September 2014

"Smile, You're on Cellphone Camera!": Regulating Online Video Privacy in the MySpace Generation

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

"SMILE – YOU'RE ON CELLPHONE CAMERA!": REGULATING ONLINE PRIVACY IN THE MYSPACE GENERATION

JACQUELINE D. LIPTON*

ABSTRACT

In the latest Batman movie,[1] Bruce Wayne's corporate right hand man, Lucius Fox, copes stoically with the death and destruction dogging his boss. Interestingly, the last straw for him is Bruce's request that he use digital video surveillance created through the city's cellphone network to spy on the people of Gotham City in order to locate the Joker. Does this tell us something about the increasing social importance of privacy, particularly in an age where digital video technology is ubiquitous and largely unregulated?

While much digital privacy law and commentary has focused on text files containing personal data, little attention has been paid to privacy interests in video files that may portray individuals in an unflattering or embarrassing light. As digital video technology is now becoming widespread in the hands of the public, this focus needs to shift. Once a small percentage of online content, digital video images are now appearing online at an exponential rate. This is largely due to the growth of online video sharing services such as YouTube, MySpace, Flickr, and Facebook. The sharing of images online is now a global phenomenon – as is the lack of explicit legal protection for privacy rights in these images.

This article examines the extent to which we do, or should, have privacy rights in digital video content. It then considers the most effective approach for regulating online video privacy. It suggests that pure legal regulation, without more, is unlikely to be up to the task. Instead, a combination of regulatory modalities will be required to effectively protect privacy interests in digital video files. These modalities will likely include the four regulatory modalities previously identified by Professor Lawrence Lessig: legal rules, social norms, system architecture, and market forces. Additionally, new regulatory modalities may need to be developed. These might include public education and non-profit institutions recognized in a regulatory role.

---

* Professor of Law, Co-Director, Center for Law, Technology and the Arts, Associate Director, Frederick K Cox International Law Center, Director, Cyberspace Law and Policy Office, 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. Thanks are also due to Josephina Manifold for her excellent research assistance. All mistakes and omissions are, of course, my own.

1 *The Dark Knight*, Warner Bros. Pictures, 2008.

TABLE OF CONTENTS

I. INTRODUCTION

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

- Electronic Frontier Foundation[2]

Not that long ago on a subway train in South Korea, a woman's dog rather infamously pooped on the floor of a subway carriage. The woman refused to clean the mess even after being offered a tissue by a fellow traveler, and the rest is Internet history.[3] Another fellow traveler took photos of her with a cellphone camera. These photographs were quickly posted on a popular Korean blog. The purpose of the posting was to shame her.[4] Ultimately, the humiliation attached to this incident resulted in a firestorm of criticism directed at her which caused her to quit her job.[5] This story is one of a number of recent episodes illustrating the way in which a person's privacy can be obliterated at the push of a button by the use of the simplest and most ubiquitous combination of digital technologies – the cellphone camera and the Internet.[6] In these episodes,[7] we see a new trend in online conduct: peers intruding into each other's privacy with video and, more generally, multi-media, files.[8]

The phenomenon of online networking, including the sharing of multi-media files, has recently attracted some media attention,[9] particularly because it is an area that is largely unregulated. Current online privacy regulations focus on the collation and

---

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

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

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

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

[6] *id*., at 99 ("One holder of a mobile phone camera can irrevocably compromise someone else's privacy …")

[7] *id*., at 211 (discussion of "Star Wars kid" episode and "Bus Uncle" episode); SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 43-48 (discussion of "Little Fatty" and "Star Wars Kid" examples about video-based privacy invasions that potentially harm an individual's reputation or cause embarrassment and humiliation).

[8] 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.")

[9] See, for example, Kim Hart, *A Flashy Facebook Page at a Cost to Privacy*, THE WASHINGTON POST, June 12, 2008 (available at http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061103759.html, last viewed on July 21, 2008) (discussing privacy issues with Facebook generally).

dissemination of text-based digital dossiers comprising personal information,[10] rather than online video images. This is unsurprising, given the fact that the widespread availability of inexpensive digital video sharing technology is a relatively recent phenomenon.[11] It is now almost trite to say that the Internet poses significant risks to privacy. In the past, these risks have been characterized as involving the collection, use, and dissemination of text-based personal information by governments,[12] businesses,[13] health care providers,[14] Internet intermediaries,[15] and prospective employers.[16] Today, we can add concerns about unauthorized uses of our personal information by our peers over networks such as MySpace,[17] Facebook,[18] Flickr,[19] and Youtube.[20] Much of this information is in video form.[21]

---

[10] See discussion in Part II.A.3 *infra*.

[11] Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1, 5 (2007) (describing some of these new technologies available in the online world); Bobby White, *Cisco Projects Growth to Swell for Online Video*, THE WALL STREET JOURNAL (June 16, 2008, available at: http://online.wsj.com/article/SB121358372172676391.html, last viewed on June 16, 2008) ("Cisco Systems Inc. is projecting a sixfold jump in Internet traffic between 2007 and 2012, as online video becomes the biggest driver of global data communications.")

[12] 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")

[13] *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.")

[14] 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).

[15] 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).

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

[17] 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.

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

[19] 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.

[20] 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.")

[21] 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).

Current online privacy regulations have two things in common. The first is their predominant focus on text-based records.[22] The second is their goal of regulating data in the hands of institutions that deal with personal information in the course of commercial, governmental, or professional activities.[23] The current regulatory matrix is not aimed at protecting individuals from peer-based privacy incursions that involve video images. This regulatory approach made sense when uses of private information on the Internet were largely confined to text-based compilations of personal information by government and private enterprises. Now there is a need for new approaches to accommodate concerns about peer-based intrusions into online privacy, particularly through the uploading and dissemination of video files. While a picture is worth a thousand words, an image of an individual in an embarrassing situation might well affect her chances of employment,[24] education, or health insurance[25] if widely disseminated online.[26]

This Article considers the need for a broader approach to online privacy regulation that takes account of these new developments. It also considers the appropriate form for such regulation, noting in particular that a traditional "command and control" regulatory approach[27] on its own is unlikely to be particularly effective in this context. Rather, it suggests a combination of approaches involving multiple regulatory

---

22 Sánchez Abril, *supra* note ___, at 5 ("Much of the legal debate about privacy on the Internet has previously centered on personally identifiable data, like a person's address, social security number, spending habits, and financial information.").

23 SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 13-21 (describing historical growth of databases in the governmental and commercial context).

24 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.")

25 For example, a picture of a person smoking, or entering an HIV clinic.

26 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.") 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*").

27 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).

modalities, such as legal rules, social norms,[28] system architecture,[29] market forces,[30] public education, and private institutions.[31]

Part II identifies gaps in current privacy regulations both in the United States and the European Union with respect to peer-based privacy incursions involving video technology. Part III suggests the development of new forms of regulation to bridge these gaps. In so doing, it advocates the interplay[32] of a variety of regulatory modalities including the four modalities of cyberspace regulation identified by Professor Lawrence Lessig: legal rules, social norms, system architecture, and market forces.[33] It further suggests augmenting these regulatory modalities with new approaches including public education, and the use of private institutions as regulators. Part IV sets out conclusions and future directions for the development of online privacy principles. While focused on digital video content, these observations will also have some application to other forms of online content including text files and email messages.[34] Nevertheless, peer-based video privacy issues are a powerful and topical case study for putting more general online privacy concerns into sharp relief.

II. ONLINE VIDEO PRIVACY - GAPS IN THE EXISTING REGULATORY FRAMEWORK

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.

---

[28] 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.")

[29] 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*").

[30] 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.")

[31] 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*").

[32] LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY, 123 (2004) (noting that the four regulatory modalities he identifies must, of necessity, interact in practice) (hereinafter, "FREE CULTURE").

[33] Lawrence Lessig, *The Architecture of Privacy*, 1 VAND J ENT L & PRAC 56, 62-63 (1999) (hereinafter, "*The Architecture of Privacy*"); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARVARD LAW REV 501, 507 (1999) (identifying the four modalities of cyberspace regulation: laws, norms, architecture, and markets) (hereinafter, "*The Law of the Horse*"); LESSIG, FREE CULTURE, *supra* note ___, at 121-123 (describing the four regulatory modalities and their need to interact to achieve effective regulation in cyberspace).

[34] For a useful consideration of problems related to viral dissemination of emails, see James Grimmelman, *Accidental Privacy Spills*, 12 JOURNAL OF INTERNET LAW 3 (2008).

- The Buggles, *"Video Killed the Radio Star"*[35]

Advances in video technologies have historically transformed societies in dramatic ways. Well before The Buggles sang about the death of radio in the wake of early video tape-recording technology,[36] late nineteenth century commentators expressed concerns about the development of the "snap camera" by Kodak.[37] This was when photography first became relatively cheap and portable.[38] It allowed private individuals and members of the press to take candid photographs in a manner never before possible.[39] It was also what ultimately spurred on Warren and Brandeis to publish their seminal article on privacy[40] that would shape the development of American privacy law for more than a century.[41]

The late 1890s was eerily similar to the present day in the sense that individuals now have a powerful new video capability at their fingertips.[42] This time around, the technology enables us to take candid digital photographs without even having to remember to carry a camera. The camera now exists in most people's cellphones. Additionally, individuals do not require anything more than a network connection to disseminate those candid images to the world. It is this unbridled distribution capacity that distinguishes our time from what has gone before. It raises concerns that are not unlike those posed to copyright law in the digital age by the ability of individual consumers to share copyrighted works online on a scope and scale never before possible.[43] As with online copyright piracy, the problems for online privacy revolve around: (a) the threat of viral online distribution of private images[44] ("dissemination

---

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

36 *id.*

37 SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 107-108.

38 *id*, 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 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").

40 Samuel D Warren and Louis D Brandeis*, The Right to Privacy*, 4 HARV. L. REV. 193 (1980).

41 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").

42 Sánchez Abril, *supra* note ___, at 11-12 (noting that almost 120 years after Warren and Brandeis published their article, history seems to be repeating itself in terms of a threat to privacy because of the rise in new communications technologies in cyberspace).

43 Raymond Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U CHI L REV 263 (2002) (identifying the ability of consumers to act as distributors as a significant change in the copyright paradigm).

44 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

problems"); (b) the possibility of others augmenting the images with additional information (true, false, or indeterminate) ("aggregation problems");[45] and, (c) the inability of the complainant to ever obtain control of the information once it hits cyberspace ("permanence problems").[46]

A. PROTECTING ONLINE PRIVACY: GAPS IN THE CURRENT LEGAL SYSTEM

1. Copyright Law

Peer-based video privacy incursions involve images captured by friends and acquaintances and distributed online, either through closed or open social networks. Examples of closed networks are online social-networking services ("OSNs") like Facebook and MySpace. In these networks, users can control who has access to their online profiles. Open networks, on the other hand, are generally accessible by anyone with an Internet connection. A popular example of an open network in this context is YouTube. It is important to note that, with respect to posted video content, control is currently generally in the hands of the holder of a given video file. This person will not necessarily be the subject of the digital image. This situation parallels the way in which the copyright system works with respect to photographs. Initial copyright in a photograph is generally granted to the photographer, and not the subject of a photograph.[47] Copyright law is thus not much help to those seeking to assert control over the dissemination of photographs in which they feature as subjects. Of course, in the unusual case where the image subject is the owner of copyright in a given image, a copyright action would be possible for unauthorized distribution of the image online.[48]

---

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.")

[45] 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.")

[46] 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."); 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."); ZITTRAIN, *supra* note ___, at 211 ("Lives can be ruined after momentary wrongs, even if merely misdeameanors.")

[47] 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.")

[48] 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. Additionally, where the image subject is a celebrity, and the image is exploited for commercial profit, a right of publicity action may be available: ANNE GILSON LALONDE, GILSON ON TRADEMARKS, at § 2.16[1] ("The right of publicity

2. Tort Law – Privacy Torts

Laws regulating intrusive photography are equally unlikely to be of much help to those concerned about the uploading and online dissemination of images in which they feature as subjects. While there are some laws that prohibit intruding into another person's private space to capture an image of that person,[49] the OSN situation will generally not attract the operation of these laws. Peer photographs are usually taken with the consent of the subject of the image. In many cases, the subject has no objection to the taking of the picture, but may later be concerned about viral online dissemination of the photograph. Laws that regulate intrusive image-capturing, while saying little about dissemination,[50] are not much help to image subjects concerned about uncontrolled online distribution. Other laws 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.[51] For one thing, the appropriation is arguably not unauthorized if the image subject has consented to the taking of the photograph. For another thing, this tort generally requires an unauthorized commercial profit motive[52] which is generally absent in the context of an OSN.

… is the right of an individual to control the commercial use of his or her name, likeness, signature, or other personal characteristics.") (hereinafter, "GILSON ON TRADEMARKS")

[49] 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.")

[50] *id*, § 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."

[51] 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.")

[52] 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 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."). Professor Solove notes that appropriation tort law in general has come to be viewed as protecting valuable property-like interests in an individual's persona: SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 187 ("The appropriation tort is often limited to instances in which a person's identity is exploited for commercial gain. The tort doesn't apply when people's names or likenesses are used in news, art, literature, and so on.")

Other branches of privacy law in the United States focus respectively on public disclosure of private facts[53] and on publicity which places a person in a false light in the eye of the public.[54] Both of these require some form of public disclosure[55] which may be missing in a closed social network such as Facebook or MySpace – although distribution over an open network such as YouTube would be another story. However, even where there is a public disclosure, it is still an open question whether the distribution of candid photographs of friends and acquaintances will amount to disclosure of private facts, or will present a person in a false light. An individual may well object to the dissemination of an image of her even though the image does not disclose any private facts about her, and does not present her in a false light for the purposes of the privacy torts.

Can we gain any insights into appropriate regulatory avenues for video privacy by comparing OSNs to the physical world in which someone might take an unflattering or embarrassing photograph of a friend, and then show it to others? The photographer has always presumably been free to show the picture to other friends or family members, and even to make copies and distribute them to other people. Those other people may well show the photograph to people outside the immediate social network of the photographer and the photographic subject. How is this different from what can happen online? The answer lies in the scope and scale of the potential distribution, including accidental or incidental distributions to multiple closed and open networks.

