, at 221 ("The central problem [for regulating privacy on the Internet] is that the organizations creating, maintaining, using, and disseminating records of identifiable personal data are no longer just "organizations" – they are people who take pictures and stream them online, who blog about their reactions to a lecture or a class or a meal, and who share on social sites rich descriptions of their friends and interactions.")

[17] Existing privacy torts generally do not extend to activities in public places, even where one would assume the video subject had some expectation of privacy or anonymity: see discussion in Part II.A.2 *infra*. Defamation law will not sanction the publication of truthful material. A "defamatory" statement is a false statement that potentially harms a person's reputation: Arlen Langvardt, *Section 43(a), Commercial*

such as the proposed Camera Phone Predator Alert bill would only notify a person that a picture of her may have been taken. It would do nothing to stem the tide of global online dissemination of a damaging image of a person. While it is now trite to say that the Internet poses significant risks to privacy, these risks have previously manifested themselves in the collection, use, and dissemination of text-based personal records by governments,[18] businesses,[19] health care providers,[20] Internet intermediaries,[21] and prospective employers.[22] Today, we need to add concerns about unauthorized uses of our personal information by our peers over networks such as MySpace,[23] Facebook,[24] Flickr,[25] and Youtube,[26] much of it in video formats.[27] An image of an individual in an

---

Falsehood, and the First Amendment: A Proposed Framework, 78 MINN. L. REV 309, 334 (1993) ("The common law defines defamation as the publication of a false and defamatory statement about the plaintiff. Defamatory statements, by definition, tend to harm the plaintiff's reputation.").

[18] Professor Solove has, in fact, devoted a large part of a book to these issues: Solove, THE DIGITAL PERSON, Part III: Government Access (2004) [hereinafter, THE DIGITAL PERSON]

[19] *id*., at 4 ("Computers enable marketers to collect detailed dossiers of personal information and to analyze it to predict the consumer's behavior. Through various analytic techniques, marketers construct models of what products particular customers will desire and how to encourage customers to consume. Companies know how we spend our money, what we do for a living, how much we earn, and where we live. They know about our ethnic backgrounds, religion, political views, and health problems. Not only do companies know what we have already purchased, but they also have a good idea about what books we will soon buy or what movies we will want to see.")

[20] See, for example, Sharona Hoffman and Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security Of Electronic Private Health Information*, 48 BOSTON COLLEGE LAW REVIEW 331 (2007); Patricia Sánchez Abril and Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 244 (2008).

[21] See, for example, Electronic Privacy Information Center, *Privacy? Proposed Google/Doubleclick Deal*, available at http://epic.org/privacy/ftc/google/ , last viewed on July 21, 2008 (expressing concern about ability of Internet intermediaries such as search engine Google and Internet advertising firm Doubleclick to monitor users' online behavior in the context of proposed merger negotiations between Google and Doubleclick).

[22] SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 203 (discussing employers' practices with respect to ascertaining and using online information about prospective hires).

[23] MySpace is a social networking service where individuals can search for and communicate with old and new friends: see www.myspace.com, last viewed on July 22, 2008.

[24] Facebook describes itself as a "social utility that connects you with the people around you.": www.facebook.com, last viewed on July 22, 2008.

[25] Flickr describes itself as "almost certainly the best online photo management and sharing application in the world": www.flickr.com, last viewed on July 22, 2008.

[26] YouTube is an online file sharing service for video files: www.youtube.com, last viewed on July 22, 2008. SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 40 ("Anybody can post videos of anybody else on YouTube. People can post pictures of you or write about you in their blogs. Even if you aren't exhibiting your private life online, it may still wind up being exposed by somebody else.")

[27] Throughout this article, "video" refers collectively to still images and multi-media video files. While I recognize there are important qualitative differences between these kinds of files, the aim of this Article is to draw a line between text-based privacy incursions, and those incursions that involve different kinds of media. In later work, I hope to draw more subtle distinctions between different non-text formats for online information. See ZITTRAIN, *supra* note ___, at 221 (noting that new threats to privacy online arise from peer based multimedia content being disseminated on the Internet, as opposed to the traditional threats where organizations collated text based data about private individuals).

embarrassing situation might well affect her chances of employment,[28] education, or health insurance.[29] As in the examples of "Star Wars kid", "dog poop girl", and "Bus Uncle", the consequences of such unauthorized dissemination can be devastating.

Video images are qualitatively different from text-based data in a variety of ways.[30] Nevertheless, most privacy literature fails to acknowledge that fact. This Article focuses on how best to protect video privacy in an age of online social networking. This issue must be considered urgently by law and policy makers to avoid the entrenchment of privacy-destroying norms when online social networking (OSN) technologies reach a critical mass point.[31] This Article argues that legal regulation alone is unlikely to solve society's video privacy problems.[32] It advocates a multi-modal approach that combines six regulatory modalities: legal rules, social norms,[33] system architecture,[34] market forces,[35] public education, and private/non-profit institutions.[36] Part II identifies gaps in privacy law with respect to online video privacy. It notes that, current tort laws are ill-suited to the digital age, and are globally disharmonized. Part III identifies practical and

---

[28] SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 38 ("Employers are looking at social network site profiles of prospective employees. Microsoft officials admit to trolling the Internet for anything they can find out about people they are considering for positions.")

[29] *id*. On the other hand, there is some suggestion that the widespread availability of personal information online cannot be stopped and might actually be beneficial to society. See, for example, Lior Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information,* 102 NORTHWESTERN UNIVERSITY LAW REVIEW, forthcoming, October 2008 (arguing that basing decisions on real information rather than dangerous and discriminatory proxies such as race actually provides social benefits overall) [hereinafter, *Reputation Nation*]

[30] JON MILLS, PRIVACY: THE LOST RIGHT, 35-37 (2008) (noting the importance of recognizing that information available through different modes of communication - such as text, audio tape, still images, and video recordings – have different impacts on privacy); 238 ("courts may be more inclined to protect against intrusive images than intrusive words"); 263 (describing British courts' readiness to extend privacy protections to photographs, but not to textual descriptions of particular misconduct). See also discussion in Part II.

[31] That is, of course, assume they haven't already reached that point. See discussion in Gaia Bernstein, *When New Technologies are Still New: Windows of Opportunity for Privacy Protection*, 51 VILLANOVA LAW REVIEW 921 (2006) (noting importance of at least thinking about making regulatory decisions to protect privacy interests before privacy-destroying norms become entrenched when the take-up of the technology reaches a critical mass) [hereinafter, *New Technologies*].

[32] JACK GOLDSMITH and TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD, 181 (2006) ("There's no reason to doubt that most people's lives are dominated not by law but by social norms, morality, and the market, or that the Internet is deeply influenced by its code.")

[33] Katherine Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L REV 1235,1238 (2005) ("Social norms are primarily understood as means to coordinate the behavior of individuals in a social group. Thus, norms may help to solve coordination problems - by determining how pedestrians pass one another on the street - and collective action problems - by stigmatizing littering - when individually rational behavior leads to collectively undesirable results.")

[34] See discussion in Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEXAS L REV 553 (1998) (describing how digital technology can be utilized as a form of regulatory mechanism for online conduct) [hereinafter, *Lex Informatica*].

[35] Ann Carlson, *Recycling Norms*, 89 CALIFORNIA LAW REV 1231, 1253 (2001) ("Markets constrain behavior through price. If the price of gasoline rises dramatically, people will drive less.")

[36] These may be defined as institutions with social benefits, rather than commercial profits, as their aim. See Neil Richards, *Intellectual Privacy*, 87 TEXAS L REV, forthcoming 2008 (describing the American Libraries Association as a regulatory institution in this sense with respect to the bill of rights it developed to protect interests of library patrons in 1939) [hereinafter, *Intellectual Privacy*].

theoretical justifications for, and possible approaches to, regulating online video privacy. Part IV sets out a framework for a new multi-modal regulatory approach based on the six modalities identified above. Part V concludes with a discussion of future directions for online video privacy regulation.

II. ONLINE VIDEO PRIVACY: GAPS IN THE EXISTING LEGAL FRAMEWORK

New technologies are radically advancing our freedoms, but they are also enabling unparalleled invasions of privacy.

- Electronic Frontier Foundation[37]

Advances in video technologies have historically facilitated dramatic social transformations. In the late nineteenth century, when photography first became relatively cheap and portable,[38] commentators expressed concerns about the development of the "snap camera" by Kodak.[39] This camera for the first time enabled private individuals and members of the press to take and distribute candid photographs in a way never before possible.[40] It was also what ultimately spurred on Warren and Brandeis to publish their seminal article on privacy.[41] Their article shaped the development of American privacy law for more than a century.[42] The fact that it was derived from the authors' concerns about *video* privacy suggests something important about video that differentiates it from other forms of information.[43]

Today's online video technologies create new threats to privacy. With cellphone cameras and the Internet, the dissemination of video – both still and multi-media - is now

---

[37] Electronic Frontier Foundation, *Privacy*, available at http://www.eff.org/issues/privacy, last viewed on May 12, 2008.

[38] SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 107 ("Kodak's snap camera was cheap and portable. Many more people could afford to own their own camera, and for the first time, candid photos of people could be taken.").

[39] *id*, at 107-108.

[40] Neil Richards and Daniel Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 THE GEORGETOWN LAW JOURNAL 123, 128-9 (2007) (describing Warren and Brandeis' concern with the combination of newspaper sensationalism and new photographic technology enabling more widescale candid photography and dissemination of resulting photographs than ever before) [hereinafter, *Privacy's Other Path*]; DANIEL SOLOVE, UNDERSTANDING PRIVACY, 15 (2008) ("Warren and Brandeis were concerned not only with new [photographic] technology but with how it would intersect with the media. The press was highly sensationalistic at the time.") [hereinafter, UNDERSTANDING PRIVACY].

[41] Samuel D Warren and Louis D Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); JON MILLS, PRIVACY: THE LOST RIGHT, 5 (2008) (noting that concerns about the advent of popular photography was probably what spurred on Warren and Brandeis in writing this article).

[42] DANIEL SOLOVE, UNDERSTANDING PRIVACY, 15 (2008) ("Many scholars have proclaimed Warren and Brandeis's article the foundation of privacy law in the United States."); Richards and Solove, *Privacy's Other Path*, *supra* note ___, at 127-8 (describing Warren and Brandeis' contribution to the privacy debate as "Privacy's Defining Moment" in heading "I").

[43] See also MILLS, *supra* note ___, at 35-37 (noting the importance of recognizing that information available through different modes of communication - such as text, audio tape, still images, and video recordings – have different impacts on privacy); 238 ("courts may be more inclined to protect against intrusive images than intrusive words"); 263 (describing British courts' readiness to extend privacy protections to photographs, but not to textual descriptions of particular misconduct).

practically instantaneous and potentially global in scope. The concerns about loss of control over personal information are much greater online than even in the gossip rags of the nineteenth century. To be published in a newspaper, albeit a scandal sheet, pictures had to make their way into the hands of an entity that produced such a publication. Today, anyone can be a publisher. Photographers do not even need a stand-alone camera to capture a candid image – most people can resort to their inexpensive and ever-present cellphones.[44] The fact that individuals can instantly snap a photograph without even thinking to carry a camera, and that they can then disseminate that image instantaneously and globally at the push of a button, raises significant problems of decontextualization. Compared to the individual writing a text-based account of an event and posting it online, the video record is likely to capture more information, including more incidental background information than might appear in a text-based record. Additionally, more thought goes into writing the text than into thoughtlessly snapping an image. Thus, more context is likely to be provided in a textual account of the same event.

Images and multi-media files are quite different from text, particularly as reagards context.[45] Textual data is often iterative. It tends to be aggregated over a period of time from different sources. This provides it both some context and a greater degree of accuracy. Concerns about digital data have focused on the way in which textual data can represent too detailed a profile of a person online[46] that is often readily available to third parties. Nevertheless, it may take a whole collection of textual data to suggest something that a picture candidly demonstrates in one digital file. An aggregated text profile, for example, may include items that suggest a person is trying to become pregnant. These data may include records involving purchase of ovulation tests, pregnancy tests, information on pregnancy, information on in vitro fertilization (IVF), and medical appointments with fertility specialists. However, a video image of the person entering an IVF clinic could potentially tell the story in one glance.

Nevertheless, the image lacks context[47]: for example, the video subject may have entered the IVF clinic for a variety of reasons, including to provide support to a friend undergoing IVF treatment. Thus, the aggregated text profile may be a more accurate reflection of a data subject's attempts to become pregnant because it is verifiable by a set of data collected over time from a variety of sources. Of course, it is equally possible that the data subject could be purchasing tests and fertility information for a friend just as easily as she could be attending an IVF clinic to provide support to a friend. Nevertheless, in general, the aggregation of multiple data records across time and from a variety of sources is less likely to be misinterpreted than a single image taken out of

---

44 See discussion in Kato Ku, *supra* note ___; Ganapati, *supra* note ___.

45 MILLS, *supra* note ___, at 35 ("Photos have a different impact than written words, and a video has a different impact than photos, as a mode of intrusion."), 36-37 (noting the importance of recognizing that information available through different modes of communication - such as text, audio tape, still images, and video recordings – have different impacts on privacy); 238 ("courts may be more inclined to protect gainst intrusive images than intrusive words"); 263 (describing British courts' readiness to extend privacy protections to photographs, but not to textual descriptions of particular misconduct).

46 SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 117-121.

47 Patricia Sánchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 73, 75 (2007) (raising contextualization concerns about images disseminated online) [hereinafter, *(My)Space*].

context. The more sources and more time involved, the more accurate the data record is likely to be.

Outside contextualization concerns, digital video poses additional problems for online privacy: the threat of viral online distribution of private images (dissemination problems);[48] the possibility of others augmenting the images with additional information - true, false, or indeterminate (aggregation problems);[49] and the inability of an image subject to ever obtain control of the information once it hits cyberspace (permanence problems).[50] These problems are highlighted below in an examination of gaps in the current laws that protect privacy.

A. PROTECTING ONLINE PRIVACY: GAPS IN THE LAW

1. Copyright Law

While copyright law has proved extremely effective in protecting property rights online, it is of little assistance to those seeking to protect privacy. Copyright in an image is generally granted to the photographer, not the photographic subject.[51] As the subject is not likely to have been the photographer, copyright law will not help those attempting to control dissemination of photographs in which they feature as subjects. Of course, in the unusual case where the subject is the copyright owner,[52] a copyright action would be

---

[48] With respect to the viral distribution of information online generally, see SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 62 ("In the offline world, rarely does gossip hit a tipping point. The process of spreading information to new people takes time, and friends often associate in similar circles, so most secrets don't spread too widely. The Internet takes this phenomenon and puts it on steroids. People can communicate with tens of thousands – even millions – of people almost simultaneously. If you put something up on the Internet, countless people can access it at the same time. In an instant, information can speed across the globe.")

[49] The idea of data aggregation appears as a sub-set of the idea of information processing in Professor Solove's "taxonomy of privacy". See, for example, SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 118 ("Aggregation is the gathering of information about a person. A piece of information here or there is not very telling, but when combined, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts.") Adding new information to video images might, in some contexts, resemble a form of identification as also contemplated in Professor Solove's taxonomy: SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 123 ("Identification is similar to aggregation because both involve the combination of different pieces of information, one being the identity of a person. However, identification differs from aggregation in that it entails a link to the person in the flesh.")

[50] SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 33 ("The Internet … makes gossip a permanent reputational stain, one that never fades. It is available around the world, and with Google it can be readily found in less than a second."), 165 (citing Professor McClurg's work suggesting that images have a quality of permanence that memories lack in the sense that people can scrutinize an image and notice details they might not see when observing the original situation); McClurg, *supra* note ___, at 928 ("[P]ersons whose private information is posted on the Internet permanently lose control over that information and, hence, that aspect of their selves."); ZITTRAIN, *supra* note ___, at 211 ("Lives can be ruined after momentary wrongs, even if merely misdeameanors."); Abril, *(My)Space*, *supra* note ___, at 75 ("Lacking the relative transience of human memory, the digital record has increased the takes of privacy today…").

[51] SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 184 ("Copyright in a photo is owned initially by the person who takes the photo, not by the person whose photo is taken.").

[52] Either because she used a timer to take the picture or because someone else assigned copyright in the image to her.

available for unauthorized distribution of the video online.[53] Interestingly, the Digital Millennium Copyright Act (DMCA) in 1998 incorporated a notice and takedown regime that gives an immediate right to have an image removed from a website on the basis of a copyright infringement. However, no similar law has been enacted for intrusions into an individual's privacy or dignity.[54]

2. Privacy Torts and Intentional Infliction of Emotional Distress

Laws regulating intrusive photography are equally unlikely to help image subjects. While some privacy torts prohibit intrusions into seclusion,[55] conduct involving OSNs will generally not attract the operation of these laws. Peer photographs are usually taken with the consent of the image subject and in a non-intrusive fashion.[56] 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.[57] Other torts aimed at personal privacy will likewise have little to no application: for example, the idea of an unauthorized appropriation of a person's name or likeness will be of little use in a peer context.[58] For one thing, the appropriation is arguably not unauthorized if the subject has consented to the taking of the photograph.[59] For another thing, this tort requires a commercial profit motive[60] which is generally absent in the OSN context, at least as between peers.

