

## Privacy 2.0

Jonathan Zittrain

Jonathan.Zittrain@chicagounbound.edu

Follow this and additional works at: <http://chicagounbound.uchicago.edu/uclf>

---

### Recommended Citation

Zittrain, Jonathan ( ) "Privacy 2.0," *University of Chicago Legal Forum*: Vol. 2008: Iss. 1, Article 3.

Available at: <http://chicagounbound.uchicago.edu/uclf/vol2008/iss1/3>

This Article is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in University of Chicago Legal Forum by an authorized administrator of Chicago Unbound. For more information, please contact [unbound@law.uchicago.edu](mailto:unbound@law.uchicago.edu).

# Privacy 2.0<sup>†</sup>

*Jonathan Zittrain<sup>‡</sup>*

The internet is generative: it allows contribution from all corners, without special accreditation or relationships to government or corporate gatekeepers.<sup>1</sup> This simple feature has allowed a blossoming of uses and abuses. Privacy problems showcase issues that can worry individuals who are not concerned about other problems resulting from the internet's generativity like copyright infringement, and demonstrate how generativity puts old problems into very new and perhaps unexpected configurations, calling for creative solutions.

The heart of the next generation privacy problem arises from the similar but uncoordinated actions of individuals that can be combined in new ways thanks to the generative Net. Indeed, the Net puts private individuals in a position to do more to compromise privacy than the government and commercial institutions traditionally targeted for scrutiny and regulation. The standard approaches that have been developed to analyze the earlier privacy threats do not work well for this new breed of the problem, but solutions applied to generative problems arising at other layers of the network can be adapted to help.

---

<sup>†</sup> Copyright © 2008 Jonathan Zittrain. This article is drawn from Chapter 9 of Jonathan Zittrain, *The Future of the Internet—And How to Stop It* (Yale and Penguin UK 2008).

<sup>‡</sup> Professor of Law, Harvard Law School. I thank Blair Kaminsky for excellent research assistance. <http://www.jz.org>.

<sup>1</sup> See Jonathan L. Zittrain, *The Generative Internet*, 119 Harv L Rev 1974, 1980 (2006) ("Generativity denotes a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences."). The internet's generative character facilitates collaborative endeavors in which people, usually in separate places, can build on past achievements to create unanticipated innovations. For example, generativity facilitated the development of the wiki, as well as its use for the encyclopedia that is Wikipedia. Wikipedia's content is in turn generatively developed, a form of recursive generativity. For a general overview, see Jonathan Zittrain, *The Future of the Internet—And How to Stop It* 67–100 (Yale and Penguin UK 2008). Five factors determine a system's generativity: "(1) how extensively a system or technology leverages a set of possible tasks; (2) how well it can be adapted to a range of tasks; (3) how easily new contributors can master it; (4) how accessible it is to those ready and able to build on it; and (5) how transferable any changes are to others—including (and perhaps especially) nonexperts." Id at 71.

## I. PRIVACY 1.0

In 1973, a blue-ribbon panel reported to the U.S. Secretary of Health, Education, and Welfare ("H.E.W.") on computers and privacy. The report could have been written today:

It is no wonder that people have come to distrust computer-based record-keeping operations. Even in non-governmental settings, an individual's control over the personal information that he gives to an organization, or that an organization obtains about him, is lessening as the relationship between the giver and receiver of personal data grows more attenuated, impersonal, and diffused. There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers-unknown, unseen and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others.<sup>2</sup>

The report pinpointed troubles arising not simply from powerful computing technology that could be used both for good and ill, but also from its impersonal quality: the sterile computer processed one's warm, three-dimensional life into data handled and maintained by faraway faceless institutions, viewed at will by strangers. The worries of that era are anything but obsolete. We are still concerned about databases with too much information that are too readily accessed; databases with inaccurate information; and having the data from databases built for reasonable purposes diverted to less noble, if not outright immoral, uses.<sup>3</sup>

Government databases remain of particular concern because of the unique strength and power of the state to amass informa-

---

<sup>2</sup> Advisory Committee to the Secretary of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens*, § II (1973), available at <<http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>> (last visited Feb 21, 2008).

<sup>3</sup> Consider Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan L Rev 1393 (2001) (examining the dangers to personal privacy posed by electronic databases).

tion and use it for life-altering purposes. The day-to-day workings of the government rely on numerous databases, including those used for the calculation and provision of government benefits, decisions about law enforcement, and inclusion in various licensing regimes.<sup>4</sup> Private institutional databases also continue to raise privacy issues, particularly in the realms of consumer credit reporting, health records, and financial data.

Over three decades ago, the H.E.W. report raised strikingly similar concerns. Due to political momentum generated by the H.E.W. report and the growing controversy over President Richard Nixon's use of government power to investigate political enemies, the U.S. Congress enacted comprehensive privacy legislation shortly after the report's release. The Privacy Act of 1974 mandated a set of fair information practices, including disclosure of private information only with an individual's consent (with exceptions for law enforcement, archiving, and routine uses), and established the right of the subject to know what was recorded about her and to offer corrections. While it was originally intended to apply to a broad range of public and private databases to parallel the recommendations of the H.E.W. report, the Act was amended before passage to apply only to government agencies' records.<sup>5</sup> Congress never enacted a comparable comprehensive regulatory scheme for private databases. Instead, private databases are regulated only in narrow areas of sensitivity such as credit reports (addressed by a complex scheme passed in 1970 affecting the handful of credit reporting agencies)<sup>6</sup> and video rental data,<sup>7</sup> which has been protected since Supreme Court nominee Robert Bork's video rental history was leaked to a newspaper during his confirmation process in 1987.<sup>8</sup>

---

<sup>4</sup> For a general discussion, see *id.*

<sup>5</sup> US Congress Sen Comm on Govt Operations and US H Govt Operations Subcomm on Govt Info & Individual Rights, *Legislative History of the Privacy Act of 1974*, at 9–28, 97–150, available at <[http://www.loc.gov/rr/frd/Military\\_Law/pdf/LH\\_privacy\\_act-1974.pdf](http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf)> (last visited Feb 21, 2008) (reporting that Senate Bill 3418 initially covered all organizations that collected personal information, but the Senate Committee on Government Operations limited the bill's scope to the federal government).

<sup>6</sup> See Fair Credit Reporting Act § 602, 15 USC § 1681 (2006) (requiring “consumer reporting agencies [to] adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer”).

<sup>7</sup> See 18 USC § 2710 (2000) (“A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person . . .”).

<sup>8</sup> Electronic Privacy Info Center, *The Video Privacy Protection Act* (“VPPA”), available at <<http://www.epic.org/privacy/vppa/>> (last visited Feb 21, 2008).

The H.E.W. report expresses a basic template for dealing with the informational privacy problem: first, a sensitivity is identified regarding some stage of the information production process—the gathering, storage, or dissemination of one's private information—and then a legal regime is proposed to restrict these activities to legitimate ends. This template has informed analysis for the past thirty years, guiding battles over privacy both between individuals and government and between individuals and "large and faceless" corporations. Of course, a functional theory does not necessarily translate into successful practice. Pressures to gather and use personal data in commerce and law enforcement have increased, and technological tools to facilitate such data processing have matured without correspondingly aggressive privacy protections.<sup>9</sup> In 1999, Scott McNealy, CEO of Sun Microsystems, was asked whether a new Sun technology to link consumer devices had any built-in privacy protection. "You have zero privacy anyway," he replied. "Get over it."<sup>10</sup>

McNealy's words raised some ire at the time; one privacy advocate called them "tantamount to a declaration of war."<sup>11</sup> McNealy has since indicated that he believes his answer was misunderstood.<sup>12</sup> But the plain meaning of "getting over it" seems to have been heeded: while poll after poll indicates that the public is concerned about privacy,<sup>13</sup> the public's actions frequently belie these claims. Apart from momentary spikes in privacy concern that typically follow high-profile scandals—such as Water-

---

<sup>9</sup> See Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* 1–36 (O'Reilly 2000).

<sup>10</sup> Polly Sprenger, *Sun on Privacy: 'Get Over It'*, *Wired* (Jan 26, 1999), available at <<http://www.wired.com/news/politics/0,1283,17538,00.html>> (last visited Feb 21, 2008).

<sup>11</sup> *Id.*

<sup>12</sup> Email from Jim Waldo, Engineer, Sun Microsystems (Apr 18, 2007) (on file with author) (recounting a conversation with McNealy in which McNealy seemed to indicate that "the statement that you have no privacy is not so much about your privacy being taken away by technology, but about your lack of privacy in the non-technology world").