Additionally, there is the permanence problem. Online images exhibit a permanence in multiple people's hands simultaneously that is largely absent in the physical world.[56] For a friend of a friend to attain a permanent copy of the original photograph, it is necessary for someone to go to the trouble of physically duplicating the photograph. Online, however, the uploading of an image to Facebook gives multiple network participants instantaneous and simultaneous access in multiple geographic locations.[57] The ability to copy and link the photograph to other websites at little to no cost increases the permanency problem. The practical result of the permanency problem

---

53 For a discussion of current problems and future directions with this branch of privacy law in the online context, see Sánchez Abril, *supra* note ___.

54 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.")

55 *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, *supra* note ___, at 9-11 (discussing practical difficulties of individual plaintiffs establishing requisite disclosures of private facts both in the physical world and online).

56 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."); 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.")

57 Grimmelmann, *supra* note ___, at 6 (making a similar comparison with contents of an email message as compared with a handwritten letter in the physical world; Grimmelmann notes that: "People who wouldn't have forwarded a letter will forward an email and they'll forward it to more people.")

is that, even if there is an effective regulatory method for an image subject to complain about online dissemination of an image, there will likely be no effective way to enforce an order to remove the image. Another troubling corollary of this problem is that information accessible in multiple locations online is often devoid of the context that it would have in the physical world.[58] This could lead to a greater incidence of embarrassing and unfair judgments about the subject of a photograph.[59]

3. Tort Law – Defamation

Obviously, the American privacy torts are of limited application in the OSN world. Are there other regulatory alternatives? It is possible that defamation law might be relevant in some cases. However, an image would have to amount to a defamatory communication for a defamation action. In many cases, an embarrassing or unflattering image will not be defamatory. Further, defamation law can do little about viral distributions of personal images, or about the permanence problem. Enforcement of a defamation order online can be problematic if the information in question exists in multiple websites and in multiple jurisdictions by the time the order is made. Additionally, internet 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 defamation suits online.[60]

4. Data Protection Law in the European Union

The European Union provides stronger data protection for its citizens than the United States under the auspices of the European Union Data Protection Directive ("the Data Protection Directive")[61]. However, there are some limitations to the reach of the Directive in the peer-based video context. The first is that the Directive is generally limited to conduct occurring within the European Union.[62] Thus, the Directive will not have global reach, subject to certain provisions that extend its operation to information of

---

58 See, for example, discussion in McClurg, *supra* note ___, at 926-927 (troubling consequences of loss of context when information is removed from its original context and revealed widely to strangers); ZITTRAIN, *supra* note ___, at 211 (problems of images being taken out of context online), 226-7 (describing issues arising from loss of context online and suggestions that hypertext protocols could be reconfigured to retain context by directing searches to original posting, rather than copies of the posting); 229-230 (loss of context can lead to blander information exchanges due to concerns about contextualization).

59 *id*., at 926-927 (troubling consequences of loss of context when information is removed from its original context and revealed widely to strangers), but see also ZITTRAIN, *supra* note ___, at 231 ("To be sure, contextualization addresses just one slice of the privacy problem, since it only adds information to a sensitive depiction. If the depiction is embarrassing or humiliating, the opportunity to express that one is indeed embarrassed or humiliated does not much help.")

60 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."). See also discussion in SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 152-153.

61 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.

62 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.

its citizens transmitted to third countries.[63] Perhaps more importantly, the Directive was drafted with the processing of text-based data in mind in the context of business or governmental dealings with personal information. There may be some question about the extent to which its provisions would apply to video files distributed by peers on OSNs. While "personal data" is defined broadly in the Directive as: "any information relating to an identified or identifiable natural person",[64] there are 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".[65] 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.

However, the second limitation on the Directive's operation may be more problematic. Article 3(2) of the Directive excludes its application from 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 provisions of the Directive. Of course, the Directive may apply to the OSNs that provide the forums for online networking, such as Facebook, MySpace, and Flickr. These services are operating businesses and are not engaged in purely personal or household activities, even if their customers' activities could be described in this way. Thus, an aggrieved plaintiff may have an avenue of recourse against a social networking site, if not against specific peers who post unauthorized images on the service.[66] Of course, enforcement of any order against an OSN service could still be problematic. Presumably, the OSN could only remove copies of a relevant image existing on its own servers and not those that had been distributed outside. Additionally, even finding all copies within the OSN's own servers could be problematic unless the particular image was tagged in some way.[67]

---

63 Data Protection Directive, Articles 25 & 26.

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

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

66 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.

67 Sue Chastain, *What is Tagging? Using Keywords for Digital Photo Organization*, ABOUT.COM: GRAPHICS SOFTWARE, available at http://graphicssoft.about.com/od/glossary/a/tagging.htm, last viewed on July 23, 2008 ("Tags are really nothing more than keywords used to describe a piece of data — be it a web page, a digital photo, or another type of digital document. Of course, organizing digital images by keywords and categories has been around for a long time, it just wasn't called "tagging" until fairly recently.")

In any event, limitations on a complainant's ability to bring actions against particular peers may be appropriate. The ability for individuals to complain about privacy incursions amongst themselves may have two important advantages over complaints against online service providers. The first is that it may help to develop social norms amongst online peers in terms of respecting each other's privacy. The second is that it would have less of a dramatic impact on online free speech and technological innovation than the ability to bring actions against online services providers. Commentators have expressed concerns in the past about over-broad use of intellectual property laws online.[68] Their concerns are with both the potential chilling of expression[69] caused by overzealous enforcement of intellectual property rights online,[70] as well as with the chilling of technological innovation that may ensue if innovators are too readily held liable for intellectual property infringements committed by their users.[71] Actions against innovators in social networking technologies may have a more adverse impact on online communications overall than actions involving only private individuals.[72]

With respect to free speech concerns, there are good arguments that the current balance between free speech and privacy rights online is weighted too heavily against privacy.[73] Particularly in the context of content created by private individuals about private individuals intended for closed social networks, it is arguable that calls for free speech are less powerful than in some other contexts. There is little suggestion that society will be harmed if individual privacy is better protected over OSNs.[74] This may be

---

[68] See, for example, Jacqueline Lipton, *Commerce Versus Commentary: Gripe Sites, Parody, and the First Amendment in Cyberspace*, 84 WASHINGTON UNIVERSITY LAW REVIEW 1327 (2006) (arguing against the overpropertization of domain names through unbridled application of trademark law); Margreth Barrett, *Domain Names, Trademarks, and the First Amendment: Searching for Meaningful Boundaries*, 39 CONN L REV 973 (2007) (discussing the need to balance free speech with trademark interests in the domain space); Todd Hartman, *The Marketplace vs. The Ideas: The First Amendment Challenges to Internet Commerce*, 12 HARV J LAW AND TECH 419 (1999); Neil Netanel, *Market Hierarchy and Copyright in Our System of Free Expression*, 53 VAND L REV 1879 (2000); Jack Balkin, *A Theory of Freedom of Expression for the Information Society*, 79 NYU L REV 1 (2004).

[69] *id.*

[70] *id.*; LESSIG, FREE CULTURE, *supra* note ___.

[71] See, for example, Alfred Yen, *Sony, Tort Doctrines, and the Puzzle of Peer-to-Peer*, 55 CASE W RES 815, 817-8 (2005) ("If technology providers become responsible for their users' misbehavior, they will stop developing and creating for fear of liability, and this will ultimately rob society of the many benefits that technology brings.").

[72] Congress has recognized this in the case of liability for online defamation and some liability for online copyright infringement by creating legislative "safe harbors" for intermediary Internet service providers against liability of their customers for relevant infringements: 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."); 17 U.S.C. § 512 (safe harbor for Internet service providers against contributory copyright infringement in particular listed circumstances).

[73] SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 89 ("The interests aligned against privacy – for example, efficient consumer transactions, free speech, or security – are often defined in terms of their larger social value. In this way, protecting the privacy of the individual seems extravagant when weighed against the interests of society as a whole.") In fact, arguments have been made that protecting privacy might actually further some of the same interests that free speech protects: SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 129-132.

[74] Daniel Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO LAW REVIEW 745, 760-764 (2007) (critiquing conceptions of privacy that pit privacy against free speech, and noting that society benefits when the value of privacy is not conceptualized within this

contrasted with situations where a digital image relates to a matter that is actually of public interest or concern, such as may be the case with an image of a public official in a comprising situation.

One example of where privacy harms may outweigh free speech concerns in practice is that relating to a young Canadian student who became known as "Star Wars Kid" online.[75] An embarrassing video file of him playing with a golf ball retriever as if it was a light saber from the "Star Wars" movies found its way online[76] and was transformed by many Internet users in various ways.[77] There may be a free speech argument that supports this conduct,[78] although one might question whether the free speech advocates for this kind of conduct think the cost justifies the end results. The young student ended up in psychiatric care for psychological damage related to his online embarrassment.[79] Thus, those who support the status quo, and oppose strengthening online privacy principles in the name of free speech, should think seriously about the conduct that can take place over open networks to humiliate and embarrass members of the very societies whose rights they seek to protect. Indeed, some commentators have argued that posting personal information about one's friends and acquaintances is unlikely to advance free speech interests in many cases.[80]

Again, these views may support developing privacy regulations that operate between peers online, rather than impacting online service providers. Perhaps the obligation should be on peers to respect each other's privacy online, and regulations

---

paradigm because individual privacy rights generally bow down before issues perceived as greater social goods such as free speech under this conception of the free speech versus privacy balance) (hereinafter, "*Nothing to Hide*").

75 SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 44-48.

76 *id*, at 44-45.

77 *id*, at 46-48.

78 Sánchez Abril, *supra* note __, at 29-32 (discussing problems of balancing First Amendment interests with the public disclosure of private facts tort in the online social networks context).

79 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…"). Similar ill fate befell "dog poop girl" in that she was apparently forced to quit her job as a result of the barrage of online harrassment about the incident involving her dog pooping on the subway train: ZITTRAIN, *supra* note ___, at 211. An even more unpleasant fate befell a Hong Kong bus passenger who later became known on the Internet as "Bus Uncle": 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 milllion people have viewed on 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.")

80 McClurg, *supra* note ___, at 928-9 ("[L]ittle justification or sociality utility exists in posting private information about an intimate partner or former partner on the Internet without the person's consent. Such information seldom will advance any core interest of free speech, yet can substantially jeopardize emotional, and even physical, security.") Of course, Professor McClurg was limiting his comments to intimate partner's in romantic relationships, but this principle holds true more generally with respect to friends and acquaintances.

should enforce these norms, rather than inhibiting the development of technologies that foster communication, such as OSNs. At least, there should be a balance between regulations that directly impact OSNs and those that operate between online peers. Remember, here, that the term "regulation" is being used broadly in this article to encompass laws, norms, market forces, system architecture, educational initiatives, and private institutions.

It is also important to acknowledge that advocating more individual privacy protection online is not necessarily advocating absolute protection to the extent that speech and communication are impossible. Rather, it is suggesting the development of some principles that would ensure that a video subject has some say in the dissemination of digital images in situations where it is reasonable to expect that the individual should be able to assert some control. Would this create a legal property right in a person's image?[81] Not necessarily. It would depend on how the control mechanism was framed. In particular, it would depend on the interplay between the various regulatory modalities identified above. Property rights are largely the creature of laws[82] and markets,[83] whereas norms and other regulatory modalities may not rely so heavily on notions of property.

B. LIMITATIONS OF CONTRACTUAL PRIVACY PROTECTIONS

Another current possibility for regulating online video privacy might be derived from the terms of use of OSNs and other online networks over which images may be disseminated. However, as with legal regulation, there are serious gaps and problems in relying on the current state of these terms of use. OSNs vary in the extent to which they impose terms on their users to respect others' privacy. Online services such as YouTube and Flickr, for example, allow large scale public dissemination of video information with little attempt at confidentiality. The operators of these services exercise some control over contents,[84] but rely heavily on their users to self-police.[85] Yahoo's terms of use, for

---

[81] SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 24-29 (critiquing property theory of privacy rights).

[82] Lessig, *The Law of the Horse, supra* note ___, at 520 ("The government could declare that information about individuals obtained through a computer network is owned by the individuals; others could take that information, and use it, only with the consent of those individuals.")

[83] See, for example, Richard Posner, *The Right of Privacy*, 12 GEORGIA LAW REVIEW 393, 397 (1978) ("That disclosure of personal information is resisted by, *i.e.,* is costly to, the person to whom the information pertains yet is valuable to others may seem to argue for giving people property rights in information about themselves and letting them sell those rights freely. The process of voluntary exchange would then assure that the information was put to its most valuable use.")

[84] 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, *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).

example, which are expressly incorporated into agreements to use Flickr, provide that each subscriber agrees not to use the online service to: "upload, post, email, transmit or otherwise make available any 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".[86] YouTube's Terms of Use provide that: "In connection with User Submissions, you … agree that you will not submit material that is copyrighted, protected by trade secret or otherwise subject to third party proprietary rights, including *privacy and publicity rights*, unless you are the owner of such rights or have permission from their rightful owner to post the material ….".[87]

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 the Yahoo and YouTube terms of use,[88] it also requests that its subscribers not use the service to: "upload, post, transmit, share, store or otherwise make available 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."[89] Facebook also 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."[90] 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."[91]

One limitation of these principles and policies is the extent to which they are legally enforceable. Even if these provisions do effectively become part of a user's contract with a relevant network,[92] the actual complainant about a privacy incursion is not a party to that contract. Thus, the victim of a privacy breach may not have standing to bring an action under the OSN's terms of use. Further, there is a definitional question as

---

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

[86] 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).

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

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

[89] *id.* See also Facebook's Code of Conduct, available at http://www.facebook.com/codeofconduct.php, last viewed on May 14, 2008.

[90] Facebook Principles, available at http://www.facebook.com/policy.php, last viewed on May 14, 2008.

[91] 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.

[92] For example, if the terms are presented in a manner where the user has to affirmatively assent to be bound by the terms, and if some meaningful consideration can be found to support the contract: *Specht v Netscape Communications Corp*, 150 F. Supp. 2d 585 (S.D.N.Y. 2001), *aff'd* 306 F. 3d 17 (2d Cir. 2002) (describing application of these contract law principles to online contractin).

to how to interpret a clause providing that a subscriber will not engage in conduct that is invasive of another person's privacy. There is no clear legal definition of conduct that is invasive of another's privacy in this context. Thus, any interpretation of such a clause would have to fall back on social norms.