---

[53] 17 U.S.C. § 106 sets out the rights of a copyright holder to prevent unauthorized reproduction, distribution, and preparation of derivative works based on a copyrighted work.

[54] 17 U.S.C. § 512(c).

[55] See, for example, California Civil Code, § 1708.8(a) ("A person is liable for physical invasion of privacy when the defendant knowingly enters onto the land of another person without permission or otherwise committed a trespass in order to physically invade the privacy of the plaintiff with the intent to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity and the physical invasion occurs in a manner that is offensive to a reasonable person.")

[56] This would also be a shortcoming of the Camera Phone Predator Alert Act, H.R. 414 (111th Cong., 2009) if it was ever enacted. It only deals with intrusive image-gathering, and not with any subsequent unauthorized dissemination.

[57] California Civil Code, § 1708.8 (f) specifically states that dissemination of images taken in contravention of the earlier provisions of the section is not in and of itself a violation of the section: "Sale, transmission, publication, broadcast, or use of any image or recording of the type, or under the circumstances, described in this section shall not itself constitute a violation of this section, nor shall this section be construed to limit all other rights or remedies of plaintiff in law or equity, including, but not limited to, the publication of private facts."

[58] SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 187 ("The appropriation tort would rarely apply to the discussion on the Internet of people's private lives or the posting of their photos.") The same might be said about the right of publicity tort: ANNE GILSON LALONDE, GILSON ON TRADEMARKS, at § 2.16[1] ("The right of publicity … is the right of an individual to control the commercial use of his or her name, likeness, signature, or other personal characteristics.") [hereinafter, GILSON LALONDE].

[59] Of course, there may be cases where the taking of the image is initially authorized, but its subsequent use in a commercial context is unauthorized. The commercial use requirement, however, will generally not be made out when peers are simply posting images of each other online.

[60] Appropriation actually appears as both a distinct limb of privacy law in the Restatement (Second) of Torts, and as a stand-alone tortious action in a number of American state jurisdictions known variously as the "right of publicity" or "personality rights tort". See 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

Other privacy torts in the United States focus respectively on public disclosures of private facts,[61] and on publicity which places a person in a false light in the eyes of the public.[62] Both of these require some form of public disclosure[63] which may be missing in a closed social network such as Facebook or MySpace – although distribution over an open network such as YouTube or Flickr would be another story.[64] However, even where there is a public disclosure, it is an open question whether the distribution will amount to a disclosure of private facts, or will present a person in a false light. An individual may object to the dissemination of an image even though it does not disclose any private facts, and does not present her in a false light.[65] The former tort also generally requires that the private facts in question must have been shameful by an objective standard which is often difficult to prove.[66] The information must also not have been newsworthy[67] - a standard that has proved notoriously difficult to define.[68]

---

for invasion of his privacy."). For an example of a right of publicity tort, see California Civil Code, § 3344(a) ("Any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of products, merchandise, goods or services, without such person's prior consent, or, in the case of a minor, the prior consent of his parent or legal guardian, shall be liable for any damages sustained by the person or persons injured as a result thereof.").

[61] For a discussion of current problems and future directions with this branch of privacy law in the online context, see Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1 (2007) [hereinafter, *Recasting Privacy*].

[62] Restatement (Second) of Torts, § 652D ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.")

[63] *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 the other would be placed."); Sánchez Abril, *Recasting Privacy*, *supra* note ___, at 9-11 (discussing practical difficulties of individual plaintiffs establishing requisite disclosures of private facts both in the physical world and online).

[64] A "closed" network is one in which the participants have some control over who has access to information and videos they post online, while an open network is generally accessible to anyone with an Internet connection.

[65] One example of this, although not a "peer" based incursion into privacy is the example of the "lady eating a peach" video that David Letterman repeatedly showed on his late night television program. It embarrassed the woman who was caught on camera eating an over-ripe peach indelicately at the U.S. Open, but it did not show anything false about her: David Usborne, *Peach Lady Puts Squeeze on TV Star,* THE INDEPENDENT, London (Feb 7, 1996) (full text available at http://findarticles.com/p/articles/mi_qn4158/is_/ai_n14027742, last viewed on January 12, 2009).

[66] Jonathan B Mintz, *The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain*, 55 MARYLAND LAW REVIEW 425, 439 (1996) ("Whether a fact is private by nature - that is, whether a reasonable person would feel seriously aggrieved by its disclosure - is the subject of some disagreement.")

[67] Abril and Cava, *supra* note ___, at 265 ("[T]o succeed on a privacy tort claim, the information must not be of public concern. If the … information disclosed is newsworthy or of public concern, the aggrieved is precluded from recover in tort, as such recovery is preempted by the formidable First Amendment.")

[68] Mintz, *supra* note ___, at 441-442 ("Facts of "legitimate public concern" or "newsworthy" facts, even if legally private**,** may be disclosed without any liability under this tort. Regardless of whether a plaintiff must affirmatively prove that facts disclosed were not newsworthy, or whether defendants can be

Related to the privacy torts is the tort of intentional infliction of emotional distress.[69] Like the privacy torts, this tort is likely to be of limited use in the situations under consideration in this Article.[70] However, that might change if courts reassess the contours of the tort in light of online activities.[71] The main problem with this tort is that it has generally required outrageous or malicious conduct on the part of a defendant.[72] It is unlikely that private individuals posting videos of each other online would be found to be engaging in such conduct.[73]

3. Defamation

For defamation law to assist a person concerned about unauthorized dissemination of an image online, the dissemination would have to amount to a defamatory communication.[74] This would require proof that the image is both false and harmful to the subject's reputation.[75] This is likely an insurmountable hurdle in most cases involving OSNs. Images are unlikely to be false for defamation purposes unless they have been doctored. Further, defamation law can do little about viral distributions of personal images, or about the permanence problem. Enforcement of a defamation order[76] online can be problematic if the information in question exists in multiple websites and in multiple jurisdictions by the time the order is made.[77] Additionally, online intermediaries such as Internet service providers, who serve as conduits for potentially defamatory content – and are often the easiest potential defendants to identify – are generally immune from liability.[78]

4. Data Protection Law in the European Union

---

said to enjoy a privilege or a defense, many have declared that the broad scope of the newsworthiness doctrine has "decimated the tort."")

69 Restatement (Second) of Torts, § 46 (1977).

70 Abril, *(My)Space*, *supra* note ___, at 81 (noting that the tort is ineffectual in the OSN context because conduct in question is usually not sufficiently "extreme and outrageous" and because many courts require physical manifestations of the claimed emotional distress).

71 MILLS, *supra* note ___, at 195 ("The law [on intentional infliction of emotional distress] is still in a stage of development, and the ultimate limits of this tort have not yet been determined.")

72 *id*.

73 It is also unlikely that OSN providers would be found to be directly liable for intentional infliction of emotional distress. Any action for secondary liability against an OSN provider would also likely prove fruitless because of the application of § 230 of the Communications Decency Act of 1996: MILLS, *supra* note ___, at 35 (discussing recent judicial applications of the Communications Decency Act, § 230, to immunize Internet service providers from liability for information that is posted by a user of the service).

74 Langvardt, *supra* note ___, at 334.

75 *id.*

76 Jennifer Meredith Liebman, *Defamed by a Blogger: Legal Protections, Self Regulation, and Other Failures*, 2006 U. ILL. J.L. TECH. & POL'Y 343, 368-372 (2006) (describing different kinds of defamation remedies that may be sought online including a retraction, an injunction, and damages).

77 *id*, at 368 (noting that even if the complainant obtains a retraction by the original poster of defamatory context, the information is likely available in many other places online, including places like the Internet Archive Project that preserves information that has already been retracted from websites)

78 47 U.S.C. § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

While this discussion has so far focused largely on American privacy law, international comparisons may be instructive. The European Union, for example, provides stronger data protection for its citizens than the United States. A cornerstone of the European Union approach to privacy is the European Union Data Protection Directive.[79] While the Directive is intended to have a wide reach, it has some limitations in the OSN context. For one thing, it is generally limited to conduct occurring within the European Union.[80] Thus, it does not have global reach, subject to provisions that extend its operation to data about its citizens transmitted to third countries.[81] Perhaps more importantly, it was drafted with the processing of textual data in mind, largely in the context of business or governmental dealings with personal information. There may be some question about the extent to which it would apply in the OSN context.

While "personal data" is defined broadly as "any information relating to an identified or identifiable natural person",[82] there are potentially two important limitations. The first is that the Directive covers "information processing activities" which are conceived in terms that contemplate largely professional, governmental, or commercial activities involving compilations of individual information. On the other hand, "processing" is defined broadly to encapsulate "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".[83] Thus, it is possible that the broad definition of personal data could include digital video images and the broad definition of processing could include dissemination of those images over an OSN.

The second limitation on the Directive's operation may be more problematic. Article 3(2) creates an exception for the processing of personal data "by a natural person in the course of a purely personal or household activity". Social networking activities might well fall within this category. If that is the case, they would not be covered by the Directive. Of course, the Directive may apply to OSNs that provide forums for online networking, such as Facebook, MySpace, and Flickr. These services are businesses that are not engaged in purely personal or household activities. An aggrieved plaintiff may have recourse against a social networking site,[84] but arguably not against specific peers who post unauthorized images on the service.

---

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

80 Most of the articles of the Directive apply to Member States of the European Union. However, some provisions impact on transfers of data to third countries: See Data Protection Directive, Articles 25 and 26.

81 Data Protection Directive, Articles 25 & 26.

82 *id*., Article 2(a).

83 *id*., Article 2(b).

84 Of course, in the United States at least, there is a possibility that actions against online service providers relating to the posting of information by users of the service would fail because of the operation of 47 U.S.C. § 230(c)(1) which immunizes Internet intermediaries from suit with respect to the speech of others.

Interestingly, the European Court of Justice (ECJ) in 2003 interpreted Article 3(2) of the Directive as not excusing the mere posting on a publicly available website of gossipy text relating to private individuals by a peer who worked in a church with them.[85] It remains to be seen whether similar reasoning would apply to video, as opposed to text records, or would apply to closed as opposed to open Internet sites. The court's concern in this case appeared to be with data being made available to an indefinite number of people.[86] Would posting information on a closed site such as Facebook meet this criterion when arguably only a limited number of people can access the information? The ECJ was also concerned that particularly sensitive information relating to a health condition – a foot injury – had been disclosed on the Internet.[87] Health information receives special protection under the Directive.[88] It remains to be seen whether the ECJ's reasoning would apply to less sensitive information, such as someone being photographed drinking at a party, or kissing their best friend's girlfriend.

B. LIMITATIONS OF CONTRACTUAL PRIVACY PROTECTIONS

Another possibility for protecting online video privacy might be found in OSNs' terms of use. OSNs currently vary widely in the extent to which they impose terms on their users to respect others' privacy.[89] YouTube and Flickr, for example, allow large scale public dissemination of video with few privacy protections. These services exercise some control over contents,[90] but rely heavily on users to self-police.[91] Yahoo's terms of

---

[85] *Re Bodil Lindqvist*, Paras 46-48 (ECJ, Luxemborg, November 6, 2003, full text available at: http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET, last viewed on December 16, 2008).

[86] *id*., at ¶ 47.

[87] *id*, at ¶ 12.

[88] Data Protection Directive, Art. 8(1) ("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.") (emphasis added)

[89] They can also change them at any time without notice to the consumer. In fact, in the early days of the Internet, a Canadian court expressly recognized a general Internet service provider's ability to do just that – and was prepared to enforce the changed terms: *1267623 Ontario Inc v Nexx Online Inc*, [1999] O.J. No. 2246, ¶ 31 (Court File No. C20546/99, Ontario Superior Court of Justice, Toronto, Ontario, June 14, 1999) ("[Defendant] is permitted to add terms to the Contract precluding a … client sending unsolicited bulk e-mail directly, or through a third party."); Abril and Cava, *supra* note ___, at 267 (noting that online contracts are effectively built on shifting sands and can be changed unilaterally without notice to consumers).

[90] See, for example, clause 7.B of YouTube's Terms of Use: "YouTube reserves the right to decide whether Content or a User Submission is appropriate and complies with these Terms of Service for violations other than copyright infringement, such as, but not limited to, pornography, obscene or defamatory material, or excessive length. YouTube may remove such User Submissions and/or terminate a User's access for uploading such material in violation of these Terms of Service at any time, without prior notice and at its sole discretion." (available at http://youtube.com/t/terms, last viewed on May 14, 2008). However, note that some commentators have suggested that many of these policies are not actually enforced in practice: Sánchez Abril, *Recasting Privacy*, *supra* note ___, at 14, fn 84 (noting that there is little to no apparent enforcement of MySpace's terms of use as an example of lack of effective policing by online social network services providers).

[91] See, for example, clause 6 of Yahoo's Terms of Use relating to "Member Conduct", available at info.yahoo.com/legal/us/yahoo/utos/utos-173.html, last viewed on May 14, 2008; clause 6 of YouTube's

use, for example, which are expressly incorporated into agreements to use Flickr, provide that each subscriber agrees not to use the online service to upload or distribute content that is: "unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, *invasive of another's privacy*, hateful, or racially, ethnically or otherwise objectionable".[92] YouTube's Terms of Use provide that users agree not to post material that is: "copyrighted, protected by trade secret or otherwise subject to third party proprietary rights, including *privacy and publicity rights*" without permission of the rights-holder.[93]

Some closed networks such as Facebook incorporate more strongly worded privacy protections into their terms of use. Not only does Facebook include a clause very similar to the above terms from Yahoo and YouTube,[94] it also requests that its subscribers not use the service to upload: "any videos other than those of a personal nature that: (i) are of you or your friends, (ii) are taken by you or your friends, or (iii) are original art or animation created by you or your friends."[95] Additionally, Facebook's terms of use provide that: "You may not post, transmit, or share User Content on the Site or Service that you did not create or that you do not have permission to post."[96] However, it is not clear whose permission is required to post what information: for example, if I take a group photograph of my high school class, do I have to obtain the whole class' permission to post the photograph? What form does that permission have to take? If I simply ask my classmates at the time of taking the photo whether anyone minds if I post the photo on my Facebook page, and no one expressly objects, would that constitute permission?

What if I take a photograph or video in a crowded mall that includes people I know and people I don't know? Do I need to obtain permission from all the photographic subjects to post the photograph online? What if I take a video of two otters swimming side by side – for some reason a popular YouTube contribution.[97] Whose permission do I need, if any, to show this video online? The zookeeper's? Any bystanders who may appear in the picture? What if one of the bystanders is doing something embarrassing,

---

Terms of Use relating to "User Submissions and Conduct", available at http://youtube.com/t/terms, last viewed on May 14, 2008.

[92] Yahoo's Terms of Use, clause 6(a), available at info.yahoo.com/legal/us/yahoo/utos/utos-173.html, last viewed on May 14, 2008 (emphasis added).

[93] YouTube's Terms of Use, clause 6.D., available at http://youtube.com/t/terms, last viewed on May 14, 2008 (emphasis added).

[94] Facebook's Terms of Use, "User Conduct" clause, available at http://www.facebook.com/terms.php, last viewed on May 14, 2008.

[95] *id.* See also Facebook's Code of Conduct, available at http://www.facebook.com/codeofconduct.php, last viewed on May 14, 2008. Facebook further provides its users with a set of Privacy Principles organized around two "core principles", the second of which states that: "There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.": Facebook Principles, available at http://www.facebook.com/policy.php, last viewed on May 14, 2008.

[96] Facebook Terms of Use, Clause on "User Content Posted on the Site", available at http://www.facebook.com/terms.php, last viewed on May 14, 2008.

[97] YouTube, "Otters Holding Hands" (available at http://www.youtube.com/watch?v=epUk3T2Kfno, last viewed on July 23, 2008).

such as picking her nose or breastfeeding her baby? What if one of the bystanders is kissing or holding hands with a homosexual partner, and it turns out that the person is not openly gay? Do I owe any greater concern for their privacy because of the potential discomfort, embarrassment or harm it might cause them to have people see this conduct online?

With respect to the "permission to post" requirement, it is likely that the drafting intention was to capture permission of those with proprietary interests in relevant content, such as copyrights or trademarks. It seems reasonable to require me to obtain permission to post something, like a movie clip, that might otherwise infringe copyright. However, privacy rights work differently – if at all – in this context because it is not always clear that there is a rights holder in this context as contemplated by many OSN terms of use. Even if there is an obvious victim harmed by the posting of an image, the nature of her legal rights in the image is unclear. Some commentators have suggested that privacy should be treated as an intangible property right,[98] but there is little consensus on this point.[99]

---

[98] SOLOVE, UNDERSTANDING PRIVACY, *supra* note __, at 24-29 (critiquing property based theories of privacy); Jessica Litman, *Information Privacy/Information Property*, 52 STAN L REV 1283, 1288-1294 (2000) (describing various theories of private information as property).