<sup>13</sup> ASNE Freedom of Info Comm and First Amendment Center, *Freedom of Information in the Digital Age* 10–12, 15 (2001), available at <<http://www.freedomforum.org/publications/first/foi/foiinthedigitalage.pdf>> (last visited Feb 21, 2008) (finding that 89 percent of adults surveyed were concerned, or very concerned, about personal privacy, and that nearly identical percentages reported that they were concerned about crime, access to quality health care, and the future of the social security system); Humphrey Taylor, *Most People Are "Privacy Pragmatists" Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits* (Harris Interactive Mar 19, 2003), available at <[http://www.harrisinteractive.com/harris\\_poll/index.asp?PID=365](http://www.harrisinteractive.com/harris_poll/index.asp?PID=365)> (last visited Feb 21, 2008) (discussing Harris Poll #17, which found that 69 percent of adults believe consumers have "lost all control of how personal information is collected and used by companies" and that 53 percent disagreed with the statement that "existing laws and organizational practices provide a reasonable level of protection for consumer privacy policy").

gate or the disclosure of Judge Bork's video rentals—we routinely part with personal information and at least passively consent to its use, whether by surfing the internet, entering sweepstakes, or using a supermarket discount card.

Current scholarly work on privacy tries to reconcile people's nonchalant behavior with their seemingly heartfelt concerns about privacy.<sup>14</sup> It sometimes calls for industry self-regulation rather than direct governmental regulation as a way to vindicate privacy interests, perhaps because such regulation is seen as more efficient or just, or because direct governmental intervention is understood to be politically difficult to achieve. Privacy scholarship also looks to the latest advances in specific technologies that could further weaken day-to-day informational privacy.<sup>15</sup> One example is the increasing use of radio frequency identifiers ("RFIDs") in consumer items, allowing goods to be scanned and tracked at a short distance. One promise of RFID is that a shopper could wheel her shopping cart under an arch at a grocery store and obtain an immediate tally of its contents; one peril is that a stranger could drive by a house with an RFID scanner and instantly inventory its contents, from diapers to bacon to flat-screen TVs, immediately discerning the sort of people who live within.

This work on privacy generally hews to the original analytic template of 1973: both the analysis and suggested solutions speak in terms of institutions gathering data, and of developing ways to pressure institutions to better respect their customers' and clients' privacy. This approach is evident in discussions about electronic commerce on the internet. Privacy advocates and scholars have sought ways to ensure that websites disclose to people what they are learning about consumers as they browse and buy. The notion of "privacy policies" has arisen from this debate. Through a combination of regulatory suasion and industry best practices, such policies are now found on many websites, comprising little-read boilerplate answering questions about

---

<sup>14</sup> See, for example, Vera Bergelson, *It's Personal But Is It Mine?: Toward Property Rights in Personal Information*, 37 UC Davis L Rev 379 (2003); Solove, 53 Stan L Rev at 1393 (cited in note 3).

<sup>15</sup> Jerry Kang and Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 Wash & Lee L Rev 93 (2005) (discussing privacy concerns that emerge as mobile, wireless devices expand internet connectivity); Jeffrey Rosen, *A Watchful State*, NY Times A1 (Oct 7, 2001) (examining the possible effects of biometric identification technology on personal privacy); Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L J 1227 (2003) (considering identity theft and privacy in the context of public identification systems and information-storage architectures).

what information a website gathers about a user and what it does with the information.<sup>16</sup> Frequently the answers are, respectively, “as much as it can” and “whatever it wants,”—but, to some, this is progress. A privacy policy allows scholars and companies alike to advance a useful fiction that the user has been put on notice of privacy practices.

Personal information security is another area of inquiry, and there have been some valuable policy innovations in this sphere. For example, a 2003 California law requires firms that unintentionally expose their customers’ private data to others to alert the customers to the security breach.<sup>17</sup> This has led to a rash of well-known banks sending bashful letters to millions of their customers, gently telling them that, say, a package containing tapes with their credit card and social security numbers has been lost en route from one processing center to another.<sup>18</sup> Bank of America lost such a backup tape with 1.2 million customer records in 2005.<sup>19</sup> That same year, a MasterCard International security breach exposed information of more than forty million credit card holders.<sup>20</sup> Boston College lost 120,000 alumni records

---

<sup>16</sup> For example, Amazon’s privacy policy describes various situations in which Amazon shares customer information with others. For instance, the policy notes that Amazon may provide customer information to third party service providers like delivery companies and marketing companies. The policy also (vaguely) states that Amazon may release information when necessary for the “[p]rotection of Amazon.com and others.” See *Amazon.com Privacy Notice*, available at <<http://www.amazon.com/gp/help/customer/display.html?nodeId=468496#share>> (last visited Feb 21, 2008).

<sup>17</sup> Cal Civil Code § 1798.82 (West 2003) (“Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”). California legislators are currently considering a variety of different proposals to amend or repeal portions of this statute.

<sup>18</sup> StrongAuth, Inc. maintains a compendium of such disclosures, including those by MasterCard International, Polo/Ralph Lauren, Bank of America, and several universities. See StrongAuth, Inc. Newsletter, *Washington’s SSB 66043 – On the Heel of CA’s SB 1386*, (May 5, 2005), available at <[http://www.strongauth.com/index.php?option=com\\_content&task=view&id=36&Itemid=42](http://www.strongauth.com/index.php?option=com_content&task=view&id=36&Itemid=42)> (last visited Feb 21, 2008).

<sup>19</sup> Robert Lemos, *Bank of America Loses a Million Customer Records*, (CNET News.com Feb 25, 2005), available at <[http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029\\_3-5590989.html?tag=st.rc.targ\\_mb](http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html?tag=st.rc.targ_mb)> (last visited Feb 21, 2008). This type of data loss is not uncommon. As one study noted, “60% of [compromised record] incidents involved organizational mismanagement: personally identifiable information accidentally placed online, missing equipment, lost backup tapes, or other administrative errors.” Kris Erickson and Philip N. Howard, *A Case of Mistaken Identity? News Accounts of Hacker and Organizational Responsibility for Compromised Digital Records*, 12 J Computer-Mediated Commun (2007), available at <<http://jcmc.indiana.edu/vol12/issue4/erickson.html>> (last visited Feb 21, 2008).

<sup>20</sup> Joris Evers, *Credit Card Breach Exposes 40 Million Accounts*, CNET News.com

to hackers as a result of a breach.<sup>21</sup> The number of incidents shows little sign of decreasing,<sup>22</sup> despite the incentives provided by the embarrassment of disclosure and the existence of obvious ways to improve security practices. For minimal cost, firms could minimize some types of privacy risk to consumers—for example, by encrypting their backup tapes before shipping them anywhere, making them worthless to anyone without a closely held digital key.

Addressing website privacy and security has led to elaborations on the traditional informational privacy framework. Some particularly fascinating issues in this framework are still unfolding: is it fair, for example, for an online retailer like Amazon.com to record the average number of nanoseconds each user spends contemplating an item before clicking to buy it? Such data could be used by Amazon.com to charge impulse buyers more, capitalizing on the likelihood that this group of consumers does not pause long enough to absorb the listed price of the item they just bought. A brief experiment by Amazon in differential pricing resulted in bad publicity and a hasty retreat as some buyers noticed that they could save as much as \$15 on a DVD by deleting browser cookies that otherwise indicated to Amazon that they had visited the site before.<sup>23</sup> As this example suggests, forthrightly charging one price to one person and another price to someone else can generate resistance. Offering individualized discounts, however, can amount to the same thing for the vendor while appearing much more palatable to the buyer. Who would complain about receiving a coupon for \$15 off the listed price of an item, even if the coupon were not transferable to any other Amazon user? (The answer may be “someone who did not get the coupon,” but to most people the second scenario is less troubling than the one in which different prices were charged from the start.)<sup>24</sup>

---

(June 20, 2005), available at <<http://news.cnet.co.uk/software/0,39029694,39190155,00.htm>> (last visited Feb 21, 2008).

<sup>21</sup> Hiawatha Bray, *BC Warns Its Alumni of Possible ID Theft After Computer Is Hacked*, Boston Globe E3 (Mar 17, 2005), available at <[http://www.boston.com/business/technology/articles/2005/03/17/bc\\_warns\\_its\\_alumni\\_of\\_possible\\_id\\_theft\\_after\\_computer\\_is\\_hacked/](http://www.boston.com/business/technology/articles/2005/03/17/bc_warns_its_alumni_of_possible_id_theft_after_computer_is_hacked/)> (last visited Feb 21, 2008).

<sup>22</sup> See Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, available at <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>> (last visited Apr 15, 2008) (showing large and consistent data breaches between Jan 2005 and Apr 13, 2008, the date of the most recent update).

<sup>23</sup> Mark Ward, *Amazon's Old Customers "Pay More"*, BBC News (Sept 8, 2000), available at <<http://news.bbc.co.uk/2/hi/business/914691.stm>> (last visited Feb 21, 2008).