This is not an insurmountable problem, but it does suggest that social norms will play a central role in resolving these kinds of disputes in the future: for example, one might argue that clauses prohibiting conduct that is "unlawful *or* invasive of another's privacy" suggest that the reference to privacy infringement is outside of, and separate from, purely legal conceptions of privacy. Otherwise, the policies would be drafted differently. If privacy within the policies was intended to connote purely *legal* privacy rights, arguably the policy would say something like: "users will not upload or transmit content that is unlawful in any way, *including* content that infringes another person's privacy rights". Juxtaposing privacy invasions with legal rights in the way that some current clauses are drafted could be regarded as a contractual attempt to enforce both legal rights and social norms relating to privacy.

With respect to clauses such as Facebook's requirement that a subscriber must only post material that she created or had permission to post, there is no definition of what constitutes "permission to post". In particular, there is no guidance as to whose permission must be obtained for the posting of what information: for example, if I take a group photograph of my high school class, do I have to obtain the whole classes' 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.[93] 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, such as picking her nose or adjusting her underwear? 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 behind this clause was to capture permission of those with proprietary interests in relevant content, such as copyrights or trademarks. It seems perfectly reasonable to require me to obtain copyright permission to post something, like a movie clip, that might otherwise infringe copyright. However, privacy rights work differently – if at all – in this

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

context. Some commentators have suggested that privacy should be treated as an intangible property right of some kind,[94] but there is little consensus on this point.[95]

YouTube's "permission to post" requirement is more closely linked to the concept of privacy rights than Facebook's requirement. YouTube requires that users agree not to submit any material that is subject to third party proprietary rights "including privacy and publicity rights" unless the user owns the relevant rights or has permission from the rights-holder to post the material.[96] Here, a privacy right is included in the concept of a property right. As noted above, this may or may not be a legally accurate conception of privacy. The privacy right is also linked with the notion of publicity rights in the YouTube clause. Publicity rights generally are treated as property rights, even though this theoretical justification for the rights has been criticized.[97] The linkage between privacy and publicity rights is a historical one. Publicity rights are generally regarded as having been born out of gaps left by the Warren and Brandeis conception of privacy[98] as applied to celebrities and public figures. Celebrities and public figures had a difficult

---

[94] 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).

[95] 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."); Posner, *supra* note ___, at 397-401 (critiquing theories that favour personal property rights in private information).

[96] Clause 6.D., YouTube's Terms of Use (available at http://www.youtube.com/t/terms, last viewed on July 23, 2008).

[97] See discussion in Jacqueline Lipton, *Celebrity in Cyberspace: A Personality Rights Paradigm for Personal Domain Name Disputes*, WASHINGTON AND LEE LAW REVIEW, forthcoming, 2008.

[98] SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 15 ("In 1890, Samuel Warren and Louis Brandeis penned their famous article, "The Right to Privacy," arguing for the legal recognition of a right to privacy, which they defined as a "right to be let alone.") It should be noted that the Warren and Brandeis conception of privacy actually drew from previous work by Thomas Cooley: Ruth Gavison, *Privacy and the Limits of the Law*, 89 YALE LAW JOURNAL 421, 437, and n.48 (1980) (noting that the concept of privacy as the "right to be let alone" is often incorrectly attributed to Warren and Brandeis, when it was actually first advanced by Cooley in T. COOLEY, LAW OF TORTS 29 (2d ed 1888); see also Diane Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L REV 291, 292 and n.2 (1983).

time convincing courts that defendants had intruded into their seclusion and infringed on their "right to be let alone", having actively sought the public eye for their livelihoods.[99]

Publicity rights were born to guard against unauthorized commercial exploitations of celebrities' names and likenesses.[100] The continuing linkage between privacy and publicity rights potentially connotes a property right in both contexts. Therefore, the drafting of YouTube's "permission to post" clause is problematic in that it implicitly requires a property right in private information as the basis for a complaint. As noted in the preceding paragraphs, it is not universally accepted that individuals have property rights in their own personal information.[101] Even those who think that individuals do – or should – own their personal information online have generally considered this question with respect to text-based data, rather than visual images.[102]

Images are qualitatively different in that they contain both more, and less, information about an individual. They capture something candid about the individual at a given moment in time.[103] Text-based data on the other hand, is iterative. The concerns about use of text-based data online have been about the way in which it can be

---

[99] GILSON ON TRADEMARKS, *supra* note ___, at § 2.16[1][a] (explaining the derivation of the right of publicity from the original Warren and Brandeis privacy conception, noting in particular that celebrities often did not suffer the same damages as private individuals with respect to commercial appropriations of their images, having sought public attention themselves; celebrities, rather, wanted to be financially compensated for unauthorized commercial profits made from their personas).

[100] *id.* (explaining the derivation of the right of publicity from the original Warren and Brandeis privacy conception, noting in particular that celebrities often did not suffer the same damages as private individuals with respect to commercial appropriations of their images, having sought public attention themselves; celebrities, rather, wanted to be financially compensated for unauthorized commercial profits made from their personas).

[101] 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."); Posner, *supra* note ___, at 397-401 (critiquing theories that favour personal property rights in private information).

[102] See, for example, discussion in Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 USF L REV 633 (2000); Litman, *supra* note ___.

[103] SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 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).

aggregated over a period of time to build up a detailed profile of a person.[104] It may take a whole collection of text-based data to suggest something that a picture candidly demonstrates in one digital file: for example, an aggregated text-based profile may include elements that suggest a person is trying to become pregnant. These records may include purchasing records and medical 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 tell the story in one glance.

Peer-based images are also qualitatively different from text in that they are likely to arise out of a relationship between the image subject and the photographer. This may suggest that both parties have rights to information contained in the image because they were both parties to a shared experience that led to the taking of the photograph. For example, a photograph at a given social event is a record of a shared experience between the photographer and the photographic subject. When information arises from relationships, and implicates joint interests in control of the information, the regulation of the dissemination of that information is more problematic than in situations where information purely pertains to one individual.[105] Of course, one could argue that much online text-based information also arises from a relationship – that of the relationship between the data subject and the organization with which the subject transacted. However, the information in the text-based data aggregation context is more likely to consist of discrete facts pertaining to the data subject[106] than the information contained in a photograph of a shared experience between two peers.

This discussion has so far not touched upon the question of the standing of a photographic or 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, say, YouTube's terms of use, her recourse would be to complain to YouTube that the subscriber had infringed her rights. It would be up to YouTube to decide whether the complaint had any merit, and whether to take any commensurate action against the subscriber, such as removing the posting, or barring the subscriber from the system.[107]

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

---

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

105 *id*., *supra* note ___, at 27 ("Personal information is often formed in relationships with others. All parties to that relationship have some claim to the information.")

106 For example, the person's name, address, telephone number, or Social Security Number.

107 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.

something qualitatively different to the way in which we conceptualize a friend in the physical world.[108] In the physical world, we know whether or not we are acquainted with a particular person. We may or may not know the person well, and we may even have forgotten the person's name. However, we are unlikely to consider someone a friend or acquaintance if we have never met them.

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 in person.[109] Although Facebook contemplates that its subscribers will use the service to find people online who they already know in the real world,[110] there is no way to ensure that this is the case in practice. It is easy to make relatively 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 who the subscriber, and the subject of any information on the subscriber's website, may not actually know. Of course, the practical problems can potentially be greater on an open network that does not even attempt to limit dissemination of information to online "friends". However, the point here is that "friends" in a closed network's terms of use may be a deceptively comforting concept for those concerned about online privacy.

III. SIX MODALITIES FOR VIDEO PRIVACY REGULATION

The problem of protecting privacy in cyberspace comes in part from an architecture that enables the collection of data without the user's consent. But the problem also comes from a background regime of entitlement that does not demand that the collector obtain the user's consent. Because the user has no property interest in personal information, information about the user is free for the taking.

- Professor Lawrence Lessig[111]

A. PROFESSOR LESSIG'S FOUR MODALITIES OF CYBERSPACE REGULATION

Like all new advances in communications technology, the rise of peer-based digital imaging capability creates new challenges for our regulatory system. Like most

---

[108] ZITTRAIN, *supra* note ___, at 218 (noting that a person's "friends" network online includes their "friends' friends' friends.")

[109] 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).

[110] 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).

[111] Lessig, *The Law of the Horse*, *supra* note ___, at 520.

digital age advances, these challenges are global in nature. As with cyberlaw more generally, we need to consider whether we are confronting the need for *new* regulatory approaches, or rather of simply expanding the application of current regulatory structures. In this context, it is important to appreciate that there is more than one possible regulatory modality for online conduct. Legal rules are not the only solution.[112]

In the early days of Internet governance debates, Professor Lawrence Lessig recognized four distinct regulatory modalities that would be useful in cyberspace.[113] They included legal rules, which Professor Lessig defined as rules that constrain our behavior by threatening punishment if we do not obey.[114] He then identified three other forms of regulation that are found in real space and that may be applied in cyberspace: social norms,[115] markets,[116] and architecture.[117] Social norms are similar to legal rules in that they threaten punishment for disobedience.[118] However, they differ in that the punishment is imposed by community, rather than government.[119] Markets regulate by imposing price constraints on certain behaviors.[120] In the privacy context in particular, Professor Lessig noted that one example of market forces as regulator is where firms are able to charge more to consumers if they provide greater assurances of personal privacy.[121] Architecture regulates by physically constraining certain types of behavior.[122] In the real world, for example, the erection of a border fence may constrain illegal immigration.[123] The

---

112 *id*., at 507-510.

113 *id*; Lessig, *The Architecture of Privacy*, *supra* note ___, at 62-63.

114 Lessig, *The Law of the Horse, supra*, note ___, at 507 ("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.")

115 *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.")

116 *id*. ("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.")

117 *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.")

118 *id*, at 507.

119 *id.*

120 *id*.

121 Lessig, *The Architecture of Privacy*, *supra* note ___, at 62.

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

123 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 ("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.")

cyberspace analog to physical world architecture is system architecture or "code".[124] According to Professor Lessig, this encompasses both the hardware and software aspects of an information technology system.[125] In the privacy context, Professor Lessig has suggested that encryption technology is an example of system architecture that could some way towards protecting online privacy.[126]

Professor Lessig further observed that none of the four modalities of regulation operates in a vacuum. They all rely on each other to some extent.[127] It is the interaction of the regulatory modalities that facilitates a given behavior in both direct and indirect ways.[128] Professor Lessig's account of regulatory modalities is very apt when one considers the regulation of digital video privacy amongst peer networks. No one modality effectively protects individual privacy in video images to the extent we might desire. Even the current interplay between these modalities arguably does not achieve that result. This article argues that we could more effectively identify and develop aspects of these, and other, regulatory modalities, as well as potential interactions between them, in ways that might better protect privacy online. In this context, it suggests the recognition of two additional regulatory modalities in the OSN context: (a) public education,[129] and, (d) private institutions.[130] Private institutions might comprise OSNs themselves, but perhaps more to the point, public interest organizations like the Electronic Frontier Foundation[131] ("EFF") and the Electronic Privacy Information Center ("EPIC").[132] The identification of new forms of regulatory modality is not inconsistent

---

[124] 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.")

[125] *id.*, at 509.

[126] Lessig, *The Architecture of Privacy*, *supra* note ___, at 63.

[127] 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 A Michael Froomkin, *The Death of Privacy?*, 52 STAN L REV 1461, 1466 (2000) ("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.")

[128] 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).

[129] 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.

[130] 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).

[131] 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).

[132] 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).

with Professor Lessig's work – he did not intend for his four regulatory modalities to be the last word on cyberspace regulation.[133]

The remainder of this Part identifies the key features of each of these six regulatory modalities and how they might be usefully applied in practice to create more effective protections for online privacy. In so doing, it necessarily considers the potential interactions between the six modalities, as it is unlikely that any one or more of these modes of regulation, operating alone, could achieve an appropriate balance of interests involving video privacy.[134] Before turning to the individual modes of regulation, it is worth first touching on the necessity of characterizing a video privacy right as either a form of property right or something else. As some of the regulatory modalities identified here, such as market forces, are often regarded as necessitating property interests for the efficient operation of markets,[135] it is important to establish the contours of video privacy rights in terms of whether or not that are, or need be, classified as a form of property.

B. PROPERTY RIGHTS IN PERSONAL INFORMATION?

One issue that has plagued privacy law has been uncertainty about whether individuals have – or should have – a property right in their personal information.[136] If such a property right is to be recognized, what form should it take? Some commentators have assumed that, absent a governmentally recognized property right in personal information, there is scant policy justification for enacting new laws to protect online privacy.[137] Professor Lessig, for example, has argued that the creation of a property right in personal information would be a matter for government.[138] Once governmentally established, the right would be instrumental in regulating unauthorized uses of personal information in terms of familiar civil and criminal law concepts such as misappropriation

---

133 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…").

134 Balancing of competing interests is a central part of developing a useful approach to privacy: SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 87 ("We live in an "age of balancing," and the prevailing view is that most rights and liberties are not absolute. Because privacy conflicts with other fundamental values, such as free speech, security, curiosity, and transparency, we should engage in a candid and direct analysis of why privacy interests are important and how they ought to be reconciled with other interests. We cannot ascribe a value to privacy in the abstract.")

135 See, for example, discussion in Posner, *supra* note ___, at 397 ("That disclosure of personal information is resisted by, *i.e.,* is costly to, the person to whom the information pertains yet is valuable to others may seem to argue for giving people property rights in information about themselves and letting them sell those rights freely. The process of voluntary exchange would then assure that the information was put to its most valuable use.")

136 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).

137 Lessig, *The Law of the Horse, supra* note ___, at 520 ("Because the user has no property interest in personal information, information about the user is free for the taking.").