[99] SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 27 ("Extending property concepts to personal information … has difficulties. Information can be easily transmitted and, once known by others, cannot be eradicated from their minds. Unlike physical objects, information can be possessed simultaneously within the minds of millions. This is why intellectual-property law protects particular tangible expressions of ideas rather than the underlying ideas themselves. The complexity of personal information is that it is both an expression of the self and a set of facts – a historical record of one's behavior."); Litman, *supra* note ___, at 1294-1295 ("Whether or not it could be easily implemented, a privacy-as-property solution carries with it some serious disadvantages. Our society has a longstanding commitment to freedom of expression. Property rights in any sort of information raise significant policy and free speech issues. Facts are basic building blocks: building blocks of expression; of self-government; and of knowledge itself. When we recognize property rights in facts, we endorse the idea that facts may be privately owned and that the owner of a fact is entitled to restrict the uses to which that fact may be put. That notion is radical. It is also inconsistent with much of our current First Amendment jurisprudence. Thus, the idea of creating property rights in personal data raises fundamental constitutional issues. If it looked likely that a property rights model would prove to be an effective tool for protecting personal data privacy, it might be worthwhile to balance the privacy and free speech interests to see which one weighed more. [H]owever, a property rights model would be ineffective in protecting data privacy. It would, in all likelihood, make the problem worse."); Richard Posner, *The Right of Privacy*, 12 GEORGIA LAW REVIEW 393, 397-401 (1978) (critiquing theories that favour personal property rights in private information); Diane Leenheer Zimmerman, *Is There a Right to Have Something to Say? One View of the Public Domain*, 73 FORDHAM L REV 297, 348-9 (2004) ("[F]rom the birth of the common law right of privacy, courts recognized that there is a downside to granting individuals control over how others can use information about them. It significantly strips others of the wherewithal to form their own ideas, utilize their own observations, and communicate about these things with friends, colleagues, and fellow citizens. The fear of this unconstitutional consequence is why broad newsworthiness rules have cabined the tort almost to the point of annihilation. This strongly suggests that the ability to use speech goods is a necessary element of what the First Amendment protects, and that, as a result, it is very risky to allow individuals to "own" or control use of their life stories.") [hereinafter, *The Public Domain*]; Diane Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WILLIAM AND MARY LAW REVIEW 665 (1992) (arguing that the increasing commodification of information potentially impinges on First Amendment freedoms) [hereinafter, *Information as Speech*].

What about the question of the standing of a video subject to bring a complaint under an OSN's terms of use? Even if that person can establish a sufficient legal interest in her image to satisfy the "permission to post" aspect of an OSN's terms of use, her recourse would be to complain to the OSN provider. It would be up to the provider to decide whether the complaint had any merit, and whether to take any action against the subscriber, such as removing the posting, or barring the subscriber from the system.[100] The complainant probably has no standing to sue the service provider directly because she is not a party to the subscriber's contract with the service provider. Additionally, at least in the United States, § 230 of the Communications Decency Act probably immunizes the service provider from secondary liability for its subscribers' postings.[101]

There are further limitations with relying on OSNs' terms of use to protect privacy. Even Facebook's requirement that users limit their postings to photographs of themselves and their friends, or photographs taken by themselves or their friends, is open to interpretation. On a closed network like Facebook, the term "friends" means something different to the way we use the term in the physical world.[102] In the physical world, we know whether or not we are acquainted with a person. We may not know them, and we may even have forgotten their name, but we are unlikely to consider someone we have never met a "friend".

This is quite different online. A "friend" on Facebook is anyone who has given you permission to join their online network of "friends", whether or not they have ever met you. Although Facebook contemplates that its subscribers will use the service to find people online whom they already know in the real world,[103] there is no way to ensure that this is the case in practice. It is easy to make anonymous online contacts on Facebook, and for those contacts to quickly be considered "friends". These contacts will increase the potential recipients of information on a subscriber's site to many people whom the subscriber, and the subject of any information on the subscriber's website, may not

---

[100] See, for example, YouTube's Terms of Use, Clause 7.B ("YouTube reserves the right to decide whether Content or a User Submission is appropriate and complies with these Terms of Service for violations other than copyright infringement, such as, but not limited to, pornography, obscene or defamatory material, or excessive length. YouTube may remove such User Submissions and/or terminate a User's access for uploading such material in violation of these Terms of Service at any time, without prior notice and at its sole discretion."), available at http://youtube.com/t/terms, last viewed on May 14, 2008.

[101] 47 U.S.C. § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. ")

[102] ZITTRAIN, *supra* note ___, at 218 (noting that a person's "friends" network online includes their "friends' friends' friends."); See Abril and Cava, *supra* note ___, at fn 69 ("The online social networking environment has brought about a sweeping change in its users' notions of intimacy, friendship, and confidentiality.")

[103] For example, Facebook's information on finding friends online states that: "Your friends on Facebook are the same friends, acquaintances and family members that you communicate with in the real world." (available at https://register.facebook.com/findfriends.php?ref_friends, last viewed on May 14, 2008). Facebook also prohibits the use of aliases online so that people who think they are being contacted by someone they actually know are really being contacted by that person: for example, the User Conduct clause of Facebook's Terms of Use prohibits impersonating any person, falsely representing yourself, and creating a false identity (available at http://www.facebook.com/terms.php, last viewed on May 14, 2008).

actually know.[104] Thus, "friends" in a closed network's terms of use may be a deceptively comforting concept.[105] Commentators have recognized a number of additional limitations with relying on contractual mechanisms to protect privacy online. These limitations include the fact that such contracts are often not consistently enforced,[106] and the fact that there are insufficient inexpensive and accessible online dispute resolution services available for contract-based disputes.[107] Another shortcoming of reliance on contractual privacy protections is the fact that the onus is currently on users of an online service to continually check back for changes in privacy policies.[108] As these policies often vary from service to service, and Internet users tend to use a variety of services,[109] this can be a particularly onerous burden. Contractual terms about privacy are also often written in abstruse or legalistic terms which are difficult for users to comprehend.[110]

---

[104] Of course, the practical problems can potentially be greater on an open network that does not even attempt to limit dissemination of information to "friends".

[105] One could argue that in the online world individuals have a responsibility to exercise more care than they currently do about who they befriend. The problem is that this is easier said than done. In the real world there are physical constraints on who can be befriended and how many friends one can make – in terms of time and geography. Additionally, in the physical world, one can glean more cues than in virtual space about whether the rewards of befriending someone outweigh the risks. These cues come from watching the person interact in real world situations. In physical spaces, we also recognize different "levels" of friendship. We can thus repose less trust in someone we do not know very well. In the OSN context, however, the choice is effectively binary – someone is either your "friend", entitling them access to anything you post online, or they are not your friend, and therefore not entitled to access your online materials at all: SOLOVE, THE FUTURE OF REPUTATION, *supra* note __, at 202 (noting that technologies like Facebook require a binary definition of the term "friend" – a "friend" is permitted access to your information while a non-friend is not - while a social network in the real world is much more complex). There are no gradations of friendship online, although there is no necessary technological impediment to developing such levels. A system could be developed in the future that would allow users to exercise discretion about who received what, and how much, information from them. This could be done by building more "levels of friendship" into OSN technologies. Thus, one could identify online peers as either "good friends", "friends", or "acquaintances" and differentiate levels of access to personal information accordingly. Abril and Cava, *supra* note ___, at 272 (suggesting the development of levels or "zones" of relationships in the context of private health information available online).

[106] Abril and Cava, *supra* note ___, at 267 ("Spotty enforcement and lack of mechanisms for dispute resolution further weaken the power of contract law online.")

[107] *id.*

[108] *id*. ("Website contracts are built on shifting sands. The professed ability of many operators to change terms of use at any moment and without prior notice leaves users in a constant state of uncertainty about their rights and privacy expectations.")

[109] *id*. ("[T]erms of use and privacy policies vary from website to website, making true understanding of each contract … difficult and impracticable, especially since most users visit several websites a day."

[110] *id*. ("Many user contracts are written abstrusely or in a legalistic style, dissuading even the most punctilious consumer from taking time out of her online pursuit to carefully read and understand them.")

III. WHY (NOT) REGULATE VIDEO PRIVACY?

A. JUSTIFICATIONS FOR VIDEO PRIVACY REGULATION

So far, this article has addressed practical problems relating to digital video privacy, and gaps in the existing legal framework. The next step is to find justifications for a new approach to video privacy. In doing so, four potential criticisms of the idea of taking a new regulatory approach should be addressed. They include the argument that there is no accepted theoretical basis for regulating privacy. It is not clear whether privacy is a property right, an aspect of personhood, or something else. In the absence of a clear and unified theoretical underpinning for privacy rights, some may argue that regulation is undesirable. The second reservation against video privacy regulation is the argument that it is more appropriate to regulate specific harms resulting from discrete privacy incursions than to regulate privacy more generally. Discrete harms may include loss of employment[111] or employment prospects,[112] physical injury,[113] psychological harm,[114] and denial of access to education or health services. A third reservation about video privacy regulation would suggest that the First Amendment may be an insurmountable barrier to the regulation of truthful speech about private individuals, at least in the United States. And a final concern about regulating video privacy is the idea that such regulation is impracticable because of the scale and global nature of online privacy problems. The remainder of this article addresses these issues and suggests a way forward by creating a multi-modal framework for online video privacy regulation.[115]

B. THE SEARCH FOR A UNIFIED THEORY OF PRIVACY

One thorny issue in any discussion of reworking or extending privacy protections is the question of the theoretical basis on which this might be done. Despite well over a century of discourse about the legal nature of privacy, no clear consensus has emerged.[116]

---

111 As in the "dog poop girl" example: see Part I *supra*.

112 As in the AutoAdmit case involving the unauthorized posting of sexually explicit information about Yale students, one of whom alleged she lost a job offer as a result of the posting: see Isaac Arnsdorf, *AutoAdmit Case Moves Forward*, YALE DAILY NEWS, Jan, 31, 2008 (available at http://www.yaledailynews.com/articles/view/23231, last viewed on January 12, 2009).

113 As in the "bus uncle: example: see Part I *supra*.

114 As in the case of "Star Wars kid": see Part I *supra*.

115 The first three issues are addressed in Part III *infra*, while the final issue about the practicality of regulating for video privacy online is addressed in Part IV *infra* along with the discussion of a suggested framework for video privacy regulation.

116 In fact, even Professor Solove's groundbreaking attempts to create a conception or taxonomy of privacy are not pinned down to one concrete unifying theory: SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 105 ("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…."); Daniel Solove, *Conceptualizing Privacy*, 90 CALIFORNIA L REV 1087, 1129 (2002) ("[T]his Article advances as "approach" to understanding privacy rather than a definition or formula for privacy….My approach is from the bottom up rather than the top down because it conceptualizes privacy within particular contexts rather than in the abstract.") [hereinafter, *Conceptualizing Privacy*].

Some commentators have argued that it is not necessary to identify any one unifying theoretical framework for privacy in order to regulate it effectively.[117] They suggest that if we can identify actual harms relating to privacy, this is a sufficient basis to formulate a regulatory framework.[118] This may be the right approach, even if it is not theoretically satisfying or complete.

This approach is also not as unusual as it might seem. Many legal rights –notably intangible property rights - developed organically as the need arose.[119] Trademarks, for example, developed to address the need to prevent unfair competition relating to false or misleading branding of goods or services.[120] There is still some dispute as to whether trademarks are appropriately characterized as property rights as a matter of theory.[121] Nevertheless, the system still works in practice. Trade secrets are another example where theoretical justifications are varied.[122] Nevertheless, the system continues to function. Even Internet domain names have an uncertain legal status as property.[123] Nevertheless,

---

117 *id.*

118 *id.*

119 Of course, there are costs and benefits to this approach. Organic development can fail to take into account the complex matrix of interests that need to be balanced, such as the need to balance free speech interests against property interests, and to distinguish different types of information speech and information property: see, for example, discussion in Zimmerman, *Information as Speech, supra* note ___. It is also possible that an organic approach might miss a critical period for regulatory decision-making after which regulations are difficult to implement and enforce, particularly if they would contradict entrenched social norms of behavior: see Gaia Bernstein, *The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONNECTICUT L REV 241 (2006) [hereinafter, *Paradoxes*]; Bernstein, *New Technologies*, *supra* note ___. These articles are in reality advocating an approach that allows for some organic/incremental development while at the same time being sensitive to points at which legal regulation – or other regulatory approaches discussed in Part IV – are necessary.

120 LEXIS, TRADEMARK AND UNFAIR COMPETITION DESKBOOK, § 1.01.

121 Mark Lemley, *The Modern Lanham Act and the Death of Common Sense*, 108 YALE L J 1687, 1693-1694 (1999) (noting in the context of United States law that it is very difficult to find a rationale to treat trademarks as a form of property). This may be compared with jurisdictions like the United Kingdom and Australia where trademarks are explicitly defined as a form of personal property in the relevant legislation: Trade Marks Act, U.K. § 2(1) (1994) ("A registered trade mark is a property right obtained by the registration of the trade mark under this Act and the proprietor of a registered mark has the rights and remedies provided by this Act."); Trade Marks Act, Austl., § 21(1) (1995) (specifically defining a "trade mark" as a personal property right).

122 Jacqueline Lipton, *Protecting Valuable Commercial Information in the Digital Age: Law, Policy, and Practice*, 6 JOURNAL OF TECHNOLOGY LAW AND POLICY 1, 9-15 (2001) (comparing the theoretical treatment of trade secrets in different jurisdictions, including Australia, the United Kingdom, and the United States) (full text available at: http://grove.ufl.edu/~techlaw/vol6/issue1/lipton.html, last viewed on July 24, 2008).

123 For example, in some contexts domain names have been regarded as a form of intangible personal property: *Kremen v Cohen*, 337 F. 3d 1024 (9th Cir. 2003) (domain names treated as property for the purposes of California's conversion law); 15 U.S.C. § 1125(d)(2)(A) (allowing *in rem* proceedings against domain names as property in certain circumstances). See also discussion in MILTON MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE, 58-61 (2002) (discussing the nature of claims to property rights in domain names). In other context, domain names are regarded as the object of a contractual license with a registering authority: *Network Solutions, Inc v Umbro International Inc*, 529 S.E.2d 80 (Va. 2000) (domain names not regarded as a new form of property for the purpose of garnishment proceedings).

the domain name system continues to function, while market forces, social norms, and judicial and arbitral decisions[124] iron out the underlying philosophical creases.

Could privacy similarly emerge as an intangible property right over time? Property rights in information have always been contentious.[125] They create concerns about chilling speech.[126] Governments who create property rights in information must act to preserve the balance between those rights and speech. This is a difficult task and is not always successfully achieved in practice.[127] There is also the valid question as to why personal information should be regarded as property in the hands of its subject. It is tempting to say that if something has value, as private information potentially does,[128] it should be treated as property. The problem with this reasoning is that much of the economic value in online information has been in text records in the hands of data aggregators.[129] While there may be good reasons to create property in compilations of text records,[130] it is not necessarily clear that personal information in the hands of the individual to whom it relates is a valuable commodity in its own right.[131]

---

[124] Arbitral decisions on domain names are actually very common under the Uniform Domain Name Dispute Resolution Policy incorporated by reference into many domain name contracts: see http://www.icann.org/en/udrp/udrp-policy-24oct99.htm, last viewed on October 14, 2008.

[125] SOLOVE, UNDERSTANDING PRIVACY, *supra* note __, at 24-29 (critiquing property based theories of privacy); Litman, *supra* note ___, at 1288-1294 (describing various theories of private information as property).

[126] Litman, *supra* note ___, at 1294-1295; Zimmerman, *The Public Domain*, *supra* note ___, at 310, 348-9; Zimmerman, *Information as Speech, supra* note ___ (arguing that the increasing commodification of information potentially impinges on First Amendment freedoms).

[127] In a federal system, the propertization of information can raise constitutional questions about which level of government has legislative competence to enact relevant laws. Perhaps even more significantly, some have argued that no government may have constitutional competence to recognize or create property rights in factual personal information because of potential encroachments on First Amendment freedoms. See discussion in SOLOVE, THE FUTURE OF REPUTATION, *surpa* note ___, at 129-132 (describing problems in attempting to balance privacy torts with the idea of free speech); Diane Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L REV 291 (1983) (suggesting that torts prohibiting true speech cannot be reconciled with the First Amendment) [hereinafter, *Requiem*]; Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN L REV 1049 (2000) (suggesting that tortious approaches to protecting privacy cannot be reconciled with the First Amendment, but that contractual approaches may avoid this criticism); See Zimmerman, *The Public Domain*, *supra* note ___, at 298, 312, 366, 369 (arguing in favor of a mandatory public domain which may encroach on the government's ability to create property rights that would interfere with the public domain of information and ideas).

[128] SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, 78-100 (detailed attempt to ascribe various possible values to different aspects of privacy).

[129] A. Michael Froomkin, *The Death of Privacy?*, 52 STANFORD L REV 1461, at 1502-3 (2000) (noting that the value of a piece of data in a consumer's hands is much less than the value of the aggregated data about many consumers in a data aggregator's hands).