<sup>24</sup> For more on price discrimination for information goods, see William W. Fisher III,



Just as data mining could facilitate price discrimination for Amazon or other online retailers, it operates in the tangible world as well. For example, as a shopper uses a loyal-customer card, certain discounts are offered at the register, personalized to that customer. Soon, the price of a loaf of bread at the store may become indeterminate: there is a sticker price, but when the shopper takes the bread up front, the store can announce a special individualized discount based on her relationship with the store. The sticker price then becomes only that, providing little indication of the price that shoppers are actually paying. Merchants can also vary the level of service they provide. Customer cards augmented with RFID tags can serve to identify those undesirable customers who visit a home improvement store, monopolize the attention of the attendants, and exit without having bought so much as a single nail. With these kinds of cards, the store would be able to discern the “good” (profitable) customers from the “bad” (not profitable) ones and appropriately alert the staff to flee from bad customers and approach good ones. (Bad customers may then share their negative experiences with others, and it might ultimately behoove the store to be more explicit about what kinds of customers get what kinds of service when differentiation takes place.)

## II. PRIVACY 2.0

While privacy issues associated with government and corporate databases remain important, they are increasingly dwarfed by threats to privacy that do not fit the standard analytical template for addressing privacy threats. These new threats fit the generative pattern also found in the technical layers for internet and PC security, and in the content layer for ventures such as Wikipedia. The emerging threats to privacy serve as an example of generativity’s downsides on the social layer, where contributions from many corners can enable vulnerability and abuse that calls for intervention. Ideally such intervention would not unduly dampen the underlying generativity. Effective solutions for the problems of Privacy 2.0 have more in common with solutions to other generative problems than with the remedies associated with the decades-old analytic template for Privacy 1.0.

## A. The Era of Cheap Sensors

We can identify three successive shifts in technology from the early 1970s: cheap processors, cheap networks, and cheap sensors.<sup>25</sup> The third shift has, with the help of the first two, opened the doors to new and formidable privacy invasions.

The first shift was cheap processors. Moore's Law observes that processing power doubles every two years or so.<sup>26</sup> A corollary is that existing processing power gets cheaper. The cheap processors available since the 1970s have allowed Bill Gates's vision of a "computer on every desk and in every home" to be realized.<sup>27</sup> Cheap processors also underlie information appliances: thanks to Moore's Law, there are now sophisticated microprocessors in cars, coffeemakers, and singing greeting cards.

Cheap networks soon followed. The pay-per-minute proprietary dial-up networks gave way to an internet of increasing bandwidth and dropping price. The all-you-can-eat models of measurement meant that, once established, idle network connections were no cheaper than well-used ones, and a web page in New York cost no more to access from London than one in Paris. Lacking gatekeepers, these inexpensive processors and networks have been fertile soil for whimsical invention to take place and become mainstream.<sup>28</sup> This generativity has arisen in part because the ancillary costs to experiment—both for software authors and software users—have been so low.

The most recent technological shift has been the availability of cheap sensors: the equipment that translates a phenomenon from the real world into bits. Today's cameras, microphones, scanners, and global positioning systems have small, accurate, and inexpensive sensors. These characteristics have made sensors much easier to deploy—and then network—in places where previously it would have been impractical to have them.

---

<sup>25</sup> See Paul Saffo, *Sensors: The Next Wave of Infotech Innovation*, available at <<http://www.saffo.com/essays/sensors.php>> (last visited Feb 21, 2008) (identifying the progression from the "processing decade" to today's internet network revolution, and arguing that sensors will be the next wave in information technology).

<sup>26</sup> See Intel, *Excerpts from A Conversation with Gordon Moore: Moore's Law*, available at <[http://download.intel.com/museum/Moores\\_Law/Video-Transcripts/Excepts\\_A\\_Conversation\\_with\\_Gordon\\_Moore.pdf](http://download.intel.com/museum/Moores_Law/Video-Transcripts/Excepts_A_Conversation_with_Gordon_Moore.pdf)> (last visited Feb 21, 2008).

<sup>27</sup> See *Microsoft's Tradition of Innovation: From Revolution to Evolution* (Microsoft Oct 25, 2002), available at <<http://www.microsoft.com/About/CompanyInformation/ourbusinesses/profile.mspx>> (last visited Feb 21, 2008).

<sup>28</sup> See Zittrain, *The Future of the Internet* at 87–91 (cited in note 1) (discussing the ways in which generative platforms foster contributions from amateur sources that find value in markets, where traditional firms would fail to make such contributions).

The proliferation of cheap surveillance cameras has empowered the central authorities found within the traditional privacy equation – government regulators. A 2002 working paper estimated that the British government had spent \$100 million on closed-circuit television systems, with many networked to central law enforcement stations for monitoring.<sup>29</sup> Such advances, and the analysis that follows them, fit the template of Privacy 1.0: governments gain access to more information thanks to more widely deployed monitoring technologies, then rules and practices are suggested to prevent whatever our notions might be of abuse. To see how cheap processors, networks, and sensors create an entirely new form of problem, we must look to the excitement surrounding the participatory technologies suggested by one meaning of “Web 2.0.” In academic circles, this meaning of Web 2.0 has become known as “peer production.”

## B. The Dynamics of Peer Production

The aggregation of small contributions of individual work can make once-difficult tasks seem easy. For example, Yochai Benkler has approvingly described the National Aeronautics and Space Administration’s (“NASA’s”) use of public volunteers, or “clickworkers.”<sup>30</sup> NASA had a tedious job involving pictures of craters from the moon and Mars. These were standard bitmap images, and they wanted the craters to be vectorized: in other words, they wanted people to draw circles around the craters they saw in the photos. Writing some custom software and deploying it online, NASA asked internet users at large to undertake the task. Much to NASA’s pleasant surprise, the volunteer clickworkers accomplished in a week what a single graduate student would have needed a year to complete.<sup>31</sup> Cheap networks and PCs, coupled with the generative ability to costlessly offer

---

<sup>29</sup> Michael McCahill and Clive Norris, *Working Paper No 6, CCTV in London* (Urban Eye Project 2002), available at <[http://www.urbaneye.net/results/ue\\_wp6.pdf](http://www.urbaneye.net/results/ue_wp6.pdf)> (last visited Feb 21, 2008).

<sup>30</sup> Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* 69 (Yale 2006), available at <[www.benkler.org/Benkler\\_Wealth\\_Of\\_Networks.pdf](http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf)> (last visited Feb 21, 2008). More information on the original project’s results and further efforts is available at the clickworkers website. See <<http://clickworkers.arc.nasa.gov/top>> (last visited Feb 21, 2008).

<sup>31</sup> See Benkler, *Wealth of Networks* at 69 (cited in note 30) (describing the success of “an experiment to see if public volunteers, each working for a few minutes here and there can do some routine science analysis that would normally be done by a scientist or graduate student working for months on end”).

new code for others to run, meant that those who wanted to pitch in to help NASA could do so.

The near-costless aggregation of far-flung work can be applied in contexts other than the drawing of circles around craters, or the production of a free encyclopedia like Wikipedia. Computer scientist Luis von Ahn, after noting that over nine billion person-hours were spent playing Windows Solitaire in a single year, devised the online “ESP” game, in which two remote players are randomly paired and shown an image. They are asked to guess the word that best describes the image, and when they each guess the same word they win points.<sup>32</sup> Their actions also provide input to a database that reliably labels images for use in graphical search engines, improving the performance of image search engines. In real time, then, people are building and participating in a collective, organic, world-wide computer to perform tasks that real computers cannot easily do themselves.<sup>33</sup>

These kinds of grid applications produce (or at least encourage) certain kinds of public activity by combining small, individual private actions. Benkler calls this phenomenon “coordinate coexistence producing information.”<sup>34</sup> Benkler points out that the same idea helps us find what we are looking for on the internet, even if we are not using a graphical search engine enhanced by the ESP game; search engines commonly aggregate the artifacts of individual internet activity, such as webmasters’ choices about where to link, to produce relevant search results.

The value of this human-derived wisdom has been exploited by spammers, who create “link farms” of fake websites containing fragments of text drawn at random from elsewhere on the Web (“word salad”) that link back to the spammers’ sites in an attempt to boost their search engine rankings. The idea is that these fake websites will be mistaken by search engine crawlers as real ones, and the search engines will rank higher those sites that are frequently linked to by other site. The most valuable links are ones placed on truly popular websites, however, and the

---

<sup>32</sup> Luis von Ahn, *Human Computation*, (Google TechTalk Jul 26, 2006), available at <<http://video.google.com/videoplay?docid=-8246463980976635143>> (last visited Feb 21, 2008).

<sup>33</sup> See, for example, Benkler, *Wealth of Networks* at 81 (cited in note 30) (discussing the potential for digital proofreading).

<sup>34</sup> Id at 33 (cited in note 30). See also Jessica Litman, *Sharing and Stealing*, 27 Hastings Commun & Enter L J 1, 39–50 (2004) (examining the concept of public activity derived from compiling private activity in the context of online media sharing and peer-to-peer networks).

piles of inter-linked “word salad” among fake, computer-generated websites do not fully trick the search engines.