138 *id*. ("The government could declare that information about individuals obtained through a computer network is owned by the individuals; others could take that information, and use it, only with the consent of those individuals.")

and theft.[139] It would also facilitate private negotiations between parties about uses of personal data.[140]

While governments can undoubtedly regulate personal information as a property right, there is a question as to whether they should. Property rights in information have always been contentious.[141] They create concerns about chilling speech.[142] Governments who create property rights in information therefore must act to preserve the balance between those rights and speech. This is a difficult task and is not always successfully achieved in practice.[143] In a federal system, the propertization of information can raise constitutional questions about which level of government has legislative competence to enact relevant laws. If the state governments are the appropriate bodies to undertake this task, problems arise as to interstate harmonization of law, particularly where information transcends state, and even national, borders at the press of a button.[144]

In any event, none of this gets to the underlying question of a policy justification for treating private information as property. It is tempting to accept that if something has value, as private information potentially does - depending on the context and how value is defined[145] - it should be treated as property. The problem with this reasoning in the context of the present discussion is that much of the economic value in online information to date has been in text records in the hands of data aggregators.[146] While there may be good arguments for creating property rights in compilations and databases

---

139 *id*. ("This declaration of [property] rights [in personal information] could … be enforced in any number of traditional ways. The state might make theft of such information criminal, or provide special civil remedies and incentives to enforce individual rights if such information is taken.")

140 Lessig, *The Architecture of Privacy*, *supra* note ___, at 63.

141 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).

142 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.")

143 SOLOVE, THE FUTURE OF REPUTATION, *surpa* note ___, at 129-132 (describing problems in attempting to balance privacy torts with the idea of free speech); Zimmerman, *supra* note ___ (suggesting that torts prohibiting true speech cannot be reconciled with the First Amendment); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN L REV 1049 (2000) (suggesting that tortious approaches to protecting privacy cannot be reconciled with the First Amendment, but that contractual approaches may avoid this criticism).

144 There may also be copyright preemption problems in some jurisdictions depending on the nature of the property rights created.

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

146 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).

in the hands of data aggregators,[147] it is not necessarily true that personal information in the hands of the individual to whom it relates is a valuable commodity in terms that justify a property right.[148]

Even where information in a video format is aggregated in forums like OSNs, there is little theoretical justification for granting a property right to either the data subject or the person who controls the photograph.[149] This is because the private individuals networking over OSNs are not likely doing so for commercial purposes that would justify or necessitate a property right either in data about them or in data about others that appears on their personal webpages. There may be a justification for importing a property right to the provider of an OSN in respect of its meta-collection of data. This is because the OSN operators might argue that they 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 utilize their vast collection of users as an incentive to attract advertisers.[150]

Of course, not all property rights are justified on the basis of economic value. Many theoretical conceptions of property do not require economic value as a necessary element, and some commentators have argued that just because something has a commercial value does not mean that it automatically merits a property label.[151] 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. An old dog-eared copy of a Shakespeare play, for example, may no longer have any real 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.

Even traditional property rights may be characterized by things other than commercial value. These things might comprise the ability to exclude others, the ability to enjoy an item free from interference, or the ability to alienate or transfer rights in the

---

147 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).

148 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).

149 Of course, the person who controls the photograph is likely to own copyright in the photograph by default, even if she has no intention of making any commercial use from the photograph: 17 U.S.C. § 102(a)(5) (includes copyright in photographs under definition of "pictorial, graphic, and sculptural works" in 17 U.S.C. § 101).

150 Although 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).

151 LESSIG, FREE CULTURE, *supra* note ___, at 19 ("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.")

item whether or not for commercial value.[152] These typical proprietary attributes are generally missing from personal information. It would be very difficult for any individual to meaningfully function in society, particularly online, without leaving footprints involving disclosures of personal information. Thus, there is no meaningful way of excluding others from personal information or to enjoy the information free from interference. Sometimes information is required by others, as by contract, to complete a purchase.[153] 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.[154] Online, individuals constantly leave digital footprints involving this kind of information.[155]

Of course, advocates of property rights in personal information may well argue that it is these very aspects of personal privacy that require a property label. The necessity of transacting with personal information on a day to day basis requires that the individual be entitled to bargain for value for exchanges involving this information.[156] However, this is a circular argument. It assumes that something should be labeled property because individuals are effectively forced to disclose it and therefore they should be compensated for doing so. This might be justified on the basis of some kind of unjust enrichment theory. In other words, data aggregating businesses are unjustly enriched by individuals if they can put together valuable consumer profiles using information "belonging to" others without compensating them for it.

However, unjust enrichment actions are not of necessity based on the identification of a property right in the plaintiff.[157] Thus, an unjust enrichment analysis does not necessarily resolve the privacy-as-property question. Additionally, the unjust enrichment solution would also suffer from the fact that restitution law has an uncertain theoretical basis.[158] Unjust enrichment may be an equally unstable basis for protecting privacy interests as property theory. Outside of property and restitution theory, there may be arguments based on autonomy and personhood for granting legal rights in personal privacy.[159] In the context of attempting to explain the philosophical underpinnings of the

---

[152] 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).

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

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

[155] *id*.

[156] 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 …").

[157] 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 …. But while the remedy for defendant's unjust enrichment will often involve restoring something to the plaintiff, remedies that consist in restoration are by no means coextensive with liability for unjust enrichment.")

[158] *id*, at 1191 (1995) ("Significant uncertainty shrouds the modern law of restitution. Few American lawyers, judges, or law professors are familiar with even the standard propositions of the doctrine, and the few who are continue to disagree about elementary issues of definition.")

[159] Daniel Solove, *Conceptualizing Privacy*, 90 CALIF L REV 1087, 1116-1121 (2002) (discussion of personhood theories of privacy) (hereinafter, "*Conceptualizing Privacy*"); Solove, *Nothing to Hide*, *supra* note ___, at 760-1 (noting that many theories of privacy view the notion of privacy as an individual right

right of publicity, which is derived from the right to privacy, various commentators have suggested basing such rights in notions of autonomy and personhood.[160] This is a possibility, but again, the theoretical contours of a right of personhood are unclear,[161] and the theory may not be any more useful than trying to pin down a privacy right as a form of property.

One question that might be worth posing at this point is whether it is actually necessary to create one single philosophical underpinning for online privacy rights, at least at this very moment.[162] This is clearly a time when individuals feel that they are being harmed, to a greater or lesser extent, by much online conduct that interferes with their ability to control their own personas in cyberspace.[163] Nevertheless, there is currently little consensus within academia or legal practice as to the nature and scope of individual privacy rights. It may be that the legal label ultimately attached to privacy rights, and the philosophical underpinnings justifying that label, need to be developed in the future as the contours of the rights develop over time.[164]

In other words, it may be that the various regulatory modalities for information privacy need a chance to work together over time ultimately to create a situation where it is easier to identify the legal nature of, and philosophical justification for, distinct online privacy rights. It may be that for the time being, all we need to do is think about privacy rights in terms of some form of control mechanism relating to the permitted accesses and uses of personal information online.[165] Obviously, this mechanism needs to be balanced against other interests including free speech and, probably to some extent, intellectual property law.[166]

---

related to protecting the individual's personal dignity); Sánchez Abril, *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).

160 See discussion in Lipton, *Celebrity in Cyberspace*, *supra* note ___, at ___.

161 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).

162 In fact, this is arguably the approach taken by Professor Solove who prefers taking a "bottom-up" approach to identifying and resolving related privacy problems as the basis for his taxonomy of privacy, rather than identifying one overarching theoretical principle to explain privacy rights: 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. If we study the problems together, we can better understand the entire cluster.")

163 SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___ (the text is replete with examples of ways in which individuals and their reputations are being harmed by online conduct).

164 Solove, *Nothing to Hide*, *supra* note ___, at 759-760 (noting that it might be worth taking an approach that focuses on solving practical problems of privacy rather than spending too much attention trying to discern a perfect theoretical basis for the concept of privacy).

165 See discussion in Jacqueline Lipton, *A Framework for Information Law and Policy*, 82 OREGON LAW REVIEW 695 (2003).

166 SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 87 ("We live in an "age of balancing," and the prevailing view is that most rights and liberties are not absolute. Because privacy conflicts with other fundamental values, such as free speech, security, curiosity, and transparency, we should engage in a candid and direct analysis of why privacy interests are important and how they ought to be reconciled with other interests. We cannot ascribe a value to privacy in the abstract.")

This approach is not as foreign as it might seem. Most intangible property rights developed organically as societal and economic needs arose. Trademarks, for example, arose initially to address needs of the commercial community to guard against unfair competition practices relating to false or misleading branding of goods and services.[167] There is still some international disagreement as to whether trademarks are appropriately characterized as property rights.[168] Nevertheless, domestic trademark laws are still able to function despite the lack of consensus as to the underlying theoretical explanation of a trademark. Trade secrets are another case in point where theoretical justifications for the rights are somewhat varied both within and between jurisdictions.[169] Nevertheless, the system is able to function in practice.

Even Internet domain names have an uncertain legal status as property. In some contexts they have been regarded as a form of intangible personal property,[170] whilst in others they are regarded as a pure contractual license.[171] Nevertheless, the domain name system continues to function, while market forces, social norms, and judicial decisions iron out the underlying philosophical creases. Indeed, Professor Solove, one of this era's leading privacy theorists, advocates a bottom up, problem-solving approach to theorizing privacy in the digital age.[172] His views reflect that fact that privacy problems in this era

---

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

168 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).

169 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).

170 *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).

171 *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).

172 Solove, *Conceptualizing Privacy*, *supra* note ___, at 1129 ("[T]his Article advances as "approach" to understanding privacy rather than a definition or formula for privacy. It is an approach because it does not describe the sum and substance of privacy but provides guidance in identifying, analyzing, and ascribing value to a set of related dimensions of practices. An approach to conceptualizing privacy should aid in solving problems, assessing costs and benefits, and structuring social relationships. My approach is from the bottom up rather than the top down because it conceptualizes privacy within particular contexts rather than in the abstract.")

require a pragmatic approach[173] based on solving particular problems,[174] acknowledging their differences, while at the same time recognizing their similarities.[175]

C. LEGAL RULES AS PRIVACY REGULATOR

1. The Role of Legal Regulation Online

Lawyers have a tendency to regard legal rules as the paramount – and sometimes the only – solution to a given problem.[176] This is not surprising, given our training. Professor Lessig has described legal rules as: "rules that constrain our behavior by threatening punishment if we do not obey."[177] He also notes that the law threatens punishment after the fact for failure to comply with pre-set rules.[178] Laws have limits as a regulatory modality, especially online. In particular, an effective enforcement mechanism has to be created to ensure that laws are appropriately enforced. This does not mean one hundred percent enforcement, but at least sufficient enforcement – or threat of enforcement – to constrain the behavior of individuals to comport legal rules. This is difficult in the online context. Enforcement can be problematic where many online actors are anonymous, or are situated in different jurisdictions. Identifying potential defendants, and enforcing laws against them can be very tricky in cyberspace. These problems can also involve significant costs to potential plaintiffs or government agencies seeking to bring action against alleged online wrongdoers.

Governments also often need to make difficult policy choices in enacting new laws, particularly where those laws seek to balance competing interests such as privacy, speech, and property rights. The novelty of much online conduct exacerbates the difficulties for governments in identifying appropriate policies on which to base legal regulation. 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 will have difficulty identifying appropriate policy justifications and balances for new laws.

---

173 SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 87-88 (describing pragmatic approach to privacy theory).

174 *id*, at 75 ("I contend that the focal point for a theory of privacy should be the problems we want the law to address.")

175 Daniel Solove, *A Taxonomy of Privacy*, 154 U PA L REV 477, 486-7 (2006) ("The taxonomy [of privacy] demonstrates that there are connections between different harms and problems. It is no accident that various problems are referred to as privacy violations; they bear substantial similarities to each other. But we also must recognize where they diverge. The goal is to define more precisely what the problem is in each context – how it is unique, how it differs from other problems, and how it is related to other types of privacy problems.").

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

177 Lessig, *The Law of the Horse*, *supra* note ___, at 507 ("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.").

178 LESSIG, FREE CULTURE, *supra* note ___, at 121 ("[L]aw constrains by threatening punishment after the fact if the rules set in advance are violated.").

Legal rules are therefore unlikely to be the stand-alone answer to privacy problems involving online video dissemination. Laws will have some place, likely an important place,[179] in the overall regulatory matrix, but they cannot solve online privacy problems on their own. The challenge for regulators is to identify exactly what role legal rules should play in relation to online video privacy issues, and how those rules should interact with other forms of regulation. Recently, commentators have made some suggestions along these lines. Professor Solove suggests that even though legal regulation will not be the complete answer to our online privacy problems,[180] online privacy regulation could be bolstered by the law: (a) recognizing privacy in public;[181] (b) better protecting confidential relationships;[182] and, (c) allowing individuals to exercise greater control over their personal information after it has been exposed to other people or even to the general public.[183]

There are, in fact, a number of specific areas in which laws might be enacted, modified or strengthened to assist in combating online privacy incursions in the situations under consideration in this article. They include: (a) torts protecting rights of privacy and publicity; (b) legislation promoting codes of conduct and technical standards for protecting privacy; and, (c) contracts and breach of confidence actions. Additionally, there are models for laws regulating information that could usefully be adapted to address privacy interests online. In this context, privacy law might draw some inspiration from lessons learned previously in digital copyright law and environmental regulation.

2. Lessons from Digital Copyright Law

Professor Solove has noted some of the parallels between the regulation of online privacy and the regulation of copyright online.[184] In particular, he identifies ways in which copyright law has managed to effectively protect copyrights in online video, despite early concerns about the ability of rights holders to exercise control over digital information.[185] He uses the example of digital copyright law to answer those who suggest that it is impossible to regulate privacy online because it is too difficult to obtain effective

---

179 *id*, 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.")

180 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.")

181 *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, *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.").

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

183 *id*, at 188.

184 *id*, at 185.

185 *id*, at 184-186.

control over digital information.[186] He notes that copyright law applies online regardless of whether information has been accidentally exposed to the public or not,[187] and even if it is in a digital format that can be readily copied.[188] His point is that the copyright example proves that legal rules can control information online, including digital video information that is easy to reproduce and disseminate at the push of a button.

In fact, there are many similarities between online privacy regulation and digital copyright regulation. Common issues include: (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[189] and other legitimate uses;[190] (c) what kinds of liability, if any, should be faced by Internet intermediaries, such as Internet service providers, for unauthorized activities of others;[191] (d) identifying appropriate forums for dispute resolution in a global information society; (e) dealing with global disharmonization of relevant legal principles;[192] (f) identifying wrongdoers in a largely anonymous online medium;[193] and, (g) providing remedies for viral online dissemination of protected information.[194] Thus, copyright law may prove a

---

[186] *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.")