[130] See, for example, Jerome Reichman and Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND L REV 51 (1997); Jacqueline Lipton, *Balancing Private Rights and Public Policies: Reconceptualizing Property Rights in Databases* 18 BERKELEY TECHNOLOGY LAW JOURNAL 773 (2003).

[131] Froomkin, *supra* note ___, at 1502-3 (noting that the value of a piece of data in a consumer's hands is much less than the value of the aggregated data about many consumers in a data aggregator's hands).

Arguments have been made that property rights would give a data subject more control over the information in a transactional sense.[132] However, if individuals have insufficient economic bargaining power against data aggregators, the existence of a property right in the hands of the individual will be of limited practical use. In the OSN context, there is arguably even less need to recognize a property right to protect individual privacy in video images – at least if the justification for the property right is based on economic value and bargaining power. This is because private individuals networking over OSNs are not likely doing so for transactional purposes that would justify or necessitate a property right in their personal information.[133] Of course, not all property rights are justified on the basis of economic value.[134] Many conceptions of property do rely on economic value.[135] While value and property are often aligned, it is not necessarily the case that something must be commercially valuable to be property or that something must be property if it has a commercial value.[136]

Putting economic value aside, property rights may be characterized by other attributes: the ability to exclude others; the ability to enjoy an item free from interference; or, the ability to alienate or transfer rights whether or not for commercial value.[137] These typical proprietary attributes are generally missing from personal information. It would be difficult for an individual to function in society, particularly online, without leaving footprints involving disclosures of personal information. Thus, there is no way of excluding others from personal information or of enjoying the information free from interference. Sometimes information is required by others, as by

---

[132] Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 687 (2000) ("Simply put, if information about us is to be bought and sold, the initial purchase should be from us, since we are the ultimate content providers. If intangible property rights are rewards for the effort expended in creating the thing to be protected, we are entitled to ownership of our personal information.")

[133] There may be a justification for imputing a property right to the OSN provider in respect of its meta-collection of data on the grounds that OSN operators do utilize this data for commercial purposes. However, even that argument is tenuous in situations where an OSN does not transact with the data *per se*, but rather utilizes its vast user base as an incentive to attract advertisers. This may be changing in practice. Recent attempts at social ad programs by some OSNs do utilize specific data about individuals and their online relationships with friends to better target advertising to their users: William McGeveran, *Facebook Inserting Users Into Ads*, Info/Law, November 8, 2007 (available at http://blogs.law.harvard.edu/infolaw/2007/11/08/facebook-social-ads/, last viewed on July 24, 2008); Megan McCarthy, *Facebook Ads Make You the Star – and You May Not Know It,* Wired Blog Network, January 2, 2008 (available at http://blog.wired.com/business/2008/01/facebook-ads-ma.html, last viewed on July 24, 2008).

[134] In fact, Professor Charles Fried implicitly accepted the proprietary nature of privacy in the context of interpersonal relationships where the privacy right would have no real economic value, but would have a social value: Charles Fried, *Privacy*, 77 THE YALE LAW JOURNAL 475, 487 (1968) (describing privacy as a form of "moral capital for personal relations" and referring to holding "title" to information about oneself).

[135] LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY, 19 (2004) ("But the "if value, then right" theory of creative property has never been America's theory of creative property. It has never taken hold within our law.") [hereinafter, FREE CULTURE]

[136] *id.* An old dog-eared copy of a Shakespeare play, for example, may no longer have any economic value, but it will still be property. On the other hand, a person's time may be valuable, but it will not necessarily be property.

[137] Courtney Tedrow, *Conceptual Severance and Takings in the Federal Circuit*, 85 CORNELL L REV 586, 591 (2000) (identifying classic property rights as including rights of exclusion, disposition, and use).

contract, to complete a purchase.[138] Other times the information is incidentally observed as part of functioning in society: for example, if you go to the shops, people will see what you look like, an image of you may be captured on a security camera in a department store, etc.[139] Online, individuals constantly leave digital footprints involving this kind of information.[140]

Of course, advocates of property rights in personal information may argue that it is these very aspects of personal privacy that require a property label. The necessity of transacting with this information on a daily basis requires that individuals be entitled to bargain for exchanges involving the information.[141] However, this is a circular argument. It assumes that something should be labeled property because individuals are forced to disclose it, and therefore they should be compensated for doing so.[142] Outside of property theory, there may be arguments based on autonomy and personhood for granting legal rights in personal information to a data subject.[143] In attempts to explain the philosophical underpinnings of the right of publicity, which is derived from the right to privacy, commentators have suggested basing such rights in notions of autonomy and personhood.[144] This is a possibility, but the theoretical contours of rights of personhood are unclear.[145] In the end, this theory may not be any more useful than trying to pin down privacy as a form of property. Ultimately, those who argue in favor of taking a bottom up approach to developing privacy regulation in the absence of one clear unifying theory probably have the right idea, at least for the present time.[146] Privacy harms today are real

---

138 For example, details of a credit card or postal address for payment or shipping purposes.

139 Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN L REV 1193, 1198 (1998).

140 *id*.

141 Bartow, *supra* note ___, at 704 ("Once I own my own data, I personally look forward to formulating a reverse "click-wrap" license, whereby any enterprise that wants me to visit its web site will have to agree to MY list of terms and conditions …").

142 Maybe this could be justified on the basis of unjust enrichment. In other words, data aggregating businesses are unjustly enriched by individuals if they can put together valuable consumer profiles using information "belonging to" consumers without compensating them for it. However, this analysis also assumes the existence of an underlying property or quasi-property right in the plaintiff's personal information, so it is again circular: Andrew Kull, *Rationalizing Restitution*, 83 CALIF L REV 1191, 1214 (1995) ("Restitution can be seen as an aspect of the legal protection of property, and many instances of what the law characterizes as unjust enrichment might be described by saying that the defendant has received property of the plaintiff by means of a transfer that was legally ineffective to convey ownership.")

143 Solove, *Conceptualizing Privacy*, *supra* note __, at 1116-1121 (discussion of personhood theories of privacy); Daniel Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO LAW REVIEW 745, 760-1 (2007) (noting that many theories of privacy view the notion of privacy as an individual right related to protecting the individual's personal dignity) [hereinafter, *Nothing to Hide*]; Sánchez Abril, *Recasting Privacy*, *supra* note ___, at 7-8 ("[O]thers have defined privacy in terms of personhood, intimacy, and secrecy."); SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 29-34 (critiquing "personhood" theories of privacy); Friend, *supra* note ___, at 483 (describing privcy as an "aspect of personal liberty").

144 See discussion in Jacqueline Lipton, *Celebrity in Cyberspace: A Personality Rights Paradigm for Personal Domain Name Disputes*, forthcoming, 65 WASHINGTON & LEE LAW REVIEW 1445 (2008).

145 In the right of publicity context, see, for example, discussion in Mark McKenna, *The Right of Publicity and Autonomous Self-Definition*, 67 U PITT L REV 225 (2005); Alice Haemmerli, *Whose Who? The Case for a Kantian Right of Publicity*, 49 DUKE L J 383 (1999).

146 SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 105 ("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

and observable, and the search for a single unifying theory may take too long to address the pressing needs facing online societies today.[147]

C. REGULATING SPECIFIC HARMS

This reasoning perhaps leads logically to the question that if privacy harms are real and observable, why not redress specific harms rather than regulating to protect privacy more generally? A number of commentators have suggested that the former approach is preferable, largely because of First Amendment concerns and because of the thought that attempting to regulate privacy online today is like locking the barn door after the horse has bolted.[148] These commentators have suggested that the best approach to remedying privacy breaches in the twenty-first century is to focus on specific damages caused by leaks of personal information, including discrimination in the workplace, healthcare, and education.[149] Indeed, some have suggested that the benefits of lack of privacy could theoretically outweigh the costs.[150] Some have even argued that the wide-scale dissemination of personal information is beneficial in that it can actually help the public to understand existing social norms.[151] However, there is reason to be skeptical of an approach that fails to consider privacy as something worthy of protection in and of itself. For one thing, many insecurities involving personal information do not result in specific damage. Widespread unregulated online privacy incursions can create a general culture of unease where individuals cannot rely on anyone to respect personal boundaries.[152]

While there are good reasons for the law to address specific harms that result from privacy breaches, such as dog poop girl's loss of her job and Star Wars kid's need for psychological treatment, this does not preclude the need to adopt some regulations that temper unbridled incursions into people's privacy by means of digital video technologies.

---

approach to a bottom-up focus on problems that are all related to each other, yet not in exactly the same way. If we study the problems together, we can better understand the entire cluster.")

147 Bernstein, *New Technologies*, *supra* note ___.

148 Scott McNealy, CEO of Sun Microsystems said famously in 1999: "You have zero privacy. Get over it.": Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED, January 26, 1999 (available at http://www.wired.com/politics/law/news/1999/01/17538, last viewed on July 25, 2008).

149 DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998); SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 73-74; Strahilevitz, *Reputation Nation, supra* note ___ (arguing that basing decisions on real information rather than dangerous and discriminatory proxies such as race actually provides social benefits overall).

150 Strahilevitz, *Reputation Nation, supra* note ___ (arguing that basing decisions on real information rather than dangerous and discriminatory proxies such as race actually provides social benefits overall); Volokh, *supra* note ___, at 1120 (the government should not use privacy torts as a proxy for anti-discrimination laws); DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE USE TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).

151 Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U CHI L REV 919, 928 (2005) ("[D]issemination [of personal information] can also help the public understand existing social norms. Indeed, gossip is often central in theories of social norm enforcement and change.")

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

Some legislation has been developed to regulate intrusive digital video photography.[153] However, what is missing is regulation of online distributions of personally humiliating, embarrassing, or damaging images.

D. PRIVACY AND THE FIRST AMENDMENT

Of course, regulating privacy involves incursions on truthful expression. This obviously runs up against the First Amendment. Professors Zimmerman and Volokh have expressed concerns that privacy torts in particular are open to criticism as unconstitutional encroachments on First Amendment freedoms.[154] These scholars would likely be unconvinced of arguments in favor of increasing the strength and scope of these torts in the online world. However, that is not to say that there is no way of better protecting privacy online without damaging First Amendment freedoms. Even First Amendment scholars have recognized other avenues for protecting privacy, including express and implied contracts of confidentiality, and extended breach of confidence actions.[155] This article also relies on an expanded concept of regulation as a multi-modal enterprise that does not rely on legislation alone to protect privacy interests. While the First Amendment aims to protect individual freedoms against government intrusions, it will generally allow societies to develop social norms, market forces, and technological solutions to perceived social problems.[156] Thus, the only question remaining is *how* an effective multi-modal regulatory framework for digital video privacy might be developed, particularly given the global scope of online video privacy problems.

IV. A MULTI-MODAL APPROACH TO VIDEO PRIVACY

There will be no single sweeping reform that will bestow privacy on each of us.

\- Professor Jon Mills[157]

---

153 See, for example, Camera Phone Predator Alert bill, H.R. 414 (111th Cong., 2009); Cal. Civ. Code §1708.8(b) ("A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.")

154 Volokh, *supra* note ___, at 1051 ("While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law."); 1122 ("restrictions on speech that reveals personal information are constitutional under current doctrine only if they are imposed by contract, express or implied"). Professor Zimmerman has also argued against the constitutionality of privacy tort law on free speech grounds: Zimmerman, *Requiem*, *supra* note ___.

155 See discussion in Part IV.A.5 *infra*.

156 For a contrasting view, see Dawn Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH L J 1115 (2005) (expressing concern that the increasing control of public forums for speech in private hands, such as OSN providers, will curtail meaningful First Amendment scrutiny and led to privacy and arbitrary decisions about what kinds of speech are available online).

157 MILLS, *supra* note ___, at 306.

The first and most important point to acknowledge about online video privacy regulation is that there is no one solution to digital age privacy problems[158] However, this does not mean that it is futile to pursue enhanced privacy protections. It simply means that regulation must be organic, adapting to societal needs as they develop. It also means that we will likely need a more nuanced approach than simply relying on legislation and the courts. Professor Lawrence Lessig famously identified four regulatory modalities that would be useful in cyberspace generally, and that would help to develop protections for online privacy in particular.[159] These modalities comprised legal rules,[160] social norms,[161] markets,[162] and system architecture.[163]

Social norms are similar to legal rules in that they threaten punishment for disobedience.[164] However, they differ from laws in that punishments are imposed by communities, rather than government.[165] Norms can be as effective, if not more effective, than legal rules.[166] The informal penalties for violating norms, while often less severe than legal punishments, have a greater likelihood of being enforced than a legal rule in

---

158 *id*.

159 Lawrence Lessig, *The Architecture of Privacy*, 1 VANDERBILT J ENT L & PRAC 56, 62-3 (1999) [hereinafter, *The Architecture of Privacy*].

160 Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARVARD L REV 501, 507 (1999) ("Law … orders people to behave in certain ways; it threatens punishment if they do not obey. The law tells me not to buy certain drugs, not to sell cigarettes without a license, and not to trade across international borders without first filing a customs form. It promises strict punishments if these orders are not followed. In this way, we say that law regulates.") [hereinafter, *The Law of the Horse*].

161 *id.* ("Norms control where I can smoke; they affect how I behave with members of the opposite sex; they limit what I may wear; they influence whether I will pay my taxes. Like law, norms regulate by threatening punishment ex post. But unlike law, the punishments of norms are not centralized. Norms are enforced (if at all) by a community, not by a government. In this way, norms constrain, and therefore regulate."). Not all norms will threaten punishment for disobedience. Some norms can be maintained without any penalty for violation: Strandburg, *supra* note___, at 1246-9 ("coordination norms" can be maintained without imposing sanctions for noncompliance because individuals have no incentive to deviate from norms that depend on a large group of people performing the same action in the same way; "epistemic norms" do not require sanctions because individuals conform to these norms as a means of economizing information costs so there is no incentive for others to enforce the norms against individuals).

162 Lessig, *The Law of the Horse, supra*, note ___, at 507 ("Markets, too, regulate. They regulate by price. The price of gasoline limits the amount one drives - more so in Europe than in the United States. The price of subway tickets affects the use of public transportation - more so in Europe than in the United States.")

163 *id*., at 507-509 ("[T]here is a fourth feature of real space that regulates behavior - "architecture." By "architecture" I mean the physical world as we find it, even if "as we find it" is simply how it has already been made. That a highway divides two neighborhoods limits the extent to which the neighborhoods integrate. That a town has a square, easily accessible with a diversity of shops, increases the integration of residents in that town. That Paris has large boulevards limits the ability of revolutionaries to protest. That the Constitutional Court in Germany is in Karlsruhe, while the capital is in Berlin, limits the influence of one branch of government over the other. These constraints function in a way that shapes behavior. In this way, they too regulate.")

164 *id*, at 507. Subsequent literature has demonstrated that norms are actually more complex than this, and that there are various different kinds of norms that operate in different ways: Strandburg, *supra* note ___. However, for the purposes of this discussion, Lessig's definition will suffice.

165 *id.*

166 Strandburg, *supra* note ___, at 1248 ("Social norms often play a more important role than legal regulation.")

many contexts.[167] Markets regulate by imposing price constraints on certain behaviors.[168] One example in the privacy context would be where online firms charge more to consumers for providing greater assurances of personal privacy.[169] Architecture, on the other hand, regulates by physically constraining certain behaviors.[170] In the real world, for example, the erection of a border fence may constrain illegal immigration.[171] The cyberspace analog to physical world architecture is system architecture or "code".[172]

None of these modalities operates in a vacuum. Their interaction facilitates given behaviors.[173] Additionally, these modalities are not comprehensive. There are other modalities that usefully regulate online conduct. Thus, we might also recognize modalities such as public education,[174] and, private/non-profit institutions.[175] The institutions comprised in the latter category might include OSNs themselves, but perhaps more to the point, public interest organizations like the Electronic Frontier Foundation

---

167 *id*, ("When social norms are feasible they can be quite effective. Though the informal penalties for violating social norms may be less severe than the penalties available under the law, the likelihood of being penalized may be quite high.").

168 Lessig, *The Law of the Horse, supra*, note ___, at 507.

169 Lessig, *The Architecture of Privacy*, *supra* note ___, at 62. Of course, Professor Lessig here may have been contemplating privacy protections for posters customers of service providers who are more likely to be *posters* of private information than victims of unauthorized postings of private information by others. However, this would depend upon the scope and nature of the privacy policy promulgated by a given online service provider. Where an online service provider offered to protect privacy of both posters and subjects of information and images, more people may be drawn to that service provider because of the signals the service provider gives about being a generally good online corporate citizen. Some online service providers do currently at least purport to protect the privacy of third parties as well as their own customers – see discussion of relevant terms of use in Parts II.B and IV.A.5.

170 Lessig, *The Law of the Horse, supra* note ___, at 507-508.

171 SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 98-99 (giving examples of ways in which physical architectures can constrain behavior); LESSIG, FREE CULTURE, *supra* note ___, at 122 (2004) ("A fallen bridge might constrain your ability to get across a river. Railroad tracks might constrain the ability of a community to integrate its social life. As with the market, architecture does not effect its constraint through ex post punishments. Instead, also as with the market, architecture effects its constraint through simultaneous conditions.").