As a result, spammers have turned to leaving comments on popular blogs that ignore the original entry to which they are attached and instead simply provide links back to their own websites. In response, the authors of blogging software have incorporated so-called CAPTCHA<sup>35</sup> boxes that must be navigated before anyone can leave a comment on a blog. CAPTCHAs—now used on many mainstream websites including Ticketmaster.com—ask users to prove that they are human by typing in, say, a distorted nonsense word displayed in a small graphic.<sup>36</sup> Computers can start with a word and make a distorted image in a heartbeat, but they cannot easily reverse engineer the distorted image back to the word. This need for human intervention was intended to force spammers to abandon automated robots to place their blog comment spam. For a while they did, reportedly setting up CAPTCHA sweatshops that paid people to solve CAPTCHAs from blog comment prompts all day long.<sup>37</sup> (In 2003, the going rate was \$2.50/hour for such work.)<sup>38</sup> But spammers have continued to explore more efficient solutions. A spammer can write a program to fill in all the information but the CAPTCHA, and when it gets to the CAPTCHA it places it in front of a real person trying to get to a piece of information—say on a page a user might get after clicking a link that says, “You’ve just won \$1000! Click here!”<sup>39</sup>—or perhaps a pornographic photo.<sup>40</sup> The

---

<sup>35</sup> CAPTCHA is an acronym for “Completely Automated Public Turing test to tell Computers and Humans Apart.”

<sup>36</sup> For a detailed discussion of CAPTCHAs, see Luis von Ahn, et al, *CAPTCHA: Using Hard AI Problems for Security*, available at <[http://www.cs.cmu.edu/~biglou/CAPTCHA\\_crypt.pdf](http://www.cs.cmu.edu/~biglou/CAPTCHA_crypt.pdf)> (last visited Feb 22, 2008). See also *Ticketmaster v RMG*, 507 F Supp 2d 1096 (C D Cal 2007) (granting a preliminary injunction on the basis of copyright infringement against a software developer whose automated tool was used to bypass the plaintiff’s CAPTCHAs).

<sup>37</sup> For a detailed discussion of CAPTCHAs, spammers’ workarounds, and human computation, see von Ahn, *Human Computation* (cited in note 32); Luis von Ahn, *CAPTCHA, the ESP Game, and Other Stuff*, available at <<http://www.cs.cmu.edu/~biglou/cycles.ppt>> (last visited Feb 22, 2008) (accompanying slides for *Human Computation*).

<sup>38</sup> von Ahn, *CAPTCHA, the ESP Game, and Other Stuff*, slide 27 (cited in note 37).

<sup>39</sup> Email from Luis von Ahn to Jonathan Zittrain (May 22, 2007) (on file with author) (describing an email informing the recipient that she had won \$1,000 and prompting her to click a link to a page that asked her to solve a CAPTCHA in order to claim her prize).

<sup>40</sup> The use of pornography in motivating individuals to fill in CAPTCHAs has been suggested but not proven. See The Official CAPTCHA Site, available at <<http://www.CAPTCHA.net/>> (last visited Feb 22, 2008) (“[I]t might be the case that some spammers use porn sites to attack CAPTCHAs.”). See also *PC Stripper Helps Spam to Spread*, (BBC News Oct 30, 2007), available at <<http://news.bbc.co.uk/2/hi/technology/7067962.stm>> (last visited March 25, 2008).

CAPTCHA is copied that instant from a blog where a spammer's robot is waiting to leave a comment, and then pasted into the prompt for the human wanting to see the next page. The human's answer to the CAPTCHA is then instantly ported back over to the blog site in order to solve the CAPTCHA and leave the spammed comment.<sup>41</sup> Predictably, companies have also sprung up to meet this demand, providing custom software to thwart CAPTCHAs on a contract basis of \$100 to \$5,000 per project.<sup>42</sup> Generative indeed: the ability to remix different pieces of the Web, and to deploy new code without gatekeepers, is crucial to the spammers' work. Other uses of CAPTCHAs are more benign but equally subtle: a project called reCAPTCHA provides an open application programming interface ("API") to substitute for regular CAPTCHAs where a website might want to test to see if it is a human visiting.<sup>43</sup> reCAPTCHA creates an image that pairs a standard, automatically generated test word image with an image of a word from an old book that a computer has been unable to properly scan and translate.<sup>44</sup> When the user solves the CAPTCHA by entering both words, the first word is used to validate that the user is indeed human, and the second is used to put the human's computing power to work to identify one more word of one more book that otherwise would be unscannable.<sup>45</sup>

### C. Peer Production and Privacy 2.0

What do CAPTCHAs have to do with privacy? New generative uses of the internet have made the solutions proposed for Privacy 1.0 largely inapplicable. Fears about "mass dataveillance"<sup>46</sup> are not misplaced, but they recognize only part of the problem, and one that represents an increasingly smaller slice of

---

<sup>41</sup> See von Ahn, *Human Computation* (cited in note 32).

<sup>42</sup> See Brad Stone, *Captchas, Online Gatekeepers Against Spam, Need an Overhaul*, (Intl Herald Trib Jun 11, 2007), available at <<http://www.ihf.com/articles/2007/06/11/business/codes.php>> (last visited Jan 11, 2008).

<sup>43</sup> See Ben Maurer, *reCAPTCHA: A New Way to Fight Spam*, (May 23, 2007) available at <<http://bmaurer.blogspot.com/2007/05/reCAPTCHA-new-way-to-fight-spam.html>> (last visited Feb 22, 2008).

<sup>44</sup> See id.

<sup>45</sup> See id.

<sup>46</sup> Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* 23 (2004); Jeffrey Rosen, *The Naked Crowd: Balancing Privacy and Security in an Age of Terror*, 46 Ariz L Rev 607, 610 (2004) ("[I]t was proposed after September 11 to engage in ambitious forms of what Roger Clarke has called 'mass dataveillance' to consolidate and analyze public and private data in the hope of unearthing unusual patterns that might predict suspicious activity.").

the pie. Solutions such as disclosure<sup>47</sup> or encryption<sup>48</sup> still work for Privacy 1.0, but new approaches are needed to match the challenge of Privacy 2.0, in which sensitive data is collected and exchanged peer to peer in configurations as unusual as that of the spammers' system for bypassing CAPTCHAs.

The power of centralized databases feared in 1973 is now being replicated and amplified through generative uses of individual data and activity. For example, cheap sensors have allowed various gunshot-detecting technologies to operate through microphones in public spaces.<sup>49</sup> If a shot is fired, sensors associated with the microphones triangulate the shot's location and summon the police. To avoid false alarms, the system can be augmented with help from the public at large, minimizing the need for understaffed police to make the initial assessment about what is going on when a suspicious sound is heard. Interested citizens can review camera feeds near a reported shot and press a button if they see something strange happening on their computer monitors. Should a citizen do so, other citizens can be asked for verification. If the answer is yes, the police can be sent. (Of course, little prevents the repurposing of general-purpose microphones for other uses once the infrastructure is in place.)

In November of 2006, the state of Texas spent \$210,000 to set up eight webcams along the Mexico border as part of a pilot program to solicit the public's help in reducing illegal immigration.<sup>50</sup> Webcam feeds were sent to a public website, and people were invited to alert the police if they thought they saw suspi-

---

<sup>47</sup> See, for example, Fred H. Cate, *Privacy in the Information Age* 113 (Brookings 1997) (proposing how notice could be used to protect privacy).

<sup>48</sup> See, for example, Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* 172–73 (Random House 2000) (explaining how, with the help of encryption, “individual internet users could come close to realizing Louis Brandeis and Samuel Warren’s ideal” of privacy).

<sup>49</sup> ShotSpotter is a company that offers some examples of this technology. See ShotSpotter, *ShotSpotter Gunshot Location System (GLS) Overview*, available at <<http://www.shotspotter.com/products/index.html>> (last visited Feb 22, 2008) (providing an overview of the company’s products); Ethan Watters, *ShotSpotter*, *Wired Magazine* 146–52 (Apr 2007), available at <<http://www.shotspotter.com/news/articles/2007/4%20-%20April/Wired%20Magazine/Wired%20Article%20Eprint%204.10.07.pdf>> (last visited Feb 22, 2008) (discussing the use and effectiveness of this technology). See also ShotSpotter, *ShotSpotter in the News*, available at <<http://www.shotspotter.com/news/news.html>> (last visited Feb 22, 2008) (providing links to articles discussing the company and its products).