[187] *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.")

[188] *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.")

[189] In fact, Professor Solove notes that copyright protections have proved so strong online that even First Amendment concerns yield before copyright: SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 186.

[190] 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).

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

[192] 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.")

[193] 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.)

[194] As Professor Solove notes, 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: SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 184-5.

useful model for enhanced privacy regulations online, particularly with respect to privacy rights in video files.

Of course, copyrights are also specific legal rights that need to be balanced against privacy rights online. The holder of the copyright in a video file will not necessarily be the subject of the video image. Copyright ownership will usually fall to the person who takes a photograph, not likely the subject of the image.[195] Because today we have strong copyright laws and relatively weak privacy laws, at least in the United States, the copyright holder will generally win any battle for control of an online video image.[196] This does not necessarily have to be the case. Strengthened privacy laws could help to redress this imbalance.[197]

In any event, the copyright model could be a useful basic model for those seeking to strengthen privacy rights online. Although digital copyright law has arguably created its own imbalances,[198] those seeking to enact laws that protect privacy rights online could learn from the past problems of digital copyright law, while taking away the lesson that online information control through legal regulation is not impossible. Of course even digital copyright law has been bolstered in many respects by contract law and technical standards.[199] It is another example of an area where legal regulation alone is not sufficient as a regulatory modality, and where the law needs to interact with other regulatory modalities. It is also an example of an area of law where balancing competing interests is important. Privacy law advocates now have an opportunity to get the balance right in the wake of some of the arguable failures of digital copyright law in this respect.

3. Lessons from Environmental Regulation

Environmental regulation is another area of law that may be instructive as a model for protecting online privacy. Professor Hirsch, for example, draws on some of the more recent legislative approaches to environmental protection as a possible model for online privacy law.[200] He identifies the way in which environmental law has moved away from command and control models[201] towards second generation initiatives that

---

195 *id*., at 184 ("Copyright in a photo is owned initially by the person who takes the photo, not by the person whose photo is taken.")

196 Professor Solove recounts a story where, in a battle for control of such an image online, the holder of copyright in the photograph was able to control a photograph of a radio call-in show host – Dr Laura Schlessinger – even against Dr Schlessinger herself: SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 183-184.

197 SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 185 (noting that the development of online copyright law suggests that privacy law could be strengthened in a similar way).

198 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 ___.

199 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).

200 Dennis D Hirsch, *Protecting the Inner Environment: What Privacy Regulation can Learn from Environmental Law*, 41 GEORGIA LAW REVIEW 1 (2006).

201 *id*., at 8.

encourage regulated parties to choose for themselves the means by which they will achieve regulatory goals.[202] He then draws on similarities between environmental regulation and information regulation,[203] to suggest lessons for information privacy law that could usefully be drawn from the experience of environmental protection legislation. He suggests that we look to the law as a means to facilitate the development of market forces to achieve desired regulatory goals.[204] Rather than suggesting enhanced information privacy laws of the command and control variety, Professor Hirsch advocates utilizing legal rules to set regulatory goals and to incentivize market players to achieve those goals.[205]

Professors Mulligan and Simitian have taken this reasoning a step further in discussing the efficacy of security breach notification laws in the United States.[206] Professors Mulligan and Simitian identify information disclosure laws in the environmental context as a useful analogy with information disclosure laws about security breaches in the online privacy context.[207] They note that information disclosure laws in both contexts facilitate the flow of information into the marketplace and allow market participants to make better and more efficient decisions about complying with regulatory goals.[208] In the environmental law context, the goals may be to reduce pollution emissions. In the information security context, the goals may be to better secure private information and to avoid data security breaches in the future. Professors Mulligan and Simitian note that laws requiring companies that collect personal information to disclose security breaches in relation to that information might give those corporations, and others, sufficient market incentives to invest in technology to prevent such breaches.[209] This again evidences the important interplay between legal rules and market forces as regulators. Of course, none of this specifically relates to the protection of privacy in digital video images, but models could be developed to enhance video privacy based on the interplay of laws and market forces along these lines. Some suggestions are considered in Part III.E *infra*.

4. Privacy and Publicity Torts

---

202 *id*.

203 *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.")

204 *id*, at 37-39 (discussing benefits of second generation regulatory strategies in encouraging market players to innovate in best methods for addressing regulatory goals).

205 *id*. (discussing benefits of second generation regulatory strategies in encouraging market players to innovate in best methods for addressing regulatory goals).

206 Deirdre Mulligan and Joseph Simitian, *Assessing Security Breach Notification Laws*, work in progress, copy on file with the author.

207 *id*., at 10-11.

208 *id*., at 11.

209 *id.*; Froomkin, *supra* note ___, at 1527 (suggesting that in the absence of at least the threat of some form of government regulation, there is little market incentive for online entities to invest in privacy enhancing technologies).

Having considered the viability of legal models for regulating information generally, it is now appropriate to turn to specific areas of law that might be extended to protect privacy interests in online video. An obvious port of call is the rather uncohesive set of privacy torts in the United States[210] which can be largely traced back to the work of Dean Prosser in 1960.[211] One or more of these torts could be strengthened to operate more effectively in an online world. Professor Sanchez Abril, for example, has suggested strengthening the tort relating to public disclosure of private facts[212] to allow it to operate more effectively in the OSN context.[213] She notes that the public disclosure tort developed at a time when the law was concerned with intrusions into physical spaces,[214] and is thus not well suited to a non-physical online world.[215] She suggests re-focusing enquiries about public versus private activities, in the context of the public disclosure tort, to better meet the needs of the information society. In particular, she suggests: (a) thinking about zones of confidentiality created by system architecture, agreements and relationship bonds, rather than physical walls;[216] (b) categorizing privacy harms that ensue from information disclosure rather than categorizing certain subject matter as *per se* private;[217] and, (c) thinking in terms of overall accessibility of online information rather than in terms of whether it was completely secret or secluded.[218]

Related to the privacy torts is the right of publicity. This tort prevents the use of someone else's name or likeness for financial benefit.[219] Professor Solove has suggested that the right of publicity could be expanded to help individuals control uses and dissemination of their images online.[220] As currently formulated, the publicity rights tort is limited to unauthorized *commercial* uses of an individual's name or likeness. Thus, it

---

210 Restatement (Second) of Torts, §§ 652A-E (1997).

211 SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 101 (describing the four types of harmful activities Prosser identified under the rubric of privacy, which were later codified by Prosser in the Restatement (Second) of Torts §§ 652A-652E (1997)). Of course, Prosser was extending on the work of Warren and Brandeis, and they, in turn, were extending to some extent on the work of Thomas Cooley: SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 101 (describing the way in which Prosser's work drew from the earlier work of Warren and Brandeis), 16(describing how Warren and Brandeis drew from the earlier comments of Judge Thomas Cooley).

212 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.")

213 Sánchez Abril, *supra* note __.

214 *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.")

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

216 *id*., at 47.

217 *id.*

218 *id.*

219 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.").

220 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 …")

does not cover many of the situations arising by unauthorized posting and dissemination of photographs on OSNs. Most of these uses are not for commercial gain, but merely for amusement and discussion.[221] Professor Solove recognizes that the right of publicity could be strengthened for use in this context, but, as with utilizing the copyright model to strengthen online privacy rights, difficult balancing issues would need to be resolved.[222] Professor Solove suggests that one might find this balance in ensuring that the appropriation tort could only apply: "when people's photos are used in ways that are not of public concern."[223] This would be consistent with recognized limitations of the public disclosure tort.[224] The appropriation limb of Dean Prosser's privacy torts[225] is clearly related to the right of publicity tort, so similar comments would apply to extending this arm of privacy law to OSNs as to the right of publicity tort.

However, the other elements of American privacy tort law are less promising for the situations under consideration in this article. The intrusion tort[226] relates largely to incursions into one's physical space or private affairs. It is unlikely to cover concerns about unauthorized dissemination of video images often captured with the consent of the image subject. Of course, the scope of this tort might be expanded to define an intrusion more broadly, perhaps in a way that contemplates intrusions into a person's peace of mind by unauthorized use or dissemination of a private image. However, this does seem a stretch and it may not always be easy to ascertain the scope of such an intrusion. The suggestions of Professors Solove and Sanchez Abril seem to be simpler avenues to achieve the desired result here.

The false light publicity tort[227] is likewise not well suited to online video situations because it is not aimed at truthful information – and images of an individual will generally represent something truthful unless they have been altered in some way to imply something untrue about the subject. An example might be photoshopping[228] an image to make it seem that the subject was drinking or taking drugs. Outside of the obvious photoshopping example, it may be very difficult in particular cases to establish false light in relation to an image that is effectively truthful in that it accurately recorded

---

221 *id.* ("The appropriation tort would rarely apply to the discussion on the Internet of people's private lives or the posting of their photos.")

222 *id*. (querying how much control we want to give people over their images online).

223 *id.*

224 *id.*

225 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.")

226 *id*., § 652B ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.")

227 *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.")

228 Wikipedia defines "photoshop" as follows: "Adobe Photoshop, or simply Photoshop, is a graphics editing program developed and published by Adobe Systems. It is the current and primary market leader for commercial bitmap and image manipulation, and is the flagship product of Adobe Systems." (http://en.wikipedia.org/wiki/Adobe_Photoshop, last viewed on July 24, 2008).

a person in a given situation. Again, Professors Sanchez Abril's and Solove's suggestions relating to extending the scope of the public disclosure tort and the publicity rights tort respectively are probably better solutions to the problems identified here than attempting to establish false light in the video privacy context.

5. Privacy Contracts and Breach of Confidence Actions

Another area where legal rules could better protect online privacy rights is through the use of express or implied contracts, and breach of confidence actions. These issues are treated together because they all rely on relationships between specific individuals. 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 by the legal system to protect a relationship that the law regards as requiring a particularly high duty of confidentiality because of its very nature. Examples are the doctor-patient relationship and the preacher-penitent relationship.[229]

Relationships that give rise to legal obligations of confidence are a good model for the legal regulation of privacy. The problem is that the kinds of situations addressed in this article relating to online video privacy do not generally involve relationships that the law would currently regard as involving legal obligations of confidence. However, this could change. Express contracts of confidentiality might be problematic here because it is unlikely that private individuals taking images of each other and posting them online have the time, inclination, or experience to enter into express contracts to protect each other's privacy. However, implied contracts recognized by the legal system might be a viable alternative.

Several commentators have recognized that implied contracts, and even express contracts in some circumstances, could be utilized in interpersonal relationships for legal enforcement of privacy and confidentiality expectations. Professor McClurg, for example, has suggested the development of implied contracts of confidentiality for intimate relationships generally.[230] His suggestion contemplates protection for both text-based information shared in confidence and video information pertaining to the relationship in question.[231] His particular concern is with dissemination of that information online.[232] His ideas could be extended to social relationships more broadly, particularly those that involve dissemination of information online.

---

[229] 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).

[230] Andrew McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U CIN L REV 887 (2006).

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

[232] *id.* (giving examples of online text-based and video disseminations of confidential information).

Professor McClurg's writings echo suggestions made earlier by both Professor Zimmerman[233] and Professor Volokh[234] about utilizing express or implied contracts, rather than tort law, to protect individual privacy.[235] Professors Zimmerman and Volokh each expressed concern that tort law protections for privacy were generally open to criticism as unconstitutional encroachments on the First Amendment freedom of speech.[236] Professor Volokh suggests that express or implied contracts of confidentiality, although not a perfect solution for privacy advocates, are the only legal method of avoiding these First Amendment concerns.[237] However, he identifies two important limitations of contractual solutions for protecting privacy that may have significant ramifications 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.[238] In the OSN situation, people disseminating each other's images online are unlikely to be in contractual relationships with the image subjects for the most part, and are also unlikely to be agents of image subjects or of image takers. The second limitation of contractual solutions is that contracts cannot be enforced against minors.[239] This may be a significant problem in the OSN context because presumably many people sharing images online are minors. Contractual solutions may also pose jurisdictional problems online given the global nature of the Internet.

In a similar vein to those suggesting the recognition of implied contracts of confidentiality, some commentators have suggested the extension of breach of confidence torts to better protect individual privacy. Professors Solove and Richards suggest extending American breach of confidence tort jurisprudence in a manner that draws from current British law on breach of confidence.[240] They note that British law, by default, currently protects a greater array of relationships of confidence than American law.[241] With respect to the First Amendment concerns raised by Professors Zimmerman and Volokh, Professors Solove and Richards acknowledge that any tort law solution to privacy problems is open to First Amendment challenge, and that tortious breach of

---

233 Zimmerman, *supra* note ___..

234 Volokh, *supra* note ___.

235 Zimmerman, *supra* note ___, at 363-364; Volokh, *supra* note ___, at 1052, 1122.

236 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, *supra* note ___.

237 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, *supra* note ___, at 363 (suggesting looking into contractual solutions for protecting privacy rather than tort law).

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

239 *id*., at 1063.

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

241 *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.")

confidence actions may be subject to the same critique.[242] However, they suggest that torts based on relationships may be less objectionable than torts generally enforceable against the world where it comes to encroachments on speech.[243]

Nevertheless, there are some limitations to the tort approach, even when based on relationships of confidence. Professors Solove and Richards have noted that the English breach of confidence tort is subject to a number of exceptions including: (a) consent; (b) information being trivial; (c) information being in the public domain; and, (d) information being in the public interest.[244] While the latter two issues are unlikely to be of much relevance to the situations contemplated in this article, the first two limitations on the action are potentially problematic. As noted in the opening section of this article, many digital images are taken with consent. This does not necessarily mean that they are *disclosed* with the consent of the image subject, although there will be a serious question as to what a consent to a disclosure means in this context. If the image subject consents to the posting of an image on a friend's Facebook page, does that contemplate downstream uses by others who may access the image from the friend's page?

There is also the potential limitation that much information posted on OSNs is trivial and should not give rise to tortious actions for breach of confidence. Again, there are going to be some serious definitional problems here. Is it the information *per se* that might be identified as trivial, or rather the context of its use online? For example, the "Star Wars Kid" episode and the "dog poop girl" episode both revolve around digital information that is *per se* fairly trivial. After all, how important is it that someone's dog pooped on the subway or that some kid played with a golf ball retriever as if it was a light saber from Star Wars? The resulting harassment and embarrassment caused to the image subject in each case was far from trivial on a personal level,[245] yet this is a result of the nature of the *use* of the images online, rather than the nature of the *information* contained in the images. An otherwise fairly trivial image can take on a life of its own online.