172 Lessig, *The Law of the Horse, supra* note ___, at 509 ("[T]he architecture of cyberspace, or its code, regulates behavior in cyberspace. The code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave.")

173 LESSIG, FREE CULTURE, *supra*, note ___, at 123 ("[T]he first point about these four modalities of regulation is obvious: They interact. Restrictions imposed by one might be reinforced by another. Or restrictions imposed by one might be undermined by another."). See also Froomkin, *supra* note ___, 1466 ("While there may be no single tactic that suffices to preserve the status quo, much less regain lost privacy, a smorgasbord of creative technical and legal approaches could make a meaningful stand against what otherwise seems inevitable."); Lessig, *The Law of the Horse, supra* note ___, at 511-534; Lessig, *The Architecture of Privacy*, *supra* note ___, at 63-64 (suggesting a combined arhictecture/market solution to protecting privacy online, that relies in part on use of the Platform for Privacy Preferences (P3P) designed by the World Wide Web Consortium).

174 Lilian Edwards and Ian Brown, *Data Control and Social Networking: Irreconcilable Ideas?*, at ___ in ANDREA M MATWYSHYN (ed), HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION, forthcoming, 2008; SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 203-204.

175 Richards, *Intellectual Privacy*, *supra* note ___, at 33 (discussing the American Libraries Association's role of protecting patron's rights and freedoms in the library bill of rights in 1939 as an example of an institution playing a regulatory role in promoting individual privacy).

(EFF)[176], the Electronic Privacy Information Center (EPIC),[177] and perhaps also academic institutions.[178] The remainder of this Part identifies the key features of each of these six modalities, and ways in which they might interact to provide more effective protections for online privacy.

A. LEGAL RULES

1. The Role of Law Online

> *[L]egal rules … play a large part in establishing the social context of privacy …. [P]rivacy is not just an absence of information abroad about ourselves; it is a feeling of security in control over that information. By using the public, impersonal and ultimate institution of law to grant persons this control, we at once put the right to control as far beyond question as we can and at the same time show how seriously we take that right.*
>
> - Professor Charles Fried[179]

Lawyers have a tendency to regard legal rules as the paramount – and sometimes the only – solution to a problem.[180] However, laws have limits, especially online. In particular, effective enforcement mechanisms can be problematic where harmful conduct involves anonymous wrongdoers who could be situated anywhere in the world. Additionally, legislatures are often faced with complex policy choices in balancing competing interests such as privacy, speech, and intellectual property rights online. The novelty of much online conduct can exacerbate these difficulties. Governments often look to social norms to discern an appropriate policy basis for new laws. In areas like online social networking, where many social norms are not fully developed, governments may have difficulty identifying appropriate directions for new laws.[181] The legislature is then faced with questions as to whether it should attempt to create and communicate new norms through its laws, or to wait and see what norms develop before legislating.

---

176 The Electronic Frontier Foundation describes itself as: "leading civil liberties group defending your rights in the digital world." (see www.eff.org, last viewed on July 23, 2008).

177 The Electronic Privacy Information Center describes itself as: "a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values." (see www.epic.org, last viewed on July 23, 2008). The identification of new forms of regulatory modality is not inconsistent with Professor Lessig's work – he did not intend for his four regulatory modalities to be the last word on cyberspace regulation: LESSIG, FREE CULTURE, *supra* note ___, at 123 ("Whether or not there are other constraints (there may well be; my claim is not about comprehensiveness), these four are among the most significant…").

178 See discussion in Part IV.F *infra*.

179 Fried, *surpa* note ___, at 493.

180 LESSIG, FREE CULTURE, *supra* note ___, at 121 ("Law is the most obvious constraint (to lawyers at least).")

181 In contrast to this, some have argued that it is necessary for decision-makers, including legislatures often to consider acting *before* social norms have developed because failure to do so may result in an inability to effectively regulate inconsistently with norms where the need arises: Bernstein, *New Technologies, supra* note ___, at 943-946 (including a discussion of entrenchment of anti-privacy norms on the Internet in the context of electronic commerce).

Legal rules are therefore unlikely to be the answer to online video privacy problems.[182] They will have an important place[183] in the regulatory matrix, but they cannot resolve online privacy issues on their own. The challenge for regulators will be to identify exactly what role legal rules should play, and how those rules should interact with other forms of regulation. Recently, commentators have suggested that online privacy regulation could be improved if law: recognized privacy in public;[184] better protected confidential relationships;[185] and allowed individuals to exercise greater control over their personal information after it has been exposed to other people or even to the general public.[186] Various approaches to legal regulation might prove fruitful in the video privacy context. Privacy law might usefully draw on some of the lessons learned from digital copyright law and environmental regulation. Additionally, privacy torts could be updated to better protect online video privacy. Law might also promote contractual and technological solutions to online video privacy problems. The following discussion considers each of these possibilities in turn.

2. Lessons from Digital Copyright Law

The case for drawing ideas from copyright law should not be overstated because of concerns that copyright law has over-propertized online information in the digital age.[187] Nevertheless, there are some salient parallels between online privacy and the protection of copyright works online.[188] Copyright law has been very successful in protecting copyrights in online video files despite early concerns about the ability of copyright holders to exercise control over information in digital formats.[189] Thus, the copyright model counters the argument that it is impossible to regulate video files online on the grounds that it is too difficult to obtain effective control over these files.[190]

---

182 SOLOVE, THE FUTURE OF REPUTATION, *supra* note __, at 193 ("There is … a limit to how much the law can do. The law is an instrument capable of subtle notes, but it is not quite a violin.")

183 LESSIG, FREE CULTURE, *supra* note ___, at 123 ("While these four modalities are analytically independent, law has a special role in affecting the three. The law, in other words, sometimes operates to increase or decrease the constraint of a particular modality.")

184 *id*, at 187. Professor Sánchez Abril has also noted that, while many traditional privacy laws are premised on a distinction between public and private conduct, this distinction has become increasingly blurred in the digital information age, which has caused expectations of privacy to become unstable and difficult to ascertain: Sánchez Abril, *Recasting Privacy*, *supra* note ___, at 5-6. See also ZITTRAIN, *supra* note ___, at 212 ("Even the use of "public" and "private" to describe our selves and spaces is not subtle enough to express the kind of privacy we might want [online]."), 216 ("Peer-leveraging technologies are overstepping the boundaries that laws and norms have defined as public and private, even as they are also facilitating beneficial innovation.").

185 SOLOVE, THE FUTURE OF REPUTATION, *supra* note __, at 187. See Richards and Solove, *Privacy's Other Path*, *supra* note ___.

186 SOLOVE, THE FUTURE OF REPUTATION, *supra* note __, at 188.

187 Pamela Samuelson, *The Copyright Grab*, 4.01 WIRED (Jan. 1996) (available at http://www.wired.com/wired/archive/4.01/white.paper.html, last viewed on July 23, 2008); LESSIG, FREE CULTURE, *supra* note ___.

188 SOLOVE, THE FUTURE OF REPUTATION, *supra* note __, at 185.

189 *id*, at 184-186.

190 *id*., at 184 ([I]s control over information really feasible? If we expose information to others, isn't it too difficult for the law to allow us still to control it? Perhaps the law is reticent about granting control because of the practical difficulties. Information spreads rapidly, sometimes like a virus, and it is not easily contained.")

Copyright law will apply online regardless of whether the relevant information has been accidentally exposed to the public,[191] and even if the information is in a digital format that can be readily copied.[192] Thus, it is technically possible to enact a law that controls the flow of video information online.

The similarities between copyright and privacy with respect to video files include questions about: (a) how to effectively control access to, and use of, digitally available information; (b) how to balance the rights of an information rights holder against competing interests such as free speech and other legitimate uses;[193] (c) what kinds of liability, if any, should be faced by Internet intermediaries, such as Internet service providers, for unauthorized activities of others;[194] (d) how to identify appropriate forums for dispute resolution in a global information society; (e) how to deal with global disharmonization of relevant legal principles;[195] (f) how to identify wrongdoers in a largely anonymous online medium;[196] and, (g) how to provide effective remedies for harms arising from the viral online dissemination of protected information.[197]

Copyright law has also developed a notice and takedown regime to give rights-holders the ability to request removal of infringing material from websites.[198] This law also provides a safe harbor from secondary infringement liability for Internet

---

[191] *id*, at 185 ("The copyright system focuses on the use of information – it allows certain uses and prohibits others. And it does so regardless of whether the information has been publicly exposed.")

[192] *id*. ("[C]opyright law provides protection even when a work can be readily copied. I don't have to take any steps to protect my work.")

[193] Legitimate uses might include those traditionally associated with copyright law such as news reporting on matters of public interest, and some non profit educational uses. In the privacy context, certain kinds of data aggregation might also be legitimate uses if appropriate safeguards against unauthorized privacy invasions are implemented. See, for example, *Whalen v Roe,* 429 U.S. 589 (1977) (upholding law requiring computerized data aggregation of information relating to prescription of certain medications, and acknowledging that appropriate information security safeguards were in place).

[194] Professor Solove notes that copyright law provides liability when third parties facilitate a copyright violation: SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 185.

[195] For example, the European Union and United States take very different approaches to privacy. The European Union approach is largely codified in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Data Protection Directive"). The United States, on the other hand, takes a more piecemeal approach to private data protection: RAYMOND KU AND JACQUELINE LIPTON, CYBERSPACE LAW: CASES AND MATERIALS, 544 (2 ed, 2006) ("[T]o date, the United States largely relies upon unfair and deceptive business practice law and self-regulation [to protect privacy]. In contrast, other nations, and most notably, the European Union have taken more aggressive steps to protect individual privacy in data collection.")

[196] 17 U.S.C. § 512 allows copyright holders, for example, to seek identifying information about alleged copyright infringers from third party services providers. See also *In re Verizon Internet Services, Inc*, 257 F. Supp. 2d 244 (D.D.C. 2003) (Internet service provider ("ISP") challenging subpoena served on it by the Recording Industry Association of America seeking identifying information for alleged copyright infringers utilizing the ISP's services.)

[197] SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 184-5 (noting that copyright law will provide remedies even when information has been exposed to public view and has not been protected by the information holder against potential viral distribution).

[198] 17 U.S.C. 512 (c).

intermediaries such as OSNs.[199] The notice and takedown idea could be extended to the privacy context if personal privacy rights are to be strengthened in digital video images. Of course, such an approach would have to take into account the potential chilling impact on free speech. Safeguards would need to be built into the system to ensure that the notice and takedown mechanism was not used frivolously to the detriment of online expression. However, there would likely be less risk of frivolous takedown notices in the privacy context, involving private individuals' reputations, than in the copyright context where powerful corporate copyright holders seem to resort to the takedown regime even in the absence of a serious likelihood that a copyright infringement has occurred.[200]

Although digital copyright law may be a useful model for enhanced online privacy protections, it needs to be kept in mind that parallels between copyright and privacy are not perfect. The constitutional underpinnings for copyrights and privacy are quite different. Copyright law has clear and express origins in the federal Constitution,[201] while informational privacy does not.[202] Thus, the online protection of copyrights by Congress is more easily justified in the face of First Amendment concerns than the protection of privacy. Additionally, copyright law in the digital age has created its own imbalances,[203] and these should be avoided in enhancing any legal protections for online privacy.[204]

3. Lessons from Environmental Regulation

Environmental regulation is another area of law that may prove instructive for online privacy, at least with respect to the role that OSN providers might play. There has

---

[199] *id.* The privacy analog to this would be § 230 of the Communications Decency Act of 1996, effectively immunizing ISPs for tort liability for speech posted by others utilizing their services.

[200] See, for example, discussion in Jennifer Urban and Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621 (2006); MICHELE BOLDRIN and DAVID K LEVINE, AGAINST INTELLECTUAL MONOPOLY, 108-110 (2008) (describing abuses of notice and takedown procedure by powerful corporate copyright holders).

[201] Art. I, Section 8, Clause 8 (granting the Congress power: "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.")

[202] Limited privacy rights have been implied into various constitutional clauses, but there is no express grant of power for Congress to protect privacy: DANIEL SOLOVE, MARC ROTENBERG AND PAUL SCHWARTZ, INFORMATION PRIVACY LAW (2 ed, 2006) ("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.")

[203] Pamela Samuelson, *The Copyright Grab*, 4.01 WIRED (Jan. 1996) (available at http://www.wired.com/wired/archive/4.01/white.paper.html, last viewed on July 23, 2008); LESSIG, FREE CULTURE, *supra* note ___; BOLDRIN and LEVINE, *supra* note ___, at 108-120.

[204] Of course even digital copyright law has been bolstered in many respects by contract law and technical standards: Michael Madison, *Legal-Ware: Contract and Copyright in the Digital Age*, 67 FORDHAM L REV 1025 (1998) (discussing uses of contractual and technological measures with copyright law in attempts by copyright holders to protect their rights online). This is another example of an important and necessary interaction between distinct regulatory modalities – contract, architecture (technology) and law. Privacy law advocates considering these interactions today have an opportunity to achieve a better balance of interests in the wake of some of the arguable failures of digital copyright law.

been a growing trend in information privacy law to look to models of environmental regulation as a basis for ascertaining best practices for online privacy.[205] Commentators have noted the ways in which environmental law has moved away from command and control models[206] towards second generation initiatives that encourage regulated parties to choose for themselves the means by which they will achieve regulatory goals.[207] These approaches could be adapted to online privacy.[208] In effect, law can be utilized as a means to foster the development of market forces that promote the kinds of privacy goals society would ideally require online. Laws could set goals of best practices for OSNs in protecting and enforcing individual privacy in terms of things like the drafting and enforcement of their terms of use and privacy policies, and their willingness to incorporate privacy-enhancing technologies into their services.[209] Here, we potentially see a complex interplay of social norms, laws, market forces, and system architecture in achieving desired privacy outcomes.

4. Privacy and Publicity Torts

Privacy torts seem to be the most obvious approach to the legal regulation of online privacy. However, as currently framed, they have significant limitations, most of which have been identified above.[210] The Restatement (Second) of Torts currently recognizes four distinct privacy torts.[211] Unfortunately, they are uncohesive in terms of coverage and have been criticized by free speech advocates.[212] Nevertheless, some of the privacy torts could be modified to better accommodate the realities of online conduct involving video content. Professor Sánchez Abril has suggested strengthening the tort relating to public disclosure of private facts[213] to operate more effectively in the OSN

---

[205] Dennis D Hirsch, *Protecting the Inner Environment: What Privacy Regulation can Learn from Environmental Law*, 41 GEORGIA LAW REVIEW 1 (2006); Deirdre Mulligan and Joseph Simitian, *Assessing Security Breach Notification Laws*, work in progress, copy on file with the author.

[206] Hirsch, *supra* note ___, at 8; Jonathan Remy Nash, *Framing Effects and Regulatory Choice*, 82 NOTRE DAME L REV 313, 320 (2006) (explaining command and control regulatory approach in the environmental context as a government setting a particular standard with which targeted actors are required to comply

[207] Hirsch, *supra* note ___, at 8.

[208] *id*., at 23 ("The privacy injuries of the Information Age are structurally similar to the environmental damage of the smokestack era. Two key concepts that have bee used to understand environmental damage – the "negative externality" and the "tragedy of the commons" – also shed light on privacy issues."); 63 (identifying other similarities between environmental regulation and information regulation, including the fact that market players regulated by both areas of law: "undergo rapid change, face stiff competition, and have the capacity for socially beneficial innovation.")

[209] The kinds of technologies that might be incorporated into OSN services in this respect are taken up in more detail in Part IV.A.6 *infra*.

[210] See discussion in Part II.A.2 *supra*.

[211] Restatement (Second) of Torts, §§ 652A-E (1997).

[212] Zimmerman, *Requiem*, *supra* note ___ (suggesting that torts prohibiting true speech cannot be reconciled with the First Amendment); Volokh, *supra* note ___ (suggesting that tortious approaches to protecting privacy cannot be reconciled with the First Amendment, but that contractual approaches may avoid this criticism).