<sup>50</sup> Sig Christenson, *Border Webcams Rack Up Millions of Hits in a Month*, *Express-News San Antonio* (Dec 10, 2006), available at <[http://www.mysanantonio.com/news/metro/stories/MYSA121106.01A.border\\_webcam.323e8ed.html](http://www.mysanantonio.com/news/metro/stories/MYSA121106.01A.border_webcam.323e8ed.html)> (last visited Feb 22, 2008).

cious activity. During the month-long trial the website took in just under 28 million hits. No doubt many were from the curious rather than the helpful, but those wanting to volunteer came forward, too. The site registered over 220,000 users, and those users sent 13,000 e-mails to report suspicious activity. At three o'clock in the morning one woman at her PC saw someone signal a pickup truck on the webcam. She alerted police, who seized over four hundred pounds of marijuana from the truck's occupants after a high-speed chase. In separate incidents, a stolen car was recovered, and twelve undocumented immigrants were stopped. To some—especially state officials—this was a success beyond any expectation;<sup>51</sup> to others it was a paltry result for such an expensive investment.<sup>52</sup>

Beyond any first-order success of stopping crime, some observers welcome involvement by members of the public as a check on law enforcement surveillance.<sup>53</sup> Science fiction author David Brin foresaw increased use of cameras and other sensors by the government and adopted an if-you-can't-beat-them-join-them approach to dealing with the privacy threat. He suggested allowing ubiquitous surveillance so long as the watchers themselves were watched: live cameras could be installed in police cars, station houses, and jails. According to Brin, everyone watching everyone would lessen the likelihood of unobserved government abuse. What the Rodney King video did for a single incident<sup>54</sup>—one that surely would have passed without major public notice but for the amateur video capturing seemingly excessive force by arresting officers—Brin's proposal could do for nearly all state activities. Of course, Brin's calculus does not adequately account for the invasions of privacy that would take place whenever random members of the public could watch, and perhaps record, every interaction between citizens and authori-

---

<sup>51</sup> Id ("[S]tate officials Sunday tout[ed] it as a success beyond anyone's dreams.").

<sup>52</sup> AP, *Texas Border Cam Test Catches 10 Illegal Immigrants*, Chi Sun-Times (Jan 8, 2007) ("It seems to me that \$20,000 per undocumented worker is a lot of money" (quoting state representative Norma Chavez) (internal quotation marks omitted)); Editorial, *Virtual Wall a Real Bust That Didn't Come Cheap*, San Antonio Express-News 6B (Jan 19, 2007) ("[T]he results are in: The plan bombed.").

<sup>53</sup> See David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* 52–54, 149–78 (Addison-Wesley 1999).

<sup>54</sup> See Neal Feigenson and Meghan A. Dunn, *New Visual Technologies in Court: Directions for Research*, 27 L & Hum Behavior 109, 117 (2003) (discussing how recent advances in visual technologies will affect legal decisionmaking, with reference to many cases that have altered the way courtrooms incorporate new technologies, including the first Rodney King trial, "in which the use of slow-motion and freeze-framing desensitized jurors to the brutality of the beatings depicted in the original videotape").



ties, especially since many of those interactions take place at sensitive moments for the citizens. And ubiquitous surveillance can lead to other problems. The Sheriff's Office of Anderson County, Tennessee, introduced one of the first live "jailcams" in the county, covering a little area in the jail where jailors sit and keep an eye on everything—the center of the panopticon. The Anderson County webcam was very Web 2.0: the website included a chat room where visitors could meet others viewing it, there was a guestbook to sign, and a link to syndicated advertising to help fund the webcam. However, some people began using the webcam to make crank calls to jailors at key moments and even, it is claimed, to coordinate the delivery of contraband.<sup>55</sup> The webcam was shut down.<sup>56</sup>

This example suggests a critical difference between Privacy 1.0 and 2.0. If the government is controlling the observation, then the government can pull the plug on such webcams if it thinks they are not helpful, balancing whatever policy factors it chooses.<sup>57</sup> Many scholars have considered the privacy problems posed by cheap sensors and networks, but they focus on the situations where the sensors serve only government or corporate masters. Daniel Solove, for instance, has written extensively on emergent privacy concerns, but he has focused on the danger of "digital dossiers" created by businesses and governments.<sup>58</sup> Likewise, Jerry Kang and Dana Cuff have written about how small sensors will lead to "pervasive computing," but they worry that the technology will be abused by coordinated entities like

---

<sup>55</sup> Id (noting that Maricopa County, Arizona, also shut its camera down after losing a lawsuit by inmates alleging abuse of their rights).

<sup>56</sup> The Anderson County jailcam was discontinued as of Nov 27, 2006; the website no longer discusses its removal. It was formerly accessible at <<http://www.tnacso.net/cont/jailcam.php>>. See AP, *Tenn. Jail Webcam Jeopardizes Security*, Boston.com News (Nov 25, 2006), available at <[http://www.boston.com/news/odd/articles/2006/11/25/tenn\\_jail\\_web\\_cam jeopardizes\\_security/](http://www.boston.com/news/odd/articles/2006/11/25/tenn_jail_web_cam jeopardizes_security/)> (last visited Feb 22, 2008). See also Christian Bottorff, *Internet Peek at Jail Life Could End Soon: Anderson County Sheriff Says Webcam Jeopardizes Security*, Tennessean.com (Nov 24, 2006), available at <[http://www.earthcam.com/media/ecnews/articles/tennessean\\_11-24-2006.pdf](http://www.earthcam.com/media/ecnews/articles/tennessean_11-24-2006.pdf)> (last visited Feb 22, 2008) ("After six years Anderson County Sheriff Paul White shut down the jail Webcam citing safety concerns.").

<sup>57</sup> In the aftermath of the September 11 attacks and the passing of the USA PATRIOT Act, the government has been increasingly likely to take an active role in issues of electronic surveillance. For an overview of surveillance law and its shifting usage by the government, see Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 Geo Wash L Rev 1264, 1278–92 (2004) (detailing electronic surveillance law leading up to the USA PATRIOT Act).

<sup>58</sup> See Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* 2–7, 13–26 (NYU 2004) (expressing concern about the collection of information held in commercial databases, public records, and government files).

shopping malls, and their prescriptions thus follow the pattern established by Privacy 1.0.<sup>59</sup> Their concerns are not misplaced, but they represent an increasingly smaller part of the total picture. The essence of Privacy 2.0 is that government or corporations, or intermediaries, need not be the source of the surveillance.

Peer-to-peer technologies can eliminate points of control and gatekeeping from the transfer of personal data and information just as they can for movies and music. The intellectual property conflicts raised by the generative internet—where people can still copy large amounts of copyrighted music without fear of repercussion—are rehearsals for the problems of Privacy 2.0.<sup>60</sup> The Rodney King beating was filmed not by a public camera, but by a private one, and its novel use in 1991 is now commonplace. Many private cameras, including camera-equipped mobile phones, fit the generative mold as devices purchased for one purpose but frequently used for another. The Rodney King video, however, required news network attention to gain salience. Videos depicting similar events today gain attention without the prior approval of an intermediary.<sup>61</sup> With cheap sensors, processors, and networks, citizens can quickly distribute to anywhere in the world what they capture in their backyard. Therefore, any activity is subject to recording and broadcast. Perform a search on a video aggregation site like YouTube for “angry teacher” or “road rage” and hundreds of videos turn up. The presence of documentary evidence not only makes such incidents reviewable by the public at large, but for, say, angry teachers it also creates the possibility of getting fired or disciplined where there had not been one before. Perhaps this is good: teachers are on notice that

---

<sup>59</sup> See Kang and Cuff, 62 Wash & Lee L Rev at 134–42 (cited in note 15) (focusing privacy concerns on mall surveillance).

<sup>60</sup> The largest difference may arise from the fact that invasions of privacy implicate the dignity of individuals rather than firms' profits, and thus there is no natural lobby to organize against this personal intrusion.

<sup>61</sup> See Good Morning America, *Expert: LAPD Officers' Behavior Not Unreasonable: An Expert Says LAPD Officers Likely Acted Within the Law in Restraining a Suspect*, ABC News (Nov 11, 2006), available at <<http://abcnews.go.com/GMA/story?id=2646425>> (last visited Feb 22, 2008) (“A videotape posted on the Web site Youtube.com shows Los Angeles police officers hitting 24-year-old William Cardenas during an arrest.”); *LA Police Brutality Video*, YouTube (posted by 3101010 on YouTube, Nov 10, 2006), available at <[http://www.youtube.com/watch?v=7\\_gFJJXLv28](http://www.youtube.com/watch?v=7_gFJJXLv28)> (last visited Feb 22, 2008) (“Video footage of a police officer repeatedly striking a suspect in the face during an arrest three months ago has triggered an FBI investigation after the video was posted on YouTube.com.”).

they must account for their behavior the way that police officers must take responsibility for their own actions.