Paradoxically, the triviality criterion that has previously cut against tort liability for unauthorized disclosures would now arguably cut against First Amendment concerns online. If information is trivial, there is arguably less need for the First Amendment to protect it. Thus, if we are talking about balancing free speech interests against privacy, it may be that the potential harm from disseminating even trivial information online so seriously outweighs any First Amendment concerns that there should be no constitutional objection to a tortious action here.

Another limitation of the breach of confidence tort on its own is that it does not deal effectively with data aggregation, and sometimes associated identification,

---

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

243 *id*, at 178-180.

244 *id*, at 165.

245 ZITTRAIN, *supra* note ___, at 211-2 (noting that "Bus Uncle" was beaten up in a targeted attack as a result of his online exposure, "dog poop girl" was ultimately forced to quit her job, and "Star Wars kid" suffered severe psychological trauma as a result of his online humiliation and embarrassment).

problems[246] such as those arising in the "dog poop girl" scenario. It was not only the subway passenger's image that was ultimately posted on the Internet. It was augmented by various Internet users with information relating to her identity and contact details.[247] This allowed her to be easily harassed and shamed in an ongoing way, and ultimately resulted in her quitting her job[248] – a result of the permanence problem. An enhanced breach of confidence tort action for the information age may well need to better take account of the problems of viral distribution, aggregation, identification, and indeed, information permanence, than existing legal models. Thus, solutions to privacy invasions based on contractual or tortious breaches of relationships of confidence are a possible solution to some of the problems addressed in this article. However, neither of them are currently sufficiently developed to deal with these problems effectively.

6. Legislating Codes of Conduct and Technical Standards

Another way in which legal rules might be used to enhance privacy protections involves utilizing laws to encourage certain social behaviors and technical standards. This is perhaps an analog to the discussion of the environmental regulation model of legislating best practices to encourage markets to behave in a particular way. Here, we are talking about legislating best practices to encourage either markets or individuals, or both, to behave in a particular way in terms of appropriate social conduct or the use and development of particular technical standards to protect privacy.

Professors Edwards and Brown, for example, suggest the possibility of developing voluntary codes of conduct or imposing legislation on OSNs with respect to their default privacy settings.[249] Drawing on the experience of the Directive on Privacy and Electronic Communications in the European Union,[250] Professors Edwards and Brown surmise that legislating mandatory privacy default settings may prove more effective in protecting individual privacy than leaving the market to its own devices.[251] One advantage of such legislated privacy-protecting default settings would be that they would also reinforce social norms relating to adequate privacy protections online.[252] This is a good example of the interplay between legal rules and emerging social norms.

In a similar vein, Professor Froomkin has suggested the enactment of legal rules to encourage the use of privacy enhancing technologies.[253] He has expressed skepticism

---

246 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.")

247 SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 1-2.

248 ZITTRAIN, *supra* note ___, at 211.

249 Edwards and Brown, *supra* note ___.

250 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).

251 Edwards and Brown, *supra* note ___.

252 *id.*

253 Froomkin, *supra* note ___.

about self-regulation, even given the availability of appropriate privacy enhancing technologies.[254] He advocates the interplay of legislation and resulting market forces to more appropriately protect privacy online.[255] He refers predominantly to text-based data aggregation problems in the early days of the Internet, rather than to peer disseminations of digital video images. However, his comments about the necessary interplay between laws and market forces to encourage privacy-enhancing behaviors online are equally applicable in this next context. He also advocates utilizing law to encourage the incorporation of privacy protections into system design.[256] This evidences the need for an interplay between law, market forces, and system architecture as modes of regulation to protect Internet privacy.

Legal rules do not only shape behavior through enforcement – or the threat of enforcement. They are also part of a large and complex matrix of regulatory modalities that shape behavior through a combination of carrots and sticks. In this context, legal rules serve a variety of functions. They can command compliance with certain specific rules in the command and control paradigm. They can also both reflect and shape social norms. Lawmakers will likely be guided by social norms in enacting rules that reflect society's expectations about acceptable conduct. However, laws can also shape social norms, as suggested by Professors Edwards and Brown observing that using law to mandate default technological privacy settings can help to shape emerging social norms about acceptable use of personal material online.[257] Legal rules can also interact with market forces, as observed by Professor Froomkin.[258] Professor Gavison also suggested the development of aspirational legal rules – such as a general explicit legal commitment to privacy protection. This would presumably be a way to help educate society about appropriate behavior with respect to personal information.[259] Thus, the law can play various roles in protecting online privacy generally, as well as specifically in the context of OSNs. The goal for law and policy makers should be to identify the appropriate legal rules to combat privacy problems online, and to ensure that these rules are suitably tailored to the problems they are intended to address. Importantly, legal rules need to interact efficiently and effectively with other regulatory modalities.

D. SOCIAL NORMS AS PRIVACY REGULATOR

Social norms are an extremely important form of regulation.[260] A norm may be defined as: "a rule governing an individual's behavior that is diffusely enforced by third parties other than state agents by means of social sanctions."[261] Norms can, in fact, be

---

254 *id*., at 1527.

255 *id*., at 1528.

256 *id*., at 1529.

257 Edwards and Brown, *supra* note __.

258 Froomkin, *supra* note ___, at 1528.

259 Gavison, *supra* note ___, at 471 (1980).

260 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.")

261 Robert Ellickson, *The Evolution of Social Norms: A Perspective from the Legal Academy*, in MICHAEL HECTHER and KARL-DIETER OPP (eds), SOCIAL NORMS (2001), at 35. See also Lawrence Lessig, *The Architecture of Privacy*, 1 VAND J ENT L & PRAC 56, 62 (1999) ("Norms protect privacy as well. At

more significant than laws,[262] particularly in areas that involve high levels of social interaction, like privacy. As Professor Zimmerman has observed, "As a general rule, legal standards for behavior cannot vary too greatly from accepted community practices without creating a risk that the community will totally disregard the law."[263] Thus, norms should inform the development of legal regulations, particularly where the laws are intended to create standards for behavior.[264]

The problem with cyberspace in this context, is that many norms are not yet well developed, meaning that it can be difficult in cyberspace to identify "accepted community practices". Particularly in relation to OSNs, norm development is in its infancy because of the relative novelty of social networking technology. Add to that the problems of globalization – 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 seems constantly to arise 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.[265] However, they are prepared to bargain with their privacy for a very small price.[266] An online shopping coupon may well entice an individual to disclose voluminous personal details with little regard to future uses of that information.[267]

---

least among individuals, norms limit the kinds of questions one might ask, or the kinds of gossip one might listen to. And among corporations, norms restrict the kind of uses that these companies will make of the data they collect. These constraints 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.")

[262] LESSIG, FREE CULTURE, *supra* note ___, at 122 ("Norms … punish an individual for violating a rule. But the punishment of a norm is imposed by a community, not (or not only) by the state. There may be no law against spitting, but that doesn't mean you won't be punished if you spit on the ground while standing in line at a movie. The punishment might not be harsh, though depending upon the community, it could easily be more harsh than many of the punishments imposed by the state.")

[263] Zimmerman, *supra* note ___, at 335-6.

[264] Although, somewhat counter to this view, Professor Solove suggests that laws can be used to shape norms in the privacy area: SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 74 ("Privacy is not just about what people expect but about what they desire. Privacy is not simply a resource existing in the state of nature that the law must act to conserve. Instead, privacy is something we construct through norms and the law …. The law should … be a tool used proactively to create the amount of privacy we desire."). Professor Zimmerman herself also acknowledges that in some circumstances, laws will shape emerging norms: Zimmerman, *supra* note ___, at 336 ("Certainly, positive law may on occasion inspire dramatic changes in ordinary behaviour and notions of decency. The civil rights amendments to the Constitution, and the statutes that flowed from them, have probably influenced external interactions as well as deeply ingrained psychological attitudes about race.")

[265] 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.").

[266] *id*.

[267] 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

In 1983, Professor Zimmerman observed that the American privacy torts at that time established norms for behavior that deviated substantially from accepted social practices.[268] This problem has likely been exacerbated today with the rise of OSNs and other peer activities online. Indeed, as recently as 2006, Professor McClurg noted that the primary social constraints online are conscience and common sense, and that these attributes are "missing in many people".[269] 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 here, although, even empirical work has its limits with respect to online privacy because individuals tend to undervalue their personal information.[270] There is an argument that empirical work may suffer less from this privacy myopia problem[271] in the OSN context than in the text-based 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.[272] In the OSN context, on the other hand, there is little prospect of individuals bargaining with their personal information for any commercial benefit,[273] so survey results about privacy expectations in this context may be more appropriately aligned with the way people actually behave online.

If it is possible to ascertain any social expectations about online privacy in the OSN context, these could usefully be reduced to Internet guidelines, somewhat akin to the way that "Netiquette" developed in the early days of the Internet. Netiquette might be defined as: "the rules of etiquette that apply when communicating over computer networks, esp. the Internet".[274] In the early days of the Internet, netiquette generally

---

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.")

[268] Zimmerman, *supra* note ___, at 335 ("[T]he [publication of private facts] tort as broadly described by Warren and Brandeis established a norm for behavior that deviates substantially from ordinary practices and that people would be unlikely and (perhaps even unwise) to adopt.")

[269] McClurg, *supra* note ___, at 891.

[270] 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.")

[271] Froomkin, *supra* note ___, at 1502 ("[C]onsumers suffer from privacy myopia: they will sell their data too often and too cheaply.")

[272] SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 96 (citing Professor Fred Cate's observation that even though people generally claim they want more privacy, their actions often belie this representation.)

[273] In other words, unlike the transactional context online, people's expectations on OSNs are generally social, rather than commercial.

[274] See dictionary.com definition of "netiquette", available at http://dictionary.reference.com/browse/netiquette, last viewed on July 18, 2008.

referred to attempts to articulate appropriate social norms with respect to the new email technologies available at the time. In 1995, for example, Intel[275] promulgated a set of guidelines in the form of a generally available memo for the Internet community. This memo was headed "Netiquette Guidelines"[276] and contained suggestions about appropriate use of email services for the then-new generation of Internet users who had not "grown up with the Internet".[277]

The idea was to set down a minimum set of appropriate email behaviors that organizations and individuals could adapt for their own use.[278] The Netiquette Guidelines also recognized the role of Internet Service Providers ("ISPs") and others who may provide access to email services in developing rules and norms for appropriate email use. The introductory section of the Guidelines explains that: "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."[279] This evidences the interplay of norms, laws, and contractual provisions in the development of appropriate online behavior.

There are some parallels between early email netiquette and online behavior involving OSNs today. 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 privacy issues into account. Indeed, as detailed in Part II.B, many OSN service providers do incorporate some privacy provisions into their terms of use. However, as also noted above, there are problems with enforcement of these terms generally, and with the fact that many victims of privacy incursions are not parties to those contracts. Some OSNs already have stated privacy policies that perhaps resemble attempts to articulate new forms of netiquette.[280] These are principles available to the whole world as statements of best practices by an OSN provider in terms of its aspirations to appropriately protect user privacy.[281]

However, terms of use and privacy policies differ from netiquette and pure social norms in the sense that they are generally written from the point of view of an online service provider, rather than the individuals utilizing the service. Thus, they generally focus on explaining 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 social norms, or netiquette, must take account of both. They must explain the appropriate behavior of online service providers

---

275 See www.intel.com, last viewed on July 24, 2008.

276 Intel, Netiquette Guidelines, available at http://www.albury.net.au/new-users/rfc1855.txt, last viewed on July 18, 2008.

277 *id*, clause 1.0 (Introduction).

278 *id.*

279 *id.*

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

281 *id.*

vis-à-vis private individuals, as well as explaining appropriate behavior of individuals amongst themselves.[282]

Some OSNs do attempt to outline a form of netiquette, describing ways in which users of their respective services should respect each other's rights and interests. YouTube and Flickr each have a set of "Community Guidelines" that attempt to describe ways in which users of the respective online communities should treat each other.[283] Flickr's guidelines, for example, are expressed as being part of a user's contract with Flickr along with Flickr's terms of use.[284] They cover issues like ensuring that no inappropriate content is posted, and remembering that children may be looking at information and video files on Flickr. 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".[285] Flickr also includes the simple suggestion: "Don't be creepy."[286] The guidelines do not say anything specifically about protecting others' privacy rights, although they do talk about protecting other people's copyrights.[287] 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 complainant is requested to file a notice of infringement with the "Yahoo! Copyright Team" who will resolve the matter.[288]

Interestingly, the Community Guidelines ask users of the service not to "upload anything that isn't theirs".[289] However, closer inspection of the relevant clause implies that this is again geared towards copyright protection rather than privacy protection. The succeeding definition of "stuff that isn't yours" in this context states that: "This includes

---

[282] 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.")

[283] 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.

[284] Flickr Community Guidelines, *supra* note ___, ("Don't forget that your use of Flickr is subject to these Guidelines and our Terms of Use.")

[285] *id*.

[286] *id*.

[287] *id*.

[288] *id*., ("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.")

[289] *id*.

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 relation to 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, and not the rights of the photographic subject. YouTube's community guidelines similarly protect copyright, but do not specifically mention privacy interests.[290]

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, so there is less perceived need to promulgate a set of community guidelines.[291] In other words, if users are able to limit views of their content to those "friends" authorized to view and 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 the use others may make of their information.[292] Of course, as the preceding discussion has demonstrated, this is only true to a point, but it may explain the difference in style between open and closed networks in terms of the perceived need to articulate community guidelines.

Now in the emerging days of OSNs might be a good time to take stock of video privacy norms, both through empirical studies and through some attempts to expressly articulate norms about privacy in this context. For example, Professors Edwards and Brown have recently noted that there currently appear to be no existing social norms against the "tagging" of photographs to make them more easily searchable.[293] However, this issue could be discussed in a forum to develop online best practices between OSN users and amongst OSN users and OSN providers. Salient issues to consider would be

---

[290] 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.")

[291] 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.")

[292] 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.")