[213] Restatement (Second) of Torts, § 652D ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.")

context.[214] She notes that the public disclosure tort developed at a time when the law was concerned with intrusions into physical spaces.[215] It is therefore not well suited to virtual environments.[216] She suggests re-focusing enquiries about public versus private activities, in the context of this tort, to better meet the needs of the information society. Notably, she advocates: (a) thinking about zones of confidentiality created by system architecture, agreements and relationship bonds, rather than physical walls;[217] (b) categorizing privacy harms that ensue from information disclosure rather than categorizing certain subject matter as *per se* private;[218] and (c) thinking in terms of overall accessibility of online information rather than in terms of whether it was completely secret or secluded.[219]

Related to the privacy torts is the right of publicity tort. In fact, the publicity tort closely tracks one of the privacy torts – the misappropriation tort.[220] Both torts prevent the use of someone else's name or likeness for financial benefit.[221] Thus, neither tort effectively covers unauthorized posting and dissemination of photographs on OSNs. Most of these uses are not for commercial gain, but merely for amusement and discussion.[222] The misappropriation-based torts might be expanded to help individuals control uses and dissemination of their images online:[223] for example, they could cover unauthorized disseminations of an individual's image even in the absence of a profit motive. Of course, there would have to be some counterbalancing forces put in place to ensure that speech was not unnecessarily chilled: for example, a broadened non-commercial appropriation tort might apply online only "when people's photos are used in ways that are not of public concern."[224]

The four American privacy torts also suffer from some common limitations. Plaintiffs are put in the awkward position of having to relive the humiliation and embarrassment of the images as they are entered into the public record as part of the court

---

214 Sánchez Abril, *Recasting Privacy*, *supra* note __.

215 *id*, at 2 ("[P]rivacy is usually a function of the physical space in which the purportedly private activity occurred."); 3 ("Traditionally, privacy has been inextricably linked to physical space.")

216 *id*, at 4 (concepts of physical space are no longer relevant in analyzing modern online privacy harms).

217 *id*., at 47.

218 *id.*

219 *id.*

220 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.")

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

222 GILSON ON TRADEMARKS, *supra* note ___, at § 2.16[1]. ("The appropriation tort would rarely apply to the discussion on the Internet of people's private lives or the posting of their photos.") Of course, it is arguable that the OSN provider's complicity in the posting might amount to financial profit motives if the OSN provider is deriving financial profit from advertising related to the online posting of video content. This proposition remains to be tested.

223 SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 187 ("The appropriation tort might be expanded to encompass a broader set of problematic uses of information about a person …")

224 *id.*

proceedings.[225] To add insult to injury, the plaintiff will have to pay a lawyer for the privilege of reliving this embarrassment. Additionally, domestic laws will always raise jurisdictional difficulties online, as compared with, say, technological solutions or contracts that specify choice of forum and choice of law.[226]

5. Privacy Contracts and Breach of Confidence Actions

Express or implied contracts and breach of confidence actions might also assist in the video privacy context. These issues are treated together here because they all rely on *relationships*. Express or implied contracts arise from the conduct of the parties and their intention to enter into legally binding obligations. Breach of confidence actions can arise from contract law or can be imposed externally to protect a relationship that the law deems to require a high duty of confidentiality. Examples are the doctor-patient relationship and the preacher-penitent relationship.[227] Relationships that give rise to legal obligations of confidence can be useful models for privacy regulation.[228] However, peer-based video privacy incursions do not generally involve relationships that the law would today regard as involving legal obligations of confidence. Of course, it is possible to expand the categories of confidential relationships recognized by the law. The question would be how best to achieve this. Express contracts of confidentiality might be problematic. It is unlikely that private individuals taking pictures of each other and posting them online have the time, inclination, or experience to enter into contracts to protect each other's privacy. However, implied contracts recognized by the legal system might be a viable alternative.

Commentators have recognized that implied contracts, and even express contracts, can be utilized in interpersonal relationships for legal enforcement of privacy and confidentiality expectations online.[229] Professors Sánchez Abril and Cava have suggested that an express promise of confidentiality between private individuals in

---

[225] MILLS, *supra* note ___, at 53-4 (describing additional privacy problems raised by the availability of court records on the Internet).

[226] Such contracts are generally upheld in the online context. See, for example, *Caspi v The Microsoft Network*, 323 N.J. Sup. 118 (App. Div. 1999).

[227] SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 214 (giving examples of relationships of confidence protected by legal rules, including attorney/client, priest/penitent, husband/wife, and, psychotherapist/patient).

[228] As early as 1968, for example, Professor Charles Fried noted the importance of focusing on privacy expectations within personal relationships: Fried, *supra* note ___, at 482 ("In general it is my thesis that in developed social contexts love, friendship and trust are only possible if persons enjoy and accord to each other a certain measure of privacy.")

[229] See Abril and Cava, *supra* note ___, at 268 ("Online, express confidentiality agreements are a more tenable solution. Facilitated through available technology, confidentiality agreements between users could assure a higher level of protection for those sharing private and personal information. In some instances, confidentiality agreements have been offered through online health ISPs as a prerequisite to membership. PatientsLikeMe.com includes such a clause as part of its terms of use. It states: "You agree not to disclose to any person or entity personally identifiable information about other members that you learn using this Site (whether posted in the Member Area by a member or emailed to you by a member) without the express consent of such member. You may disclose information of a general nature (that could not identify the member who provided such information or whom such information is about) to third parties outside this Site, subject to the above restriction on non-commercial use.").

respect of health care information could be built into online health care architectures.[230] Professor McClurg has suggested the development of implied contracts of confidentiality for intimate relationships generally.[231] His suggestion contemplates protection for both textual information shared in confidence and for video information pertaining to the relationship.[232] His ideas could be extended to social relationships more broadly.

Professor Volokh suggests that express or implied contracts of confidentiality are the only legal method of avoiding First Amendment problems.[233] However, he identifies two important limitations on contract-based solutions that may have particular resonance in cyberspace. The first is that contractual enforcement will generally not apply to third parties, unless, for example, the third party can be found to be an agent of one of the contracting parties.[234] In the OSN situation, people disseminating each other's images online may not be in any kind of relationship with an image subject let alone a contractual relationship. The second limitation of contractual solutions is that contracts cannot be enforced against minors.[235] This may be a significant problem in the OSN context because presumably many people sharing images online are minors.

Some commentators have suggested the extension of breach of confidence actions to better protect privacy.[236] For example, British law currently protects a greater array of relationships of confidence than American law.[237] American tort law could be extended to cover a greater variety of relationships of confidence, particularly online. Such an approach may again be less objectionable on First Amendment grounds than reliance on extending privacy torts because rights arising from relationships are not enforceable against the whole world.[238] Of course, one limitation of the breach of confidence

---

230 *id*, at 276 ("Cyber-patients have the duty of confidentiality to fellow patients. All information disclosed on health networking websites is privy and not to be divulged or otherwise disseminated. Users should not disclose any information obtained through the website unless specifically authorized. Similarly, disclosing cyber-patients should be as clear as possible regarding the level of confidentiality they expect. Cyber-patients have the duty to obtain the consent of family members and others whose health information they disclose. Relevant information regarding the health of family members is a vital part of a complete medical record. However, cyber-patients must understand these individuals also have rights to privacy in their health information. Cyber-patients must, therefore, obtain the informed consent of their family members before posting such information on the website.").

231 McClurg, *supra* note ___.

232 *id*., at 887-888 (giving examples of online text-based and video disseminations of confidential information).

233 Volokh, *supra* note ___, at 1062 ("I certainly do not claim that a contractual approach to information privacy, even with a large dollop of implied contract, is a panacea for information privacy advocates …. I claim only that contractual solutions are a constitutional alternative and may be the only constitutional alternative, not that they are always a particularly satisfactory alternative."); Zimmerman, *Requiem*, *supra* note ___, at 363 (suggesting looking into contractual solutions for protecting privacy rather than tort law).

234 Volokh, *supra* note ___, at 1061.

235 *id*., at 1063.

236 Richards and Solove, *Privacy's Other Path*, *supra* note ___.

237 *id*., at 158-160 (2007); SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 137 ("England, which rejects Warren and Brandeis's privacy torts, recognizes a breach-of-confidence tort. Unlike the American version, which applies only in a few narrow contexts, the English tort applies much more generally and extends even to spouses and lovers.")

238 Richards and Solove, *Privacy's Other Path*, *supra* note ___178-181.

approach is that, even a broadened concept of relationships of confidence will not cover situations such as dog poop girl and Bus Uncle where there is no relationship at all between the image taker and the image subject, other than that they happen to be sharing a mode of public transportation.

6. Legislating Codes of Conduct and Technical Standards

Legal rules might also enhance privacy by encouraging the adoption of certain social behaviors and technical standards.[239] Here, we are talking about legislating best practices to encourage either markets or individuals, or both, to behave in a particular way to better protect online privacy. Legislation might be targeted at OSNs with respect to best practices for default privacy settings.[240] This might involve requiring OSNs to incorporate technological privacy protections by default, such as refusing access by one user to another's information without asking the second user a series of security questions and having her check a permissions screen.[241] Another example would be requiring OSNs to set their systems to prevent copying and pasting of digital information and images unless a particular user opted to allow her images to be copied by others.[242]

Legal rules do not only shape behavior through enforcement – or the threat of enforcement. They also serve a communicative function about appropriate online conduct.[243] They can thus reflect, and in some cases even direct, the development of social norms. In the video privacy context, law will be an important piece of the regulatory matrix both by punishing inappropriate behaviors, and by signaling the contours of acceptable behaviors. However, law cannot operate in a vacuum. The following discussion considers the other five regulatory modalities that must interact with law to achieve an effective regulatory matrix.

---

239 This is an extension of the idea of drawing on the environmental regulation model to encourage markets, and in this case individuals as well, to behave in a particular way.

240 Edwards and Brown, *supra* note ___ (Drawing on the experience of the Directive on Privacy and Electronic Communications in the European Union - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (available at http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf, last viewed on July 24, 2008) – Professors Edwards and Brown suggest that legislating mandatory privacy default settings may prove more effective in protecting individual privacy than leaving the market to its own devices.)

241 This is effectively what many closed networks do now. Facebook, for example, does not let a user access another's profile unless the second user accepts the first as a "friend".

242 Of course, for privacy protection purposes, this would require permission of the image subject as well as potentially the image owner which could be technically unwieldy in practice.

243 See, for example, Fried, *supra* note ___, at 493 ("By using the public, impersonal and ultimate institution of law to grant persons this control, we at once put the right to control as far beyond question as we can and at the same time show how seriously we take that right.")

B. SOCIAL NORMS

Social norms are an extremely important form of regulation.[244] Norms may be defined as rules that are: "diffusely enforced by third parties other than state agents by means of social sanctions."[245] Norms can be more significant than laws,[246] particularly in areas that involve high levels of social interaction,[247] like privacy. The problem with cyberspace is that many norms are not yet well developed. Particularly in relation to OSNs, norm development is in its infancy because of the relative novelty of social networking technology. This state of affairs contains both advantages and disadvantages for privacy advocates. Advantages include the ability to make privacy-protecting regulatory decisions before privacy-destroying norms become entrenched. However, disadvantages include the difficulties of ascertaining appropriate levels of privacy protection in the absence of clearer information about social expectations. This paradox is not new in the online privacy context.[248] However, it requires serious thought by decision-makers before potentially harmful norms become entrenched.[249]

Globalization also raises difficulties of identifying and enforcing norms online. Are we talking about one global society's norms? Or rather an overlapping group of online societies, like the overlapping networks of "friends" on an OSN? Yet another problem of identifying privacy norms online relates to the ambiguity or cognitive disconnect that arises when people are surveyed about online privacy. In the few surveys that have been conducted on attitudes to online privacy, respondents generally rate the idea of privacy in the abstract very highly.[250] However, they are prepared to bargain with their privacy for a very small price.[251] An online shopping coupon may well entice an individual to disclose voluminous personal details with little regard to future uses of that information.[252]

---

244 SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 93 ("One of the primary ways that society intervenes in people's lives is through the enforcement of norms.")

245 Lessig, *The Architecture of Privacy*, *supra* note ___, at 62 ("[Norms] are different from law – they are enforced … not by the state, but by the sanctions of other members of a particular community. But they are nonetheless a source of constraint, functioning to protect privacy.")

246 Strandburg, *supra* note ___, at 1248.

247 *id.*

248 See discussion in Bernstein, *New Technologies*, *supra* note ___ (describing similar dynamics with respect to commercial transactions on the Internet and data aggregation by Internet commerce companies).

249 *id.*

250 SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 73 (citing the work of economists Alessandro Acquisti and Jens Grossklags); Eric Goldman, *On My Mind: The Privacy Hoax*, available at http://www.ericgoldman.org/Articles/privacyhoax.htm, last viewed on July 24, 2008 ("But what do these surveys really prove? Consumers may tell survey takers they fear for their privacy, but their behavior belies it. People don't read privacy policies, for example. In a survey taken last year by the Privacy Leadership Initiative, a group of corporate and trade association executives, only 3% of consumers read privacy policies carefully, and 64% only glanced at--or never read--privacy policies.").

251 *id*.

252 SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 87 ("Since people routinely give out their personal information for shopping discount cards, for access to websites, and even for free, some market proponents (especially the self-regulators) argue that the value of the data is very low to the individuals."); Froomkin, *supra* note ___, at 1502 ("[C]onsumers suffer from privacy myopia: they will sell their data too often and too cheaply. Modest assumptions about consumer privacy myopia suggest that even Americans who place a high value on information privacy will sell their privacy bit by bit for frequent flyer miles.")

So how do we identify and enforce social norms as they relate to content, particularly video content, shared over OSNs? Some empirical work may be helpful, although to date empirical work has had its limits because individuals typically undervalue their personal information.[253] There is an argument that empirical work may suffer less from this problem in the OSN context than in the textual data aggregation context. In the latter context, where much of the survey work has been done so far, consumers' abstract expectations of privacy are often not aligned with their behavior when faced with the choice of trading their information for some minor commercial benefit, such as online shopping coupons or frequent flyer miles. In the online video context, on the other hand, there is little prospect of individuals bargaining with their personal information for any commercial benefit because their transactions are generally social rather than commercial. Thus, self-reported survey results about privacy expectations in OSNs may be more appropriately aligned with the way people actually behave. Another possible method of identifying emerging privacy norms online is to consider blog postings and associated comments that deal with privacy issues. More and more often, online privacy incursions are reported on blogs, and various individuals will comment about related expectations of privacy.[254] A comprehensive survey of some of these postings may illuminate prevailing societal views about privacy, and identify areas in which norms are still developing.

If it is possible to ascertain any social expectations about online privacy in the OSN context, these could usefully be reduced to Internet guidelines, akin to the way that netiquette developed in the early days of the Internet. Netiquette has been defined as "the growing body of acceptable, though as yet largely unwritten, etiquette with respect to conduct by users of the Internet".[255] In the early days of the Internet, netiquette generally referred to attempts to articulate appropriate social norms with respect to the new email technologies available at the time.[256]

Private organizations or individuals who may have a stake in the future operation of OSNs might encourage the articulation of netiquette principles for OSNs that take

---

There are other alternative explanations for consumers failing to act in privacy protecting ways online: Bernstein, *Paradoxes, supra* note ___, at 290 (suggesting that consumers are actually unaware of the extent of privacy threats accordingly online which leads them to fail to adequately protect their privacy using already available technological tools and social behaviors).

[253] SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 87; Froomkin, *supra* note ___, at 1502.

[254] For an example of this, see Owen Thomas, *Your Privacy is an Illusion: Bank Intern Busted by Facebook* (Gawker, November 17, 2007, available at http://valleywag.gawker.com/321802/tech/your-privacy-is-an-illusion/bank-intern-busted-by-facebook, last viewed on January 23, 2009) (example of employer finding image on Facebook of employee at a Halloween party on a day when employee was allegedly out of the office for a family emergency – and associated comment on the story by web users).

[255] *1267623 Ontario Inc v Nexx Online Inc*, [1999] O.J. No. 2246 (Court File No. C20546/99, Ontario Superior Court of Justice, Toronto, Ontario, June 14, 1999) ("[Netiquette] is defined as the growing body of acceptable, though as yet largely unwritten, etiquette with respect to conduct by users of the Internet.")

[256] In 1995, for example, Intel promulgated a set of guidelines in the form of a generally available memo for the Internet community. These "Netiquette Guidelines"[256] contained suggestions about appropriate use of email services for the then-new generation of Internet users who had not "grown up with the Internet": Intel, Netiquette Guidelines, available at http://www.albury.net.au/new-users/rfc1855.txt, last viewed on July 18, 2008.

privacy into account. Indeed, many OSN service providers currently do incorporate privacy provisions into their terms of use.[257] However, there are problems with enforcement of these terms generally,[258] and with the fact that many victims of privacy incursions are not parties to these contracts.[259] Some OSNs have privacy policies that resemble attempts to articulate new forms of netiquette.[260] These are generally available statements of best practices by an OSN provider about its aspirations to appropriately protect user privacy.[261] However, terms of use and privacy policies differ from netiquette and social norms in the sense that they are generally written from the point of view of an OSN provider, not the individuals using the service. Thus, they focus on what the service provider will or will not do with personal information, rather than with the kind of respect individual users of the service should pay to each other's privacy. Emerging online norms, or netiquette, must take account of both the appropriate behavior of OSN providers vis-à-vis private individuals, and the appropriate behavior of individuals amongst themselves.[262]

Some OSNs attempt to outline a form of netiquette, describing ways in which users of their services should treat each other. YouTube and Flickr each have a set of "Community Guidelines" along these lines.[263] The Community Guidelines cover issues like ensuring that no inappropriate content is posted, and remembering that children may be looking at information and video files. They additionally include terms like: "Flickr is not a venue for you to harass, abuse, impersonate, or intimidate others. If we receive a valid complaint about your conduct, we'll send you a warning or terminate your account".[264] Flickr also includes the simple suggestion: "Don't be creepy."[265] The guidelines do not say anything about protecting others' privacy rights, although they do talk about respecting others' copyrights.[266]

---

257 See discussion in Part II.B *supra*.

258 *id*.