If so, it is not just officers and teachers: we are all on notice. The famed “bus uncle” of Hong Kong upbraided a fellow bus passenger who politely asked him to speak more quietly on his mobile phone.<sup>62</sup> 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 2 million people have viewed one version of the exchange.<sup>63</sup> (Others have since created derivative versions of the exchange, including karaoke and a ringtone.<sup>64</sup>) Weeks after the video was posted, the Bus Uncle was beaten up in a targeted attack at the restaurant where he worked.<sup>65</sup> In a similar incident, a woman’s dog defecated on the floor of a South Korean subway. She refused to clean it up, even when offered a tissue—though she cleaned the dog—and left the subway car at the next stop.<sup>66</sup> The incident was captured on a mobile phone camera and posted to the internet, where the poster issued an all points bulletin seeking information about the dog owner and her relatives and about where she worked.<sup>67</sup> She was identified by others who had previously seen her and the dog, and the resulting firestorm of criticism apparently caused her to quit her job.<sup>68</sup>

The summed outrage of many unrelated people viewing a disembodied video may be disproportionate to whatever social norm or law is violated within that video. Lives can be ruined after momentary wrongs, even if merely misdemeanors. Teacher behavior in a classroom, for example, is largely a matter of standards and norms rather than rules and laws. But the presence of scrutiny, should anything unusual happen, can halt desirable pedagogical risks if there is a chance those risks could be taken

---

<sup>62</sup> *Bus Uncle*, (YouTube May 11, 2006), available at <<http://www.youtube.com/watch?v=RSHziqJWYcM>> (last visited July 21, 2008).

<sup>63</sup> *Id.* (showing 2,034,671 views and 1,277 comments as of July 21, 2008).

<sup>64</sup> See *Hong Kong’s “Bus Uncle” Beaten Up by Three Men*, Channel NewsAsia (June 8, 2006), available at <<http://www.channelnewsasia.com/stories/eastasia/view/212671/1.html>> (last visited Feb 22, 2008).

<sup>65</sup> *Id.*

<sup>66</sup> Jonathan Krim, *Subway Fracas Escalates into Test of the Internet’s Power to Shame*, Wash Post D01 (July 7, 2005), available at <<http://www.washingtonpost.com/wp-dyn/content/article/2005/07/06/AR2005070601953.html>> (last visited Feb 22, 2008).

<sup>67</sup> *Id.*

<sup>68</sup> See *id.* (“Humiliated in public and indelibly marked, the woman reportedly quit her university.”).

out of context, misconstrued, or become the subject of pillory by those with perfect hindsight.

These phenomena affect students as well as teachers, regular citizens rather than just those in authority. And ridicule or mere celebrity can be as chilling as outright disapprobation. In November 2002 a Canadian teenager used his high school's video camera to record himself swinging a golf ball retriever as though it were a light saber from *Star Wars*.<sup>69</sup> By all accounts he was doing it for his own amusement. The tape was not erased, and it was found the following spring by someone else who shared it, first with friends and then with the internet at large. Although individuals want privacy for themselves, they will line up to see the follies of others, and by 2006 the "Star Wars Kid" was estimated to be the most popular word-of-mouth video on the internet, with over 900 million cumulative views.<sup>70</sup> It has spawned several parodies, including ones shown on prime time television. This is a consummately generative event: a repurposing of something made for completely different reasons, taking off beyond any expectation, and triggering further works, elaborations, and commentaries—both by other amateurs and by Hollywood.<sup>71</sup> It is also a privacy story. The student who made the video has been reported to have been traumatized by its circulation, and in no way did he seek to capitalize on his celebrity.<sup>72</sup>

In this hyperscrutinized reality, people may moderate themselves instead of expressing their true opinions. To be sure, people have always balanced between public and private expression. As Mark Twain observed:

We are discreet sheep; we wait to see how the drove is going, and then go with the drove. We have two opinions:

---

<sup>69</sup> For details on Star Wars Kid, see Wikipedia, *Star Wars Kid*, available at <[http://en.wikipedia.org/wiki/Star\\_Wars\\_kid](http://en.wikipedia.org/wiki/Star_Wars_kid)> (last visited Feb 23, 2008).

<sup>70</sup> *Star Wars Kid Is Top Viral Video*, BBC News (Nov 27, 2006), available at <<http://news.bbc.co.uk/2/hi/entertainment/6187554.stm>> (last visited Feb 23, 2008).

<sup>71</sup> See, for example, Heather Adler, *Stephen Colbert Aims His Lightsaber at Star Wars*, Dose.ca (Aug 24, 2006), available at <<http://www.dose.ca/celeb/story.html?id=10261eb6-0469-4198-a16a-1f302275b2a9>> (last visited Feb 23, 2008) (describing the Comedy Central show host's mocking of the Star Wars Kid); *White & Nerdy* (Google Video, Sept 19, 2006), available at <<http://video.google.com/videoplay?docid=1384277706451157121>> (last visited Feb 23, 2008) ("Weird Al" Yankovic's music video from his album "Straight Outta Lynwood," which includes a scene imitating the Star Wars Kid). For a list of other pop-culture references, see Wikipedia, *Star Wars Kid* (cited in note 69).

<sup>72</sup> See Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* 44–48 (Yale 2007).

one private, which we are afraid to express; and another one—the one we use—which we force ourselves to wear to please Mrs. Grundy, until habit makes us comfortable in it, and the custom of defending it presently makes us love it, adore it, and forget how pitifully we came by it. Look at it in politics.<sup>73</sup>

Today we are all becoming politicians. People in power, whether at parliamentary debates or press conferences, have learned to stick to carefully planned talking points, accepting the drawbacks of appearing stilted and saying little of substance in exchange for the benefits of predictability and stability.<sup>74</sup> Ubiquitous sensors threaten to push everyone toward treating each public encounter as if it were a press conference, creating fewer spaces in which citizens can express their private selves.

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.<sup>75</sup> By one definition they mean who manages the space: a federal post office is public; a home is private. A typical restaurant or inn is thus also private, yet it is also a place where the public gathers and mingles: someone there is “in public.” But while activities in private establishments open to the public are technically in the public eye,<sup>76</sup> what transpires there is usually limited to a handful of eyewitnesses—likely strangers—and the activity is ephemeral. No more, thanks to cheap sensors and cheap networks to disseminate what they glean. As our previously *private* public spaces, like classrooms and restaurants, turn

---

<sup>73</sup> Mark Twain, Volume II *Mark Twain's Autobiography* 10 (Harper 1924).

<sup>74</sup> This was a lesson learned by George Allen, a Republican candidate in the 2006 U.S. Senate campaign who was caught on camera calling an Indian supporter of his opponent by the derogatory epithet “macaca.” Carl Hulse, *Senator Apologizes to Student for Remark*, NY Times A20 (Aug 24, 2006), available at <<http://www.nytimes.com/2006/08/24/washington/24allen.html>> (last visited Feb 23, 2008). See also Dale Eisman, *Others Will Have “Macaca Moments,” Pundits Say*, Virginian-Pilot (Dec 1, 2006), available at <[http://www.redorbit.com/news/technology/751673/others\\_will\\_have\\_macaca\\_moments\\_pundits\\_say/index.html](http://www.redorbit.com/news/technology/751673/others_will_have_macaca_moments_pundits_say/index.html)> (last visited Feb 23, 2008) (noting the inevitability of another slip caught on videotape as “hundreds of citizen activists, armed with cell-phone cameras [are] ready to catch any awkward moment and misstatement to distribute it through cyberspace.”).

<sup>75</sup> See Solove, *The Future of Reputation*, 7–9, 162–89 (cited in note 72).

<sup>76</sup> Such places, while private, are sometimes treated by the law as places of “public accommodation,” in recognition of their hybrid status. This classification imposes some responsibility on their owners for equal treatment of patrons. See 42 USC § 12181(7) (2000) (defining a public accommodation as a restaurant and inn, among other things, for purposes of the Americans with Disabilities Act); 42 USC §§ 2000a(b)(1)–(2) (2000) (classifying inns and restaurants as places of public accommodations for the purposes of the 1964 Civil Rights Act).

into *public* public spaces, the pressure will rise for us to always be on press conference behavior.

There are both significant costs and benefits inherent in expanding the use of our public selves into more facets of daily life. Our public face may be kinder, and the expansion may cause us to rethink our private prejudices and excesses as we publicly profess more mainstream standards and, as Twain says, "habit makes us comfortable in it."<sup>77</sup> On the other hand, as law professors Eric Posner and Cass Sunstein point out, strong normative pressure can prevent outlying behavior of any kind, and group baselines can themselves be prejudiced.<sup>78</sup> Outlying behavior is the generative spark found at the social layer, the cultural innovation out of left field that can later become mainstream. Our information technology environment has benefited immeasurably from experimentation by a variety of people with different aims, motives, and skills. In the same way, our cultural environment is bettered when commonly held and rarely revisited views can be challenged.

The framers of the American Constitution embraced anonymous speech in the political sphere as a way of being able to express unpopular opinions without having to experience personal disapprobation.<sup>79</sup> No defense of a similar principle was needed

---

<sup>77</sup> Twain, Volume II *Mark Twain's Autobiography* at 10 (cited in note 73).