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

whether tagging photographs might somehow impinge on a video subject's expectations of 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?[294] It would be interesting to find out how OSN users feel about this issue. On a more basic level, it would be interesting to try and articulate just what kinds of uses or precautions against re-use are expected by those sharing video images online.[295]

The problem of identifying and articulating appropriate social norms for OSNs should not be underestimated. Professor Grimmelman has recently noted that even in the context of email – one of the more ubiquitous and long term aspects of Internet communication – social norms have their limits.[296] Even for email which has relatively well developed social norms, the ever-changing landscape of the Internet, in terms of increasingly rapid and voluminous connections between ever larger groups of people, causes these norms to falter in certain situations.[297] Thus, social norms are a useful and integral part of Internet communications,[298] and should be articulated and developed as a meaningful part of Internet regulation generally, and OSN regulation in particular. However, norms, like laws, must interact with other modes of regulation to be truly effective in practice.

E. MARKET FORCES AS PRIVACY REGULATOR

Market forces as a regulatory modality 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, conversely, and perhaps paradoxically, the market can dictate social norms through the nature of its products and services. If all market players provide products that only conform with a certain sub-set of possible social behaviors then social behaviors will, by default, have to conform with what is available on the market. However, if the 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

---

294 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.

295 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.")

296 Grimmelman, *supra* note ___, at 7 ("Social norms won't magically save us.")

297 *id*., ("Well-understood norms do – and will – prevent many privacy accidents. But they have never been a complete solution, and the advent of the Internet has rendered them strikingly less effective. More people, more anonymity, fewer non-verbal cues, greater individual autonomy, and the list goes on and on. Today, more so than at any time in history, we can interact with people whose values are not our own, and we can do so under highly fluid and ambiguous conditions. Quasi-private emails leak out *all the time* now, not because we want what is private to become public, but because it has become so hard to tell private from public in the context of email. Social norms will not rebottle this genie.")

298 *id*., at 6 ("Social norms aren't going to go away anytime soon; we can ocunt on them to take care of a lot of the subtle negotiations surrounding the exchange of "private" information.")

conform with their desires and 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.[299]

Over the course of Internet governance debates generally, many commentators have expressed skepticism about the ability, or inclination, of markets to regulate online privacy appropriately.[300] The Internet causes the unprecedented ability of online market players to make financial gains from individuals' personal information with very little legal recourse available for those who are concerned about protecting their privacy. Where the incentives are missing for markets to protect their customers' privacy, there is likely to be little realistic self-regulation absent at least a serious threat of government intervention.[301]

However, in the specific situations under discussion in this article, it is possible that 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.[302] While text-based 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 this way likely outweigh any commensurate benefits of doing so. Additionally, video information may not be linked to a particular person's identity so a targeted marketer would have no guidance as to how to target advertisements to an image subject.[303] The fact that your image is available on my Facebook page does not necessarily give a data aggregator searching that image any personally identifying information that would necessarily enable them to find you for the purposes of aggregating data about you. Of course, the image may be tagged with some of your identifying details, or may be accompanied by text identifying you. However, it would be much more difficult for a data aggregator to profit from this information as it is to deal

---

299 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).

300 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).

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

302 *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.")

303 However, facial recognition technology is becoming more sophisticated and can enable an image subject to be more easily identified than in the past: ZITTRAIN, *supra* note ___, at 214-215.

with text-based information disclosed directly to a company online during an Internet purchase - or even personal information derived from tracking a person's web-surfing habits.

Because of these attributes of online video, it is arguable that the interests of OSN service providers and those of their users in terms of privacy protection are not so disparate as the interests of e-commerce merchants and their consumers. If the OSN service providers obtain more commercial value by protecting their users' privacy than by failing to do so, there may well be market incentives for those service providers to compete with each other in offering stronger forms of privacy protections for their users. Facebook, for example, does offer more detailed privacy protections in relation to video files than some of its competitors as identified in Part II.B. However, the fact that it has strongly worded privacy protections in its terms of use does not necessarily mean that it enforces those terms in practice. Additionally, Facebook is an interesting example in that it markets itself as having strong privacy protections. Nevertheless, it has been strongly criticized for attempts to utilize information derived from its users to market items to their online "friends".[304]

This evidences a distinct practical problem with over-reliance on market forces as a form of online privacy regulation. What an entity says it does, and what it actually does, with respect to its users' privacy may be two different things. An online service 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 in conduct that seems to completely contradict its promises.[305] Of course, in a perfect market, the consumer would simply take her business elsewhere. Yet, in online markets there is often no competitive "elsewhere" to go. If you want to interact socially online, you often have little choice between service providers, as is often the case in the physical world with a variety of products and services. The other problem that may inhere in cyberspace as it does in the physical world is that the terms of service of competing service providers may be so complex and different, and difficult to compare, that in the absence of a requirement of some standardized format to provide consumers with necessary comparative information,[306] consumers will be unable to make meaningful choices.

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 online service providers with respect to privacy policies.[307] Even if a large group of consumers objects to a given privacy policy, there are collective action problems because it is often difficult in practice for consumers to collectively

---

[304] 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).

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

[306] For example, the Annual Percentage Rate ("APR") required to be made available by finance providers so that consumers can more easily and realistically compare their services.

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

express to online service providers their privacy preferences.[308] The drafting of privacy policies in current practice also tends to be fairly toothless in terms of a serious attempt at protecting user privacy. 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.[309] Additionally, privacy policies tend to be regularly updated unilaterally by online service providers, thus putting an unrealistic obligation on users to routinely check back on the policy to keep track of the privacy terms.[310]

Market forces may be a useful and important form of online regulation. However, it seems that market incentives are often insufficient in online contexts to effectively protect users' privacy interests.[311] This may be an area in which it is necessary for legal rules to interact with market forces to create more appropriate outcomes.[312] There are a number of ways in which the law can interact with markets to achieve more socially beneficial outcomes than markets achieve on their own. Obviously, command and control regimes may work here, provided that there is a realistic threat of enforcement of laws requiring appropriate levels of privacy protection by online service providers. A command and control regime may, for example, require market players to maintain and enforce their privacy policies, with threats of legal action for failure to do so.[313]

There may also be more subtle ways in which the law can encourage market players to act in desired ways. As noted in Part III.C.3, Professors Mulligan and Simitian have observed ways in which data breach disclosure laws can provide necessary incentives for markets to engage in best practices when dealing with personally sensitive information.[314] This model draws to some extent from recent approaches to environmental regulation, and can be an effective way to encourage market players to invest adequate time and resources into developing best practices in a given area.[315] Such a model could be extended to encourage online service providers to utilize contractual and technological means to protect their users' privacy.

As noted in Part III.C.6, Professors Edwards and Brown have suggested legislation as a way to require market players to utilize certain default privacy settings to

---

308 *id*.

309 *id*, at 83.

310 *id.*

311 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.")

312 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.")

313 This does not necessarily contradict the earlier point about focusing regulation on peer behavior than on controlling OSNs *per se*. The kind of regulation contemplated here would only require OSNs to keep to their words and enforce their own privacy policies. It does not impose new substantive obligations on them.

314 Mulligan, *supra* note ___, at 10-11.

315 See Hirsch, *supra* note ___.

protect the privacy interests of their users.[316] They also suggest the development of model contracts that could be incorporated into OSNs' terms of use to protect privacy.[317] This could presumably be achieved as a private market-based exercise or through legislation, or a combination of both. In fact, Professor Solove has additionally suggested that laws could be utilized much better than they currently are to ensure meaningful enforcement of privacy contracts.[318] He notes that, in the past, enforcement of privacy contracts has been problematic because courts have generally required proof of monetary damages.[319] Laws could alter this paradigm to allow compensation for other types of harms resulting from infringements of privacy contracts.

As with legal regulation and social norms, market solutions are not, and are never likely to be, a perfect form of online privacy regulation on their own. Nevertheless, in concert with the other modes of regulation, they will be an important factor in the developing online privacy protection matrix. Without buy-in from online service providers, whether it be obtained through carrots or sticks, or through a combination of both, there is little hope of meaningfully protecting privacy online. While social norms between individuals should develop to protect privacy rights online, the cooperation of service providers will be necessary to effectively enforce privacy expectations in the future.

F. SYSTEM ARCHITECTURE AS PRIVACY REGULATOR

While commentators have generally expressed skepticism about market forces *per se* as privacy regulators, they have been more optimistic about the potential to utilize system architecture to better protect online privacy. Professor Lessig has defined system architecture in the privacy context as: "technologies for re-creating privacy where other technologies may have erased it."[320] Many commentators have acknowledged the profound impact that system architecture potentially has on personal privacy online.[321] One obvious advantage of architecture as a regulatory modality for privacy is that it is more proactive than other forms of regulation, notably legal regulation.[322] Architecture

---

316 Edwards and Brown, *supra* note ___, at ___. However, some commentators would disagree with this approach: SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 201 ("The law should not force companies to set specific defaults, but the companies should be encouraged to think about how the design of their websites affects privacy.")

317 Edwards and Brown, *supra* note ___, at [page 10-27 of draft].

318 SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 179 (noting that courts currently will often acknowledge a privacy problem but will fail effectively to redress harms caused by the problem).

319 *id*, at 183.

320 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.

321 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).

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

creates structures upfront that are intended to prevent harm, while laws generally provide remedies when harms occur.[323]

However, again the problem with reliance on architecture as a privacy regulator is that it does not necessarily work well on its own. Privacy-enhancing technologies can be expensive and there is often little to no market incentive for online service providers to invest in it. Already ubiquitous privacy enhancing technologies in the hands of consumers that are included in much available software can be problematic in that many consumers do not have the technological know-how to use them effectively (or at all). The solution may be to "change the default settings" in a number of ways: that is, to sell software with the privacy-protecting default settings turned on at their highest level, and to require online service providers to invest in technologies to protect their users' privacy. However, this may require legal intervention to achieve the desired results. Professors Edwards and Brown suggest that laws may be needed that require OSN providers to change their default positions on privacy.[324]

One issue for OSNs will be to identify available system architectures to protect user privacy. An obvious example is the closed network format utilized by Facebook and MySpace. These services use available technology to limit users to accessing information of other users that they are authorized to access. On Facebook, for example, 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.[325] Given the easy availability of these options, one might ask why Internet users posting video images continually flock to open services like YouTube. This may be evidence of social norms and market forces at play. Customers who are less concerned about privacy may arguably be using open networks and those who are more concerned about privacy are flocking to Facebook.[326] YouTube is also geared towards audio-visual, multimedia content, whereas Facebook caters to a variety of different kinds of content. That is also a function of the respective services' market segment.

---

[323] *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."")

[324] Edwards and Brown, *supra* note ___, at ___.

[325] 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.")

[326] Indeed, in the context of online privacy policies, market self-regulation proponents would argue that consumer behavior in these contexts does evidence social norms with respect to privacy. In situations where consumers ignore privacy interests in a privacy policy when making decisions about which services to use, the argument goes that these consumers are not particularly interested in privacy: See Solove, THE DIGITAL PERSON, *supra* note ___, at 82.

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.[327] Of course, this does not deal with the problems of unauthorized dissemination of relevant images prior to the expiration of the original posted image, or the permanence of any copies made available on other websites. Especially if images have been tagged, they may still be easy to find on multiple websites even after the original image has been removed from an online profile. However, automatic expiration settings would, to some extent, limit the availability of personal information online. Additionally, 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 to some extent.

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. For example, code could be written that would prohibit cutting and pasting initially, while at the same time sending a request to the image holder and image subject to request permission to the dissemination of the image. The holder and subject could then respond, and that response would translate into a permission or non-permission to the requester to copy the image. If a response was not received from either the image holder or the image subject, the default setting would presumably be to refuse permission to copy the image. Alternatively, or additionally, the image could simply be tagged with permissions when originally uploaded.[328] This would not prevent unauthorized disseminations of images *per se*, but it would be a use of technology that could bring the privacy preferences of the image subject into public view. Thus, this approach may assist in online norm development with respect to the protection of others' privacy. 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.[329] However, this technological solution is somewhat limited in that the relevant tags are lost once an image is copied outside the Facebook network.[330]

This discussion has not been a comprehensive survey of possible technological solutions to video privacy problems. It is merely intended to establish that there are technological options that have not yet been seriously investigated that could better protect online video privacy than is currently the case in practice. Many of the technologies that would enable enhanced privacy protection for video images are in

---

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

[328] 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.")

[329] 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.")

[330] *id.*

existence today and have yet to be applied in this context.[331] 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 it worth their while to employ these technologies;[332] (b) lack of awareness of these technologies by users; (c) lack of financial incentives for online service providers to develop and deploy these technologies;[333] and, (d) lack of clarity about current and emerging social norms in relation to online privacy, particularly in the video and multi-media context.

Some of the more obvious advantages to developing technological solutions to emerging privacy problems are their effectiveness[334] and their global reach.[335] As noted by Professors Edwards and Brown, if OSNs such as Facebook wanted to better protect privacy on a global scale, it would be a simple matter for them to create privacy defaults as a matter of system architecture that would operate in all countries where Facebook was accessible to users.[336] These professors further note that such a system could be facilitated by a matrix of statutes that legislate for more privacy-friendly default settings, thus utilizing law to encourage the development of technological solutions.[337] Again, we see the likely need for technological solutions to interact with laws and other modes of regulation in order to be truly effective in practice.

G. OTHER MODES OF REGULATION

1. Education as Privacy Regulator

As Professor Lessig suggested in the early days of the Internet, to understand online regulation – or any regulation for that matter - it is necessary to understand the interplay of at least four regulatory modalities – legal rules, social norms, market forces, and system architecture.[338] However, this may not be the end of the story. In recent years, commentators have suggested new modes of regulation that may be equally important online, particularly with respect to protecting individual privacy interests. This is not inconsistent with Professor Lessig's work. He did not claim that the four

---

331 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 LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY, 147-153 (2004).

332 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.")

333 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 …").

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

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

336 *id.*

337 *id*., at [page 10-29 of current draft].