259 *id.*

260 See, for example, Facebook's Privacy Policy, available at http://www.facebook.com/policy.php, last viewed on July 18, 2008.

261 *id.*

262 Intel's Netiquette Guidelines focus on behavior amongst individuals using text-based electronic communications services, while at the same time acknowledging the role of service providers in the behavioral equation. See, for example, clause 1.0 ("Individuals should be aware that no matter who supplies their Internet access, be it an Internet Service Provider through a private account, or a student account at a University, or an account through a corporation, that those organizations have regulations about ownership of mail and files, about what is proper to post or send, and how to present yourself. Be sure to check with the local authority for specific guidelines."); clause 4.1.1 ("Remember that all these services belong to someone else. The people who pay the bills get to make the rules governing usage. Information may be free - or it may not be! Be sure you check.")

263 Flickr Community Guidelines, available at http://www.flickr.com/guidelines.gne, last viewed on July 22, 2008; YouTube Community Guidelines, available at http://www.youtube.com/t/community_guidelines, last viewed on July 22, 2008. In fact, Flickr expresses that its Community Guidelines are part of its terms of use so they may have contractual force as well as reflecting desired social norms: Flickr Community Guidelines, *supra* note ___, ("Don't forget that your use of Flickr is subject to these Guidelines and our Terms of Use.")

264 *id*.

265 *id*.

266 *id*. In particular, Flickr suggests ways of amicably resolving copyright disputes by encouraging first that a complainant privately contact the alleged copyright violator. Then, if that does not succeed, the

Flickr's Community Guidelines also ask users of the service not to "upload anything that isn't theirs".[267] However, closer inspection of the relevant clause suggests that this is geared towards copyright protection rather than privacy protection. The definition of "stuff that isn't yours" states that: "This includes other people's photos, video and/or stuff you've collected from around the Internet." The possessive pronoun here relates to "photos, videos and other stuff", suggesting that it is the ownership of a digital image that is important to Flickr, rather than the holder of privacy interests in the image. In other words, where the photographer is a different person to the photographic subject, it would seem that Flickr's guidelines only contemplate protection of the photographer's rights in the image, not the rights of the photographic subject.[268]

In contrast to services like Flickr and YouTube, some of the closed networks like MySpace and Facebook do not have specific sets of Community Guidelines outside of their standard terms of use and privacy policies. This may be because their users are automatically regarded as having more control of content because of the closed nature of the network. Thus, there is less perceived need to promulgate a set of Community Guidelines.[269] In other words, if users are able to limit views of their content to "friends" authorized to access their profiles, then there is less need for the service provider to promulgate a set of rules about how community members should treat each other. Community members can rely on the technical defaults they set to limit uses others may make of their information.[270]

---

complainant is requested to file a notice of infringement with the "Yahoo! Copyright Team" who will resolve the matter. Their Community Guidelines state that: "If you see photos or videos that you've created in another member's photostream, don't panic. This is probably just a misunderstanding and not malicious. A good first step is to contact them and politely ask them to remove it. If that doesn't work, please file a Notice of Infringement with the Yahoo! Copyright Team who will take it from there. You may be tempted to post an entry on your photostream or in our public forum about what's happening, but that's not the best way to resolve a possible copyright problem. We don't encourage singling out individuals like this on Flickr."

[267] Flickr Community Guidelines, *supra* note ___.

[268] YouTube's community guidelines similarly protect copyright, but do not specifically mention privacy interests: YouTube Community Guidelines, *supra* note ___, ("Respect copyright. Only upload videos that you made or that you are authorized to use. This means don't upload videos you didn't make, or use content in your videos that someone else owns the copyright to, such as music tracks, snippets of copyrighted programs, or videos made by other users, without necessary authorizations. Read our Copyright Tips for more information.")

[269] This assertion may find support in the fact that one of the most "open" of all networks, the Wikipedia, has an extremely detailed set of guidelines referred to as "Wikiquette" to assist people posting information to behave appropriately vis-à-vis other posters. See Wikipedia: Etiquette, available at http://en.wikipedia.org/wiki/Wikipedia:Etiquette, last viewed on July 23, 2008; CASS SUNSTEIN, INFOTOPIA: HOW MANY MINDS PRODUCE KNOWLEDGE, 155 (2006) ("When active debates are occurring about the content of articles, it is necessary to have good norms to provide some discipline. The term "Wikiquette" refers to the etiquette that Wikipedians follow. Wikiquette helps to ensure that the active debates are transferred to separate "talk pages." These are the deliberative forums on Wikipedia, in which those who disagree explain the basis for their disagreement. What is noteworthy is that the articles themselves are (mostly) solid, and that partisan debats have a specifically designed location.")

[270] ZITTRAIN, *supra* note ___, at 226 ("Facebook, for example, offers tools to label the photographs one submits and to indicate what groups of people can and cannot see them.")

Of course, this is only true to a point, but it may explain the difference between open and closed networks in terms of the perceived need to articulate Community Guidelines.[271] Paradoxically, users of closed OSNs such as Facebook may be particularly vulnerable to unbridled dissemination of their personal information and images due to developing norms against rejecting requests from people who want to "friend" you online.[272] Norms also appear to be developing that you cannot "unfriend" someone once you have accepted them as a friend.[273] Thus, the apparent control a user has on Facebook over who accesses their information may be much more illusory than it appears.

Outside the OSN context, the "spoiler" communities that investigate likely outcomes of reality television shows provide some useful examples of emerging online norms about privacy. One example involves the online communities that privately investigate likely contestants and outcomes on the popular *Survivor* television series.[274] These communities try to ascertain the identities of contestants on upcoming series of *Survivor*, the locations in which upcoming series will be filmed, and the order in which contestants will be voted off the program.[275] Of course, attempts to investigate the lives of actual contestants tread a fine line between legitimate fan interest in the program and invading the privacy of the contestants.[276] One norm that has developed within the *Survivor* spoiler community is the use of "brain trusts".[277] These are small subsets of the spoiler community who conduct much of the detailed investigation of contestants through encrypted websites that are not accessible to the general online community.[278] Part of the aim here is to protect the privacy of the contestants, as well as ensuring a higher degree of accuracy once the brain trust posts its findings to the general community.[279] The use of encryption technology to protect discussions implicating contestants' privacy suggests an intriguing interplay between developing privacy norms and system architecture.

All of these examples evidence ways in which online communities are beginning to develop and recognize privacy norms, including norms relating to video files. Thus, it may now be time to take stock of video privacy norms, and to attempt to ascertain where laws, technologies, and market practices, are lagging behind community expectations of privacy. For example, there currently appear to be no prevailing rules about the

---

[271] Norms may also play a part in this distinction. Those posting to YouTube may expect public availability of content, while those posting in closed networks expect more privacy protections.

[272] 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.")

[273] *id.*

[274] *Survivor* is shown on the CBS network in the United States. For a detailed history of the series and its development, see http://en.wikipedia.org/wiki/Survivor_(US_TV_series), last viewed on December 10, 2008. See also HENRY JENKINS, CONVERGENCE CULTURE: WHERE OLD AND NEW MEDIA COLLIDE, 25 (2006) (describing *Survivor* as a popular CBS show that started the reality television trend).

[275] JENKINS, *supra* note ___, 25-26.

[276] *id*., 36-7 ("[T]here is a thin, thin line between investigating those who have chosen to insert themselves into the public spotlight and stalking them at their home or workplace …. The community spends a great deal of time debating, exactly where you draw the line.")

[277] *id*, 38.

[278] *id.*

[279] *id*. ("The brain trusts … argue that this closed-door vetting process protects privacy and ensures a high degree of accuracy once they do post their findings.")

"tagging"[280] of photographs to make them more easily searchable.[281] Salient issues about appropriate regulation here would be whether there are any identifiable norms relating to the impact tagging might have on individual privacy. Even if an individual has consented to the posting of her image on Facebook, and acknowledges the possibility that others may see it and copy it, does that necessarily mean that she consents to tagging which enables easier and potentially larger scale searching and copying of the image?[282] It would be interesting to find out how OSN users feel about this issue.[283] Norms could then be calibrated with legal rules that encourage best practices in technologies, online contracting, and other market and social practices.

C. MARKET FORCES

Market forces often go hand in hand with social norms. Social desires and expectations dictate, to a certain extent, what the market is able to sell, and perhaps paradoxically, the market can dictate social norms through the nature of its products and services.[284] If all market players provide products that are limited to a given sub-set of possible social behaviors then social behaviors will, by default, have to conform to what is available in the market. However, if consumers are not happy with the available choices, they may either refuse to buy a service at all, or they may petition the service provider to change the service to better conform to their expectations. The immediate user backlash against Facebook's "Beacon" advertising scheme launched in late 2007 is an example of consumers demanding changes to an online service to better suit their privacy expectations.[285]

---

[280] "Tags" are currently defined by Wikipedia as follows: "A tag is a non-hierarchical keyword or term assigned to a piece of information (such as an internet bookmark, digital image, or computer file). This kind of metadata helps describe an item and allows it to be found again by browsing or searching. Tags are chosen informally and personally by the item's creator or by its viewer, depending on the system. On a website in which many users tag many items, this collection of tags becomes a folksonomy." (see http://en.wikipedia.org/wiki/Tag_(metadata), last viewed on February 1, 2009).

[281] Edwards and Brown, *supra* note ___, at [10-17 of draft].

[282] Of course, tagging also potentially assists with searching and removal of content where an image subject might have objected to its online dissemination, so the technology cuts both ways here.

[283] Professor Zittrain has noted that tagging may only be the beginning of the problem for online image privacy as facial recognition software becomes more sophisticated and video images can now be matched quite easily with tagged text descriptions: ZITTRAIN, *supra* note ___, at 214 ("Web sites like Riya, Polar Rose, and MyHeritage are perfecting facial recognition technologies so that once photos of a particular person are tagged a few times with his or her name, their computers can then automatically label all future photos that include the person – even if their image appears in the background.")

[284] This is not unlike the way that law can communicate norms, but law can also enforce norms. The interplay between modes of regulation can be quite complex and paradoxical at times.

[285] The Beacon program involved divulging to a user's "friends" what products the user had bought online on the basis that the user's friends may be interested in similar products. See discussion in William McGeveran, *Facebook Retreats Somewhat on Beacon Privacy*, Info/Law, December 2, 2007 (available at http://blogs.law.harvard.edu/infolaw/2007/12/02/facebook-retreats-socialads/, last viewed on July 24, 2008); SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 80 (citing various examples of online service provides cancelling initiatives due to public outcry about privacy, including Yahoo! eliminating a reverse telephone number search from its People Search site).

Commentators have been skeptical about the inclination of markets to regulate online privacy.[286] The Internet allows market players to make gains from individuals' personal information with very little legal recourse available for loss of privacy. Where are the incentives for market players to protect privacy in the absence of government regulation?[287] Maybe in the situations under discussion in this article industry self-regulation might fare better than it has in the context of text-based data aggregation. In the OSN context, at least as relates to video images, we are not talking about information that has commercial value when aggregated into large databases.[288] While textual information from a personal profile on Facebook might be of interest to online marketers, video information is less likely to have any significant appeal. Even if it were possible to utilize images to ascertain whether an image subject might be interested in a certain style of clothing, for example, the difficulties in processing video information in a way that easily identifies the subject's details for targeted advertising purposes likely outweigh any commensurate benefits of doing so, at least on the basis of today's technology.

Because of these attributes of online video, it is arguable that the interests of OSN service providers and their users in terms of privacy protection are not so disparate. If OSN service providers obtain more commercial value by protecting their users' privacy than by failing to do so, there may be sufficient market incentives for those service providers to compete with each other in offering privacy protections to their users. Facebook, for example, does offer stronger privacy protections in relation to video files than some of its competitors.[289] However, the fact that it has strongly worded privacy protections in its terms of use does not necessarily mean that it enforces them in practice. Facebook is also interesting in that it markets itself as having strong privacy protections. Nevertheless, it has been criticized for attempts to utilize information derived from its users to market items to their online "friends".[290]

This evidences a distinct practical problem with over-reliance on markets as privacy regulators. What an entity says it does, and what it actually does may be two different things. An OSN provider can use promises of privacy to entice users to accept its services, and then can fail to live up to those promises even to the extent of engaging

---

286 Lessig, *The Architecture of Privacy*, *supra* note ___, at 63 ("There is much to be skeptical about with [a solution to privacy problems involving market regulation] – not the least of which being that the interests of commerce might well be different from the interests of the consumer."); Mark Lemley, *Private Property*, 52 STAN L REV 1545, 1554 (2000) ("If we want privacy, we must be willing to accept the fact that there is no good "market solution" and endorse some government regulation of the behavior of data collectors."); Froomkin, *supra* note ___, at 1524-5 (expressing skepticism about industry self-regulation in the absence of a serious threat of government regulation).

287 Froomkin, *supra* note ___, at 1524-5 (expressing skepticism about industry self-regulation in the absence of a serious threat of government regulation).

288 *id*., at 1469 ("Data accumulation enables the construction of personal data profiles. When the data are available to others, they can construct personal profiles for targeted marketing, and even, in rare cases, blackmail.")

289 See discussion in Part II.B *supra*.

290 William McGeveran, *Facebook Inserting Users Into Ads*, Info/Law, November 8, 2007 (available at http://blogs.law.harvard.edu/infolaw/2007/11/08/facebook-social-ads/, last viewed on July 24, 2008); Megan McCarthy, *Facebook Ads Make You the Star – and You May Not Know It,* Wired Blog Network, January 2, 2008 (available at http://blog.wired.com/business/2008/01/facebook-ads-ma.html, last viewed on July 24, 2008).

in conduct that completely contradicts its promises.[291] In a perfect market, the consumer would simply take her business elsewhere. Yet, in online markets there is often no competitive "elsewhere" to go – and the transaction costs of moving all of your personal information to another OSN are high[292] relative to the benefits of doing so. If you want to interact socially online, you may have little real choice between service providers.

There are a number of other difficulties with reliance on privacy policies to protect consumers' interests online. There are problems of inequality of bargaining power between consumers and OSN providers.[293] Even if a large group of consumers objects to a privacy policy, there are collective action problems. It is often difficult for consumers to collectively express their privacy preferences to OSN providers.[294] Privacy policies tend to be fairly toothless in practice. These policies are often drafted in vague, aspirational terms with little serious attempt at making specific representations of exactly how a user's privacy will be protected.[295] Additionally, privacy policies tend to be regularly updated unilaterally by OSN providers, thus putting an unrealistic obligation on users to routinely check back on the policy to keep track of the privacy terms.[296] Market forces may be a useful and important form of regulation. However, market incentives are often insufficient to effectively protect users' privacy.[297] This may be an area in which it is necessary for legal rules to interact with market forces to facilitate more appropriate outcomes.[298]

D. SYSTEM ARCHITECTURE

System architecture has been defined as: "technologies for re-creating privacy where other technologies may have erased it."[299] One salient example of a privacy protecting architecture is the Platform for Privacy Preferences (P3P) project, which supports the development of software code that allows websites and Internet users to set automatic privacy default preferences on their computers that other computers can read

---

[291] SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 81-87 (describing failures of contracts and market forces in protecting privacy).

[292] For example, the costs of moving relevant information and perhaps even having to set up a new email account along with a new personal profile – and notifying others of your new email address.

[293] SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 82.

[294] *id*.

[295] *id*, at 83.

[296] *id.*

[297] Froomkin, *supra* note ___, at 1527 ("A more generic problem with self-regulatory schemes, even those limited to e-commerce or Web sites in general, is that they regulate only those motivated or principled enough to take part in them.")

[298] In the associated context of online data aggregation and privacy concerns, Professor Froomkin has suggested the need for an approach that combines legislation, market forces, and social norms: Froomkin, *supra* note ___, at 1528 ("One way of creating incentives for accurate, if not necessarily ideal, privacy policies would be to use legislation, market forces, and the litigiousness of Americans to create a self-policing (as opposed to self-regulating) system for Web-based data collection.")

[299] Lessig, *The Architecture of Privacy*, *supra* note __, at 63. For completeness, it should be noted that others have defined architecture more broadly in this context. Professor Solove, for example, appears to contemplate that system architecture includes hardware and software as well as the default attributes of relationships between individuals and those who control or process their information: SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 97-101.

without the need for human intervention.[300] For example, if a user sets high privacy settings, her computer might automatically deny access to certain websites that do not meet those standards. Architecture can have a profound impact on privacy.[301] One of its obvious advantages is that it can be more proactive than many other forms of regulation.[302] It creates *ex ante* constraints that prevent harm, while laws, for example, often provide remedies after harms have occurred.[303] Nevertheless, the problem with architecture is that it does not necessarily work well on its own. Privacy-enhancing technologies can be expensive and there is often little incentive for OSNs to invest in it absent government regulation requiring them to do so. While there may be incentives for consumers to invest in privacy-enhacing technologies, many consumers are insufficiently knowledgeable to work with these technologies. This is where public education plays an important role in the privacy matrix.[304]

Some OSNs already do employ privacy-enhancing architectures. A salient example is the closed network format utilized by Facebook and MySpace. These services use technology to limit users to accessing information of other users that they are authorized to access.[305] There are other examples where technological solutions may be implemented to better protect online video privacy. For example, Professors Edwards and Brown have suggested the possibility of automatic data expiration settings to combat the permanency problem of digital data in the OSN context.[306] Of course, expiration settings do not automatically deal with the problems of unauthorized dissemination of images prior to the expiration of the original post, or of the permanence of any copies made available on other websites. Especially if images have been tagged, they may be easy to find on multiple websites even after the original image has expired. In fact, with projects such as the Internet Archive, many images will continue to be available in some

---

300 See Platform for Privacy Preferences Project website: available at http://www.w3.org/P3P/Overview.html, last viewed on December 17, 2008.

301 SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 200 ("The technological design of the websites has an enormous impact on people's privacy."); Joel Reidenberg, *Rules of the Road for Global Electronic Highways: Merging Trade and Technical Paradigms*, 6 HARV J L & TECH 187 (1993); Reidenberg, *Lex Informatica, supra* note ___; Froomkin, *supra* note ___, at 1529-1533 (describing potential for use of privacy enhancing technologies as a form of system architecture to protect privacy).

302 SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 100.

303 *id.*; LESSIG, FREE CULTURE, *supra* note ___, at 122 ("[A]s with the market, architecture effects its constraint through simultaneous conditions. These conditions are imposed not by courts enforcing contracts, or by police punishing theft, but by nature, by "architecture."")

304 See discussion in Part IV.E *infra*.

305 On Facebook, you cannot access any detailed information about another user unless you ask them if you can be their "friend", and they accept you as a "friend" over the network: See Facebook's Profile Page, available at http://www.facebook.com/privacy/?view=profile, last viewed on July 24, 2008 (allowing Facebook users to limit access to their profiles to "friends", or even to "friends of friends"). Facebook also allows users to block particular people from accessing their profiles: See Facebook, "Block People", available at http://www.facebook.com/privacy/ , last viewed on July 24, 2008 ("If you block someone, they will not be able to find you in a Facebook search, see your profile, or interact with you through Facebook channels (such as Wall posts, Poke, etc.). Any Facebook ties you currently have with a person you block will be broken (for example, friendship connections, Relationship Status, etc.). Note that blocking someone may not prevent all communications and interactions in third-party applications, and does not extend to elsewhere on the Internet.")

306 Edwards and Brown, *supra* note ___, at [10-31 of current draft].

form even after all "live" images have been removed from relevant websites.[307] Nevertheless, automatic expiration settings would, to some extent, limit the availability of some personal information online. If multiple sites adopted the practice of automatic data expiration, then even copied images would eventually be removed from multiple sites, thus potentially lessening the permanency problem.

Technological solutions might also be developed to prevent unauthorized cutting and pasting of digital video files in the absence of consent by the image holder and the image subject. Code can be written to prohibit cutting and pasting,[308] while at the same time sending a request to the image holder and image subject for permission to disseminate the image. The holder and subject could then respond, and that response could translate into a permission or non-permission to use the image. If a response was not received from either the image holder or the image subject, the service could simply refuse permission to copy the image.[309] Alternatively, or additionally, the image could be tagged with permissions when originally uploaded. This would not prevent unauthorized disseminations of images *per se*, but it would bring the privacy preferences of the image subject into public view. Such an approach may assist in online norm development. In fact, some OSNs are experimenting with these kinds of tags. Facebook has offered technology to label photographs in order to indicate what groups of people are authorized to view them.[310] However, this system is limited in that the tags are lost when an image is copied outside the Facebook network.[311] To fully protect privacy, tags would have to be utilized by image subjects as well as owners of online images. This could prove unwieldy in practice.

This is obviously not a comprehensive survey of technological solutions to video privacy problems. It is merely intended to establish the availability of technological options that have not yet been seriously investigated and that might better protect online privacy. Many technologies that would enable enhanced privacy protection for video images are in existence today and have yet to be implemented in this context. The failure to apply them likely has to do with a combination of factors including: (a) assumptions by some online service providers that users do not care sufficiently about privacy to make

---

307 Using the "Wayback Machine" on the Internet Archive, one can browse through historical records of 85 billion web pages archived since 1996: http://www.archive.org/web/web.php, last viewed on September 29, 2008.

308 Copy control technologies online have been utilized in the copyright context extensively in recent years. See, for example, discussion of copy control technologies employed by Adobe with respect to the sale of eBooks in LESSIG, FREE CULTURE, *supra* note ___, at 147-153.

309 This would not be dissimilar to the Creative Commons license utilized to express copyright holders' preferences as to permitted uses of a given copyright work: see, Creative Commons, Choosing a License: Creative Commons Licenses, available at http://creativecommons.org/about/licenses/meet-the-licenses, last viewed on July 30, 2008. See also ZITTRAIN, *supra* note ___, at 225 ("As people put data on the Internet for others to use or reuse – data that might be about other people as well as themselves – there are no tools to allow those who provide the data to express their preferences about how the data ought to be indexed or used. There is no Privacy Commons license to request basic limits on how one's photographs ought to be reproduced from a social networking site. There ought to be.")

310 ZITTRAIN, *supra* note ___, at 226 ("Facebook … offers tools to label the photographs one submits and to indicate what groups of people can and cannot see them. Once a photo is copied beyond the Facebook environment, however, these attributes are lost.")

311 *id.*

it worth their while to employ these technologies;[312] (b) lack of awareness of these technologies by users; (c) lack of financial incentives for online service providers to develop and deploy these technologies;[313] and, (d) lack of clarity about social norms regarding online privacy, particularly in the video and multi-media context. Some of the more obvious advantages of developing technological solutions to emerging privacy problems are their effectiveness[314] and their global reach.[315] For example, if OSNs such as Facebook wanted to better protect privacy on a global scale, it would be a simple matter for them to create technological privacy defaults that would automatically operate in all countries where their services were accessible.[316]

E. EDUCATION

In recent years, commentators have started to focus on new modes of regulation that may be equally important for online privacy as the four regulatory modalities discussed above. One example is public education.[317] In the context of online privacy, we should consider who has the responsibility to educate the public, and how prescriptive or otherwise such education may be.[318] If, for example, social norms really are yet to develop in many online contexts, then education, at least at this point in time, might best be aimed at generating more of a public dialogue on privacy than on instructing the public about privacy. On the other hand, the public should certainly be instructed about currently available privacy-enhancing technologies so that these technologies might be used more effectively in practice.

---

312 SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 82 ("Companies only rarely compete on the basis of the amount of privacy they offer. People often do not weigh privacy policies heavily when choosing companies.")

313 Froomkin, *supra* note ___, at 1524 ("Since the economic incentive to provide strong privacy protections is either weak, nonexistent, or at least nonuniformly distributed among all participants in the marketplace, most serious proposals for self-regulation among market participants rely on the threat of government regulation …").

314 LESSIG, FREE CULTURE,*supra* note ___, AT 147-153 (discussing effectiveness of copy control technologies in the eBook copyright context).

315 Edwards and Brown, *supra* note ___, at [page 10-28 of current draft].

316 *id.*

317 *id.,* at [page 10-27 of current draft]; SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 204 ("Education is the most viable way to shape people's choices in [regard to information disclosed online]. For example, one study indicated that people have a lot of misunderstandings about who is able to search their Facebook profiles …. We need to spend a lot more time educating people about the consequences of posting information online."). Others have noted the importance of public education in as a regulatory force in society learning about privacy interests: Bernstein, *Paradoxes, supra* note ___, at 264 (talking about the role of genetic counselors in educating the public about privacy rights with respect to genetic testing and dissemination of personal information from genetic testing); Froomkin, *supra* note ___, at 1506 ("Legal rules prohibiting data collection in public are not the only possible response; defenses against collection might also include educating people as to the consequences of disclosure or deploying countertechnologies such as scramblers, detectors, or masks."); Abril and Cava*, supra* note ___, at 271-2 (suggesting that sometimes even the mere mention of privacy on a web service raises caution levels of the users of that service).

318 Abril, *(My)Space*, *supra* note ___, at 87 (suggesting that OSNs have a role as public educators with respect to online privcy).

Public education is currently an important, if under-utilized, regulatory modality for online privacy, both in the video context and with respect to unauthorized uses and disseminations of personal information more generally. Even if the education component only consists of explanations about the loss of control people increasingly have over their personal information online, this might inform the development of social norms. It might facilitate a situation where Internet users are more cautious about what information they disclose online, both about themselves and about their friends and acquaintances. The final regulatory modality addressed here – private or non-profit institutions – potentially interacts usefully with public education in that many of these institutions can serve an important public education role.

F. INSTITUTIONS

Another mode of regulating privacy revolves around the recognition of institutions as privacy regulators.[319] In a recent article on the importance of "intellectual privacy", Professor Neil Richards utilizes the example of libraries, and in particular, the American Library Association (ALA) in promoting free speech and intellectual liberty against the threat of government surveillance.[320] He discusses the ALA's 1939 library bill of rights which declared aspirations of intellectual freedom and privacy of library patrons.[321] Others have recognized the importance of institutions as regulators in various online contexts. Professor Lessig, for example, has emphasized the work of non-profit institutions as a potential regulatory modality in the digital copyright context. He cites the examples of the Public Library of Science (PLoS)[322] and the Creative Commons[323] as non-profit organizations whose work aims to facilitate more effective use of copyright works for the benefit of society as a whole.[324]

Institutions can also serve an important role in advocating for law reform. Some institutions might investigate social norms on issues like privacy, and advocate for legislation that better reflects those norms. Additionally, some institutions such as the

---

319 Richards, *Intellectual Privacy, supra* note___, at 33.

320 *id*., at 33-34.

321 *id*., at 32-33. Of course, one might suggest that the idea of "institutions as regulators" is really a subset of market forces as a regulatory modality. However, there are subtle differences. Market forces are determined largely by commercial interests. Institutional interests, however, may be more aspirational and focused on the needs of bettering society generally.

322 LESSIG, FREE CULTURE, *supra* note ___, at 281-282.

323 *id*, at 282-286.

324 The PLoS is a nonprofit organization that maintains a repository of scientific work in electronic form that is made permanently available for free: *id*, at 281-282. The Creative Commons is a nonprofit corporation that assists copyright holders in granting more flexible permissions for uses of their works: *id*, at 282 ("[Creative Commons's] aim is to build a layer of *reasonable* copyright on top of the extremes that now reign. It does this by making it easy for people to build upon other people's work, by making it simple for creators to express the freedom for others to take and build upon their work. Simple tags, tied to human-readable descriptions, tied to bullet-proof licenses, make this possible."). Creative Commons describes its mission as follows: "Creative Commons provides free tools that let authors, scientists, artists, and educators easily mark their creative work with the freedoms they want it to carry. You can use CC to change your copyright terms from "All Rights Reserved" to "Some Rights Reserved"." (See www.creativecommons.org, last viewed on July 30, 2008.).

EFF[325] routinely file amicus briefs in judicial proceedings,[326] thus playing into the judicial side of the regulatory equation. The question for video privacy in the OSN context, and online privacy generally, is whether there are currently any institutions that could appropriately fulfill an institutional regulatory function. Because most of the players in the OSN privacy matrix are commercial enterprises and private Internet users, it is difficult to identify an analog to the ALA, the PLoS, or Creative Commons in the privacy context. The closest obvious contenders are some public interest organizations that aim to protect rights and freedoms online, such as the EFF and the EPIC.[327] Other similar organizations may be developed in the future specifically to take on an institutional role in protecting privacy online.

These kinds of organizations tend not to be particularly well funded,[328] at least as compared with corporate interests. They certainly do important work in advocating for the rights of Internet users who may not be able to protect their own individual interests online because of collective action problems, or lack of knowledge about relevant law and technology. Perhaps part of the regulatory equation for protecting privacy online should be to pay more attention to, and encourage funding for, organizations such as the EFF and EPIC. At the very least, these kinds of institutions can play an important regulatory role, particularly as public educator and advocate,[329] in protecting online privacy.

Academic institutions are another set of non-profit organizations that can play a public education role.[330] They can assist in developing statements of best practices about online privacy, as well as disseminating information to the public about these issues. This is already done through conferences and symposia.[331] A greater array of publications, and greater accessibility of conferences and conference proceedings, including free online availability,[332] could be a useful aspect of the ongoing privacy matrix. Clearly public education and institutions as regulatory modalities have significant synergies, and they could be more usefully employed in the future development of online privacy principles, alongside the other regulatory modalities.

---

325 GOLDSMITH and WU, *supra* note ___, at 18 (describing the founding of the EFF as an organization that would use tools of "political participation, litigation, education, seminars, and campaigns" to develop a legal conception of cyberspace that would defend it from intrusions by territorial governments).

326 *id.*

327 The Electronic Privacy Information Center describes itself as: "a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values." (see www.epic.org, last viewed on July 23, 2008).

328 Much of the EFF's funding relies on volunteer work and donations: http://www.eff.org/helpout, last viewed on July 25, 2008. EPIC relies on support from individual and private institution contributions and legal awards: http://epic.org/epic/annual_reports/2005.pdf, last viewed on July 25, 2008.

329 GOLDSMITH and WU, *supra* note ___, at 18.

330 ZITTRAIN, *supra* note ___, at 244-245 (suggesting that universities take on a stronger leadership role in the Internet's future development more generally).

331 For example, the annual Computers Freedom & Privacy Conference, www.cfp.org, last viewed on July 25, 2008.

332 For example through podcasting.

V. CONCLUSIONS

Privacy has become the object of considerable concern. The purely fortuitous intrusions inherent in a compact and interrelated society have multiplied. The more insidious intrusions of increasingly sophisticated scientific devices into previously untouched areas, and the burgeoning claims of public and private agencies to personal information, have created a new sense of urgency in defense of privacy.

- Professor Charles Fried[333]

As evidenced by Professor Fried's comments from the late 1960s, privacy rights have been of significant concern since long before the Internet generation. However, the exponential rise of online privacy-destroying technologies[334] has led to increasing concerns about individual privacy in recent years. The scope and scale of online privacy violations can be truly devastating, as evidenced by the fate of dog poop girl, Star Wars kid, and Bus Uncle. A number of regulatory avenues have been identified to better protect digital privacy. However, the pace of technological change raises significant challenges for successful regulation. It is now time to start thinking more urgently about creating a workable matrix of regulatory approaches that better protects online privacy, particularly with respect to video and multi-media files disseminated online.

One might argue that this article has overstated the case about the need for digital video privacy regulation. Commentators have suggested that privacy is not a highly held value in cyberspace[335] so there is no need to protect it.[336] With respect to OSNs in particular, some would argue that privacy concerns are a "blip" phenomenon, and that time will educate Internet users to be more careful about video images and other information they place online, or allow to be placed online about them.[337] However, these views are problematic for a number of reasons. For one thing, even if current Internet users' apparent carelessness about personal information online is temporary, the effects of this carelessness may be widespread, permanent, and devastating because of the global and increasingly archival nature of today's online content.[338] Coupled with the aggregation and contextualization problems identified in Part II, the "blip" of unfortunate behavior today may have serious long term consequences for many people.

---

333 Fried, *supra* note ___, at 475.

334 Froomkin, *supra* note ___, at 1468-1501 (detailed survey of modern privacy-destroying technologies).

335 MILLS, *supra* note ___, at 187 ("The fact is that current society defines less and less to be private. People are putting personal information on Web sites, such as MySpace and YouTube, that would be unthinkable even thirty years ago.")

336 Goldman, *supra* note ___ ("mainstream consumers don't change their behavior based on online privacy concerns. If these people won't take even minimal steps to protect themselves, why should government regulation do it for them?").

337 Edwards and Brown, *supra* note ___, at [page 10-33 of the current draft].

338 CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS, 237 (2008) ("An interesting effect of digital archiving is that much casual conversation is now captured and stored for posterity, so it is possible to look back in time and find simple messages whose importance becomes obvious only with the passage of time.")

The Internet fundamentally challenges our perspectives on social, political, and economic behaviors every decade or so. Each shift requires decision makers to re-think basic assumptions about human interaction within progressively shorter timeframes. User-generated content on OSNs is a new crunch point in this online evolution, particularly as regards privacy. This article has demonstrated that serious privacy harms can result from unbridled dissemination of video files online. It suggests that it is time to consider a new multi-modal regulatory approach to protect individual privacy. If we do not act now, privacy-destroying norms may become entrenched and it will be much more difficult to protect privacy in the future. Even over-zealous action now can be reined in later if subsequently found to be overly protective of privacy to the detriment of other important interests such as free speech. There is little downside to considering regulatory action to protect privacy. Regulation, imperfect as it may be, can be revised later, but today's video privacy incursions may have far-reaching and potentially devastating consequences.