<sup>78</sup> See Eric A. Posner and Cass R. Sunstein, *The Law of Other States*, 59 Stan L Rev 131, 162 (2006) ("In a reputational cascade, people think that they know what is right, or what is likely to be right, but they nonetheless go along with the crowd in order to maintain the good opinion of others. Suppose that Albert suggests that global warming is a serious problem and that Barbara concurs with Albert, not because she actually thinks that Albert is right, but because she does not wish to seem, to Albert, to be ignorant or indifferent to environmental protection. If Albert and Barbara seem to agree that global warming is a serious problem, Cynthia might not contradict them publicly and might even appear to share their judgment, not because she believes that judgment to be correct, but because she does not want to face their hostility or lose their good opinion. It should be easy to see how this process might generate a cascade."). New and unique ideas can have important effects; for a general discussion, see Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (Back Bay 2000), but unless widely held views are consistently challenged, incorrect ideas can become deeply ensconced. See Cass R. Sunstein, *A New Progressivism*, 17 Stan L & Pol Rev 197, 210–11 (2006) ("[S]mall or even large groups of people [can] end up believing something—even if that something is false—simply because other people seem to believe it."). See also Irving L. Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascos* (Houghton Mifflin 2d ed 1982) (discussing how group pressure can lead members to agree to a result that they personally think is wrong).

<sup>79</sup> See *McIntyre v Ohio Elections Commission*, 514 US 334, 360 (1995) (Thomas concurring) ("There is little doubt that the Framers engaged in anonymous political writing. The essays in the Federalist Papers, published under the pseudonym of 'Publius,' are only the most famous example of the outpouring of anonymous political writing that occurred during the ratification of the Constitution."); id at 361 (Scalia dissenting) ("[T]he histori-

for keeping private conversations in public spaces from becoming verbatim public broadcasts—disapprobation that begins with small “test” groups but somehow becomes societywide—since there were no means by which to perform that transformation. Now that the means exist, a defense is called for lest we run the risk of letting our social system become metaphorically more applanicized: open to change only by those few radicals so disconnected from existing norms as to not fear their imposition at all.

Privacy 2.0 is about more than those who are famous or those who become involuntary “welebrities.” For those who happen to be captured doing particularly fascinating or embarrassing things, like Star Wars Kid or an angry teacher, a utilitarian might say that 900 million views is first-order evidence of a public benefit far exceeding the cost to the student who made the video. It might even be pointed out that the Star Wars Kid failed to erase the tape, so he can be said to bear some responsibility for its circulation. But the next generation privacy problem cannot be written off as affecting only a few unlucky victims. Neither can it be said to affect only genuine celebrities who must now face constant exposure not only to a handful of professional paparazzi but also to hordes of sensor-equipped amateurs. (Celebrities must now contend with the consequences of cell phone video of their slightest aberrations—such as one in which a mildly testy exchange with a valet parker is quickly circulated and exaggerated online<sup>80</sup>—or more comprehensive peer-produced sites like Gawker Stalker, where people send in local sightings of celebrities as they happen.<sup>81</sup> Gawker strives to relay the sightings within fifteen minutes and place them upon a Google map,<sup>82</sup> so that if Jack Nicholson is at Starbucks, one can arrive in time to stand awkwardly near him before he finishes his latte.

“[O]n the Web, everyone will be famous to fifteen people.”<sup>83</sup> Cybervisionary David Weinberger, in this twist on Andy Warhol’s famous quotation, posed the central issue for the rest of us. Although Weinberger made his observation in the context of

---

cal evidence indicates that Founding-era Americans opposed attempts to require that anonymous authors reveal their identities on the ground that forced disclosure violated the ‘freedom of the press.’”).

<sup>80</sup> See TMZ Staff, *Elisha: The B\*tch Next Door!*, TMZ.com (Nov 14, 2006), available at <<http://www.tMZ.com/2006/11/14/elisha-the-b-tch-next-door/>> (last visited Jan 15, 2008).

<sup>81</sup> See <<http://gawker.com/stalker/>> (last visited June 1, 2007).

<sup>82</sup> See id.

<sup>83</sup> David Weinberger, *Small Pieces Loosely Joined: A Unified Theory of the Web* 104 (Perseus 2002).

online expression, explaining that microaudiences are worthy audiences, it has further application. Just as cheap networks make it possible for businesses to satisfy the “long tail,” serving the needs of obscure interests every bit as much as popular ones<sup>84</sup> (Amazon.com is virtually able to stock a selection of books far beyond the bestsellers found in a physical bookstore), peer-produced databases can be configured to track the people who are of interest only to a few others.

How will the next generation privacy problem affect average citizens? Early photo aggregation sites like Flickr were premised on a seemingly dubious assumption that turned out to be true: not only would people want an online repository for their photos, but they would often be pleased to share them with the public at large. Such sites now boast hundreds of millions of photos,<sup>85</sup> many of which are also sorted and categorized thanks to the same distributed energy that got Mars’s craters promptly mapped. Proponents of Web 2.0 sing the praises of “folksonomies,” bottom-up tagging done by strangers, in contrast to expert-designed and -applied canonical taxonomies like the Dewey Decimal System or the Library of Congress schemes for sorting books.<sup>86</sup> Metadata describing the contents of pictures makes images far more useful and searchable. Combining user-generated tags with automatically generated data makes pictures even more accessible. Camera makers now routinely build cameras that use the Global Positioning System to mark exactly where on the planet each of the pictures it snaps was taken and, of course, to time- and date-stamp them. Websites 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 im-

---

<sup>84</sup> Traditionally, retailers, television networks, and movie theaters were forced to try to identify mainstream, popular choices. They had to favor middle-ground material because they had only a limited amount of shelf space, prime-time hours, or screens, respectively, and needed to maximize their sales. Online marketplaces do not have that limitation: “A hit and a miss are on equal economic footing, both just entries in a database called up on demand, both equally worthy of being carried. Suddenly, popularity no longer has a monopoly on profitability.” Chris Anderson, *The Long Tail*, 12.10 *Wired* 2 (Oct 2004), available at <<http://www.wired.com/wired/archive/12.10/tail.html>> (last visited Feb 23, 2008).

<sup>85</sup> Flickr had more than 500 million photos as of May 2007. Email from Meagan Busath, public relations representative, Flickr, to Jonathan Zittrain (May 24, 2007, 15:17 EDT) (on file with author).

<sup>86</sup> David Weinberger, *Everything is Miscellaneous: The Power of the New Digital Disorder* 165–66 (Henry Holt 2007).



age appears in the background.<sup>87</sup> In August 2006 Google announced the acquisition of Neven Vision, a company working on photo recognition, and in May 2007 Google added a feature to its image search so that searchers can limit their search to images of people (to be sure, this is still short of identifying which image is which).<sup>88</sup> Massachusetts officials have used such technology to compare mug shots in “Wanted” posters to driver’s license photos, leading to arrests.<sup>89</sup> Mash together these technologies and functionalities through the kind of generative mixing allowed by their open APIs and it becomes trivial to receive answers to questions like: Where was Jonathan Zittrain last year on the fourteenth of February? Or, who could be found near the entrance to the local Planned Parenthood clinic in the past six months? The answers need not come from government or corporate cameras, which are at least partially secured against abuse through well-considered privacy policies from Privacy 1.0. Instead, the answers come from a more powerful, generative source: an army of the world’s photographers, including tourists sharing their photos online without firm (or legitimate) expectations of how they might next be used and re-used.<sup>90</sup>

Those uses may be surprising or even offensive to those who create the new tools or provide the underlying data. The Christian Gallery News Service was started by antiabortion activist Neal Horsley in the mid 1990s.<sup>91</sup> Part of its activities included the Nuremberg Files website, where the public was solicited for

---

<sup>87</sup> Riya is a visual search engine that helps users find similar images. See About Riya, <<http://www.riya.com/about>> (last visited March 16, 2008). Polar Rose is a browser plug-in that identifies people in public photographs on the Web. See Polar Rose, <<http://www.polarrose.com/>> (last visited March 16, 2008). MyHeritage uses visual searching technology to locate users’ family members online. See About MyHeritage.com, <<http://www.myheritage.com/about-myheritage>> (last visited March 16, 2008).

<sup>88</sup> See Posting of Loren Baker to Search Engine Journal, *Google, Neven Vision & Image Recognition* (Aug 15, 2006), available at <<http://www.searchenginejournal.com/google-neven-vision-image-recognition/3728/>> (last visited Feb 23, 2008); Jacqui Cheng, *Facial Recognition Slipped into Google Image Search*, *Ars Technica* (May 30, 2007), available at <<http://arstechnica.com/news.ars/post/20070530-facial-recognition-slipped-into-google-image-search.html>> (last visited Feb 23, 2008).

<sup>89</sup> See Adam Liptak, *Driver’s License Emerges as Crime-Fighting Tool, but Privacy Advocates Worry*, *NY Times* A10 (Feb 17, 2007), available at <<http://www.nytimes.com/2007/02/17/us/17face.html>> (last visited Feb 23, 2008).

<sup>90</sup> U.S. law generally does not provide a privacy right protecting those who are in public from being photographed (or preventing the publication of resulting photographs). See, for example, *Gil v Hearst Publishing Co*, 253 P2d 441, 444–45 (Cal 1953) (holding that a couple photographed at their place of business at a public market had no cause of action against the photograph’s publisher).

<sup>91</sup> See Christian Gallery News Service, available at <<http://www.christiangallery.com/>> (last visited Feb 23, 2008).

as much information as possible about the identities, lives, and families of physicians who performed abortions, as well as about clinic owners and workers.<sup>92</sup> When a provider was killed, a line would be drawn through his or her name. (The site was rarely updated with new information, and it became entangled in a larger lawsuit lodged under the U.S. Freedom of Access to Clinic Entrances Act.<sup>93</sup> The site remains accessible.) An associated venture solicits the public to take pictures of women arriving at clinics, including the cars in which they arrive (and corresponding license plates), and posts the pictures in order to deter people from nearing clinics.<sup>94</sup>

With image recognition technology mash-ups, photos taken as people enter clinics or participate in protests can be instantly cross-referenced with their names. One can easily pair this type of data with Google Maps to provide fine-grained satellite imagery of the homes and neighborhoods of these individuals, similar to the “subversive books” maps created by computer consultant and tinkerer Tom Owad tracking wish lists on Amazon.com.<sup>95</sup>

This intrusion can reach places that the governments of liberal democracies refuse to go. In early 2007, a federal court overseeing the settlement of a class action lawsuit over New York City police surveillance of public activities held that routine po-

<sup>92</sup> See *The Nuremberg Files*, available at <<http://www.christiangallery.com/atrocity/>> (last visited Feb 23, 2008).

<sup>93</sup> See *Planned Parenthood of Columbia/Willamette, Inc v American Coalition of Life Activists*, 422 F3d 949, 951–52 (9th Cir 2005) (modifying the jury verdict against the American Coalition of Life Activists for their “campaign of terror and intimidation,” which included operating the Nuremberg Files website).

<sup>94</sup> See *Abortion Cams: Shame Deters Abortion*, available at <<http://www.abortioncams.com/>> (last visited Feb 23, 2008). The website is premised on the belief that showing the images of clinic patients will either shame or scare women away from having an abortion. See *How to Deter Abortion*, available at <<http://www.abortioncams.com/deter.htm>> (last visited Feb 23, 2008) (“Would a preacher want to be photographed going into a whore house, would a Priest want to be photographed going into a sex chat room with grade school kids? Neither would a mother want to be photographed going in to kill her baby.”).

<sup>95</sup> See Posting of Tom Owad to Applefritter, *Data Mining 101: Finding Subversives Within Amazon Wishlists*, available at <<http://www.applefritter.com/bannedbooks>> (submitted Jan 4 2006) (last visited Feb 23, 2008). See also Paul Marks, “Mashup” Websites Are a Dream Come True for Hackers, 2551 New Scientist 28 (May 12, 2006), available at <<http://www.newscientisttech.com/channel/tech/electronic-threats/mg19025516.400-mashup-websites-are-a-hackers-dream-come-true.html>> (last visited Feb 23, 2008) (“Mashups . . . are created by merging data from two or more websites . . . Mashups merge location-based information with other online sources to create an application that amounts to more than the sum of its parts. For instance, [www.chicagocrime.org](http://www.chicagocrime.org) combines Google Local’s maps with Chicago’s crime database, pinpointing the city’s crime hot-spots.”).

lice videotaping of public events was in violation of the settlement:

The authority . . . conferred upon the NYPD "to visit any place and attend any event that is open to the public, on the same terms and conditions of the public generally," cannot be stretched to authorize police officers to videotape everyone at a public gathering just because a visiting little old lady from Dubuque . . . could do so. There is a quantum difference between a police officer and the little old lady (or other tourist or private citizen) videotaping or photographing a public event.<sup>96</sup>

The court expressed concern about a chilling of speech and political activities if authorities were videotaping public events. But police surveillance becomes moot when an army of little old ladies from Dubuque is naturally videotaping and sharing nearly everything: protests, scenes inside a mall (such that amateur video exists of a random shootout in a Salt Lake City, Utah, mall),<sup>97</sup> or picnics in the park. 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. Cheap processors, networks, and sensors enable a new form of beneficial information flow as citizen reporters can provide footage and front line analysis of newsworthy events as they happen.<sup>98</sup> For example, OhmyNews is a wildly popular online newspaper in South Korea with citizen-written articles and reports. (Such writers provide editors with their national identity number so articles are not fully anonymous.) Similarly, those who might commit atrocities within war zones can now be surveilled and recorded by civilians so that their actions may be watched and ultimately punished, a potential sea change for the protection of human rights.<sup>99</sup>

---

<sup>96</sup> *Handschu v Special Service Division*, No 71 Civ 2203 (S D NY Feb 15, 2007), available at <[http://graphics.nytimes.com/packages/pdf/nyregion/20070215\\_nycruling.pdf](http://graphics.nytimes.com/packages/pdf/nyregion/20070215_nycruling.pdf)> (last visited Feb 23, 2008).

<sup>97</sup> See *Home Video: Utah Mall Shooting*, FOX News (Feb 16, 2007), available at <<http://www.foxnews.com/story/0,2933,252395,00.html>> (last visited Feb 23, 2008).

<sup>98</sup> See AFP, *Internet Users Transformed into News Reporters*, Breitbart.com (Feb 11, 2007), available at <[http://www.breitbart.com/article.php?id=070211104154.4keqosqw&show\\_article=1](http://www.breitbart.com/article.php?id=070211104154.4keqosqw&show_article=1)> (last visited Feb 23, 2008) ("You have tens of millions of people around the world with cell phones with cameras connected to providers. It's like having an army of stringers out." (quoting Scott Moore, head of Yahoo News)).

<sup>99</sup> Witness.org was founded with the idea that it would be easier to bring perpetrators to justice if there was photographic or video evidence of their crimes. Its mission is to use

For privacy, peer-leveraging technologies might make for a much more constrained world rather than the more chaotic one that they have wrought for intellectual property. More precisely, a world where bits can be recorded, manipulated, and transmitted without limitation means, in copyright, a free-for-all for the public and constraint upon firms (and perhaps upstream artists) with content to protect. For privacy, the public is variously creator, beneficiary, and victim of the free-for-all. The constraints—in the form of privacy invasion that Jeffrey Rosen crystallizes as an “unwanted gaze”<sup>100</sup>—now come not only from the well-organized governments or firms of Privacy 1.0, but from a few people generatively drawing upon the labors of many to greatly impact rights otherwise guaranteed by a legal system.

### III. PRIVACY AND REPUTATION

At each layer where a generative pattern can be discerned, we can ask whether there is a way to sift out what we might judge to be bad generative results from the good ones without unduly damaging the system’s overall generativity. This is a question raised at the technical layer for network security, at the content layer for falsehoods in Wikipedia and failures of intellectual property protection, and now at the social layer for privacy.<sup>101</sup> Can we preserve generative innovations without giving up our core privacy values? Before turning to answers, it is helpful to explore a final piece of the Privacy 2.0 mosaic: the impact of emerging reputation systems. This is both because such systems can greatly impact our privacy<sup>102</sup> and because reputational tools may help solve the generative sifting problem at other layers.

---

“video and online technologies to open the eyes of the world to human rights violations.” See <[http://witness.org/index.php?option=com\\_content&task=view&id=26&Itemid=78](http://witness.org/index.php?option=com_content&task=view&id=26&Itemid=78)> (last visited Feb 23, 2008).

<sup>100</sup> See Rosen, *Unwanted Gaze* (cited in note 48).

<sup>101</sup> See Zittrain, *The Future of the Internet* at 64 (cited in note 1).

<sup>102</sup> Consider Solove, *The Future of Reputation* (cited in note 72).

Search is central to a functioning Web,<sup>103</sup> and reputation has become central to search. If people already know exactly what they are looking for, a network needs only a way of registering and indexing specific sites. Thus, IP addresses are attached to computers, and domain names to IP addresses, so that we can ask for [www.cnn.com](http://www.cnn.com) and go straight there. But much of the time we want help in finding something without knowing the exact online destination. Search engines help us navigate the petabytes of publicly posted information online, and for them to work well they must do more than simply identify all pages containing the search terms that we specify. They must rank them in relevance.

There are many ways to identify what sites are most relevant. A handful of search engines auction off the top-ranked slots in search results on given terms and determine relevance on the basis of how much the site operators would pay to put their sites in front of searchers.<sup>104</sup> These search engines are not widely used.<sup>105</sup> Most have instead turned to some proxy for reputation.

---

<sup>103</sup> Urs Gasser, *Regulating Search Engines: Taking Stock and Looking Ahead*