338 Lessig, *The Law of the Horse, supra* note ___, at 507-510; Lessig, *The Architecture of Privacy*, *supra* note ___, at 62-63; LESSIG, FREE CULTURE, *supra* note ___, at 121-124.

regulatory modalities that he identified were intended to be comprehensive.[339] Other forms of regulatory constraint are possible. Professors Edwards and Brown, for example, have suggested the importance of public education as a mode of regulation for privacy interests in the OSN context.[340] Professor Solove has similarly indicated the importance of public education as at least a partial answer to online privacy problems.[341]

Of course, one may define public education as merely being a subset of social norms in the sense that education of the public will ultimately help to identify social norms as it will focus the attention of the public on a particular issue in a way likely to shape public attitudes about the issue. However, for present purposes, it may be useful to regard public education as a separate subset of information regulation. This separate focus allows us to identify the kinds of education that may become important in the privacy context. We should also consider who has responsibility to educate the public, and how prescriptive or otherwise such education may be. If, for example, social norms really are yet to develop in many online privacy contexts, then the education side of the regulatory equation, at least at this point in time, should perhaps be aimed at eliciting views from the public rather than instructing the public about privacy. On the other hand, the public should certainly be instructed about available privacy-enhancing technologies so they might put more pressure on online service providers to employ those technologies or make them more widely available. Additionally, where such technologies are already available but the public has little information about how to use them, public education is an important form of regulation to address this disconnect.

Professor Froomkin has suggested, at least in the context of unauthorized data aggregation, that public education may become a regulatory modality for privacy along with other avenues such as technological responses and legal solutions.[342] It is probably safe to say that public education is 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.

2. Institutions as Privacy Regulators

Another possible mode of regulating privacy has recently been suggested by Professor Richards. In the context of conceptualizing a new theory of "intellectual

---

339 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…").

340 Edwards and Brown, *supra* note ___, at [page 10-27 of current draft].

341 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.")

342 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.")

privacy", he has identified institutions as potential forms of privacy regulators.[343] In this context, he utilizes the example of libraries, and in particular, the American Library Association ("ALA") in promoting free speech values and intellectual liberty against the threat of government surveillance.[344] He discusses the ALA's 1939 library bill of rights which declared aspirations of intellectual freedom and privacy of library patrons.[345] 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.

In fact, even Professor Lessig has recognized the work of non-profit institutions as a potential regulatory modality in the digital copyright context. In the Afterword of his text, *Free Culture*, he cites the examples of the Public Library of Science ("PLoS")[346] and the Creative Commons[347] as non-profit organizations whose work aims to better balance the rights of the public to utilize copyright works against the commercial interests of content holders. The PLoS is a nonprofit organization that maintains a repository of scientific work in electronic form that is made permanently available for free.[348] The Creative Commons is a nonprofit corporation that aims to facilitate copyright holders in granting more flexible permissions for uses of their works.[349] 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"."[350]

The question for video privacy in the OSN context, and online privacy generally, is whether there are currently any institutions that could fulfill an institutional regulatory function, such as the function performed by the ALA in protecting library patrons' intellectual privacy. Because most of the players in the OSN privacy matrix are commercial enterprises and private Internet users, it is perhaps difficult to identify an analog to the ALA in the library context. The closest obvious contenders are probably some public interest organizations that aim to protect rights and freedoms generally online. Examples are the Electronic Frontier Foundation ("EFF"),[351] and the Electronic Privacy Information Center ("EPIC").[352]

---

343 Richdards, *Intellectual Privacy, supra* note___, at 33.

344 *id*., at 33-34.

345 *id*., at 32-33.

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

347 *id*, at 282-286.

348 *id*., at 281-282.

349 *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.")

350 See www.creativecommons.org, last viewed on July 30, 2008.

351 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).

352 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

These organizations tend not to be particularly well funded,[353] 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 privacy 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 in the future 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 in concert with public education in protecting online privacy. These organizations already perform a public education role in the sense of the media coverage they obtain for their activities,[354] and the public lectures their officers provide on online liberties.[355] Their websites also contain much educational information about individual rights online. It may be that greater focus on public education as a modality of regulation for online privacy could cast more light on the activities of organizations that are already attempting to publicize issues relating to individual freedoms online.

Academic institutions are another example of largely non-profit institutions that can play an important public education role.[356] 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 in terms of academic conferences and symposia on these issues.[357] However, a greater array of publications, and greater accessibility of conferences and conference proceedings, including free online availability,[358] could be a useful aspect of the ongoing privacy regulation matrix. Clearly public education and institutions as regulatory modalities have a lot of synergies between them, and could be more usefully employed in the future development of online privacy principles, alongside legal rules, social norms, market forces, and system architecture.

IV. CONCLUSIONS

Privacy rights online have been of growing concern in the past decade or so as privacy destroying technologies increase in prevalence.[359] As noted by Professor Solove, much of the destruction of privacy online is incidental to other activities being relatively

---

to protect privacy, the First Amendment, and constitutional values." (see www.epic.org, last viewed on July 23, 2008).

353 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.

354 For example, the EFF maintains a publicly accessible register of recent media coverage of its activities on its homepage: See "EFF in the News", available at www.eff.org, last viewed on August 10, 2008.

355 For example, the EFF maintains a publicly accessible online calendar of events at which its officers are speaking: http://www.eff.org/event, last viewed on August 10, 2008.

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

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

358 For example through podcasting.

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

innocently, if somewhat carelessly, conducted by online actors.[360] The rise of OSNs is yet another area in which those interacting relatively innocently online are creating potentially long term threats to individual privacy. A number of regulatory avenues have already been identified to better protect digital privacy problems. They include legal rules, social norms, market forces, system architecture, public education, and an enhanced role of institutions as regulators. The problem is the pace of change and development of technologies for gathering and sharing both text-based and video/multi-media information. By the time the regulatory modalities have been effectively deployed to counteract new technological privacy problems, much personal information, including potentially damaging or embarrassing information in video formats, will already be widely displayed online. It is now time to start thinking more carefully about the potential of each regulatory modality, and the most efficient way for the regulatory modalities to interact with each other to protect online privacy interests.

This Article has examined a number of advantages and disadvantages of six distinct, yet interrelated, regulatory modalities. It has considered ways in which these modalities could be employed to better protect privacy interests in digital images, noting that digital images raise privacy concerns that are often distinct from those that arise in relation to the gathering and dissemination of text-based data about individuals. One of the most salient problems with digital video images is that the image subject is usually a different person to the person who originally captured the image and posted it online. The image taker may well be protected by copyright law, but this will be of no avail to the image subject seeking to protect her online privacy.

One might argue that there is no need to focus on digital privacy, or more particularly digital video privacy, in the short term. Commentators have suggested in the past that privacy is not a highly held value in cyberspace so there is no need to protect it.[361] 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.[362] However, these views are not universally accepted. There are explanations for Internet users' apparent lack of concern for privacy, including: (a) their lack of education about potential privacy breaches and impacts of those breaches on their lives, (b) the lack of forethought that young people often put into their actions while they are developing their lives and personalities and using OSNs to do so; and, (c) the lack of meaningful modes of protecting online privacy for those who want to take advantage of online services such as OSNs.

---

360 SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 53.

361 *id*, at 82 ("Self-regulatory proponents would [argue] that [the fact that consumers rarely choose companies based on their privacy policy] indicates that privacy isn't very important to most people. If people really cared about privacy, the self-regulators argue, then they would refuse to deal with companies offering inadequate levels of privacy."); 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?").

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

There is also a body of literature arguing that an attempt to regulate privacy online today is like locking the barn door after the horse has bolted.[363] Some commentators have suggested that the appropriate approach to remedying privacy breaches in the 21st century is to focus on specific damages caused by leaks of personal information, including discrimination in the workplace, healthcare, and education.[364] Indeed, some have suggested that the benefits of profiling and lack of privacy could theoretically outweigh the costs in the long term.[365] In particular, Professor Strahilevitz has argued that the wide-scale dissemination of personal information can actually help the public understand existing social norms.[366]

However, there is reason to be skeptical of an approach that focuses not on protecting privacy, but solely on specific harms caused by resultant leaks of information. For one thing, many insecurities involving personal information do not result in specific harms in terms of possible racial profiling in health care, education, and employment, or even identity theft.[367] In fact, many online privacy incursions do not result in any one specific harm, but rather in a general culture of unease where individuals cannot rely on anyone taking care or control over sensitive information about them.[368]

Another objection to attempting to develop Internet privacy regulation arises from the global nature of the Internet. Cyberspace has historically raised jurisdictional concerns – and the idea has been voiced that the Internet cannot[369] and arguably should not be regulated because it would be tantamount to an attempt to impose one country's

---

[363] 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).

[364] 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).

[365] Froomkin, *supra* note ___, at 77 ("And perhaps it really is better to be watched, and the benefits of mass surveillance and profiling outweigh the costs."); 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).

[366] 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.")

[367] For a detailed discussion of problems of treating even identity theft as a specific harm, see SOLOVE, THE DIGITAL PERSON, *supra* note ___, at 115-119.

[368] *id*, at 53 ("A person's lack of control is exacerbated by the often thoughtless and irresponsible ways that bureaucracies use personal information and their lack of accountability in using and protecting the data. In other words, the problem is not simply a lack of individual control over information, but a situation where *nobody* is exercising meaningful control over the information."); 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.")

[369] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, available at http://homes.eff.org/~barlow/Declaration-Final.html, last viewed on July 25, 2008 ("Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.")

laws on the rest of the world.[370] There are at least two answers to this argument. The first is that history has shown that the Internet can be regulated and indeed has been effectively regulated in a number of areas – notably the protection of intellectual property rights online.[371] The second is that difficulties inherent in Internet regulation depend to a large extent on the subject matter of the regulation. In areas where cross-cultural views of particular problems can be aligned fairly easily on a substantive level, international regulation is not so difficult.

Some domestic examples in a federal system can illustrate this point easily enough. In the United States, legislatures at both the state and federal level have had much more trouble enacting legislation to protect minors from indecent and harmful online content[372] than they have had in enacting legislation to curtail unsolicited commercial emails (or "spam").[373] One of the reasons why this has been the case is that there is less substantive disagreement between social groups about the contours of appropriate regulatory responses to spam[374] than there is on defining content harmful to minors.[375]

One of the leading privacy experts, Professor Solove, has suggested that despite disharmonization in terms of values and terminology ascribed to privacy protection in

---

370 See, for example, *Dow Jones & Co v Gutnick*, [2002] HCA 56 (10 Dec 2002), ¶ 200 per Justice Callinan ("[W]hat the appellant seeks to do is to impose upon Australian residents for the purposes of this and many other cases, an American legal hegemony in relation to Internet publications. The consequence, if the appellant's submission were to be accepted would be to confer upon one country, and one notably more benevolent to the commercial and other media than this one, an effective domain over the law of defamation, to the financial advantage of publishers in the United States, and the serious disadvantage of those unfortunate enough to be reputationally damaged outside the United States.") (available at http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html, last viewed on July 25, 2008).

371 SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 184 ("Control in the privacy context is seen as outlandish or impossible. Copyright law demonstrates otherwise. It reveals that the law is willing and able to control information.")

372 See, for example, *American Libraries Association v Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997) (striking down state law that made it illegal to distribute material harmful to minors over the Internet); *Reno v American Civil Liberties Union*, 521 U.S. 844 (1997) (striking down sections of federal Communications Decency Act of 1996 that attempted to limit the distribution of inappropriate content over the Internet); *Ashcroft v American Civil Liberties Union*, 542 U.S. 656 (2004) (striking down sections of federal Child Online Protection Act that attempted to protect minors from inappropriate Internet content). However, contrast these cases with *United States v American Library Association, Inc*, 539 U.S. 194 (2003) (in which the Children's Internet Protection Act was upheld with respect to conditioning government funding for libraries on their willingness to utilize filtering software to protect minors from inappropriate material online).

373 *State of Washington v Heckel*, 122 Wn. App. 60; 93 P. 3d 189 (2004) (upholding state legislation restricting certain aspects of unsolicited commercial email).

374 See, for example, *State of Washington v Heckel*, 143 Wn.2d 824, 837-838; 24 P.3d 404,411-412; (2001); *aff'd* 122 Wn. App. 60; 93 P. 3d 189 (2004) (noting that different state laws regulating unsolicited commercial email were drafted in substantially the same terms, so that it was not imposing an undue burden on a defendant to require him to comply with a given state's laws for the purposes of the Dorment Commerce Clause analysis).

375 See, for example, *Ashcroft v American Civil Liberties Union*, 535 U.S. 564, 577 (2002) (describing a law's attempts to regulate online speech with relation to "community standards" as being problematic because community standards are widely divergent in different geographic areas even within the United States).

different countries, there is "a significant degree of consensus about the kinds of problems involved."[376] If this is indeed the case, globalization arguably does not pose a significant problem to privacy regulation. Laws and social norms identified in one country are unlikely to be strikingly dissimilar to those in other countries. Additionally, as pointed out by Professors Edwards and Brown, technological solutions to privacy problems can easily have a global reach.[377] Thus, if there is relative consensus on aims of privacy regulation amongst cultures, this enables laws and norms to develop that effectively have a global reach and that can easily enough be bolstered by globally applicable technological solutions to privacy problems. Regulators could also achieve global economies of scale in public education initiatives if the concerns of the public in different countries are largely the same in substance.

Many commentators have indicated that a multi-pronged regulatory approach is necessary with respect to cyberspace generally.[378] Others have applied this view to privacy protections more specifically.[379] This work has been extremely important and useful and must continue to be extended to deal with new privacy issues as they arise online. One of the newer issues is the relative lack of privacy protection for video images and other multi-media files shared over OSNs. The above discussion has utilized this example to demonstrate how a multi-pronged regulatory approach can address these social concerns in ways that fill in gaps in the current legal matrix for privacy protection. Exercises like this will continue to be necessary in the future as new technologies arise that enable new types of privacy incursions. This article has demonstrated the need to think in terms of often intricate and detailed interactions of various regulatory approaches in order to achieve more appropriate balances of privacy rights and other interests in cyberspace. It will hopefully serve as a useful model for future discourse on online privacy protections more generally.

---

376 SOLOVE, UNDERSTANDING PRIVACY, *supra* note ___, at 183-184.

377 Edwards and Brown, *supra* note ___, at ___.

378 Lessig, *The Law of the Horse*, *supra* note ___, at 507-510; Reidenberg, *Lex Informatica*, *supra* note ___.

379 Lessig, *The Architecture of Privacy*, *supra* note ___, at 62-63; Froomkin, *supra* note ___, at 1466; SOLOVE, THE FUTURE OF REPUTATION, *supra* note ___, at 189-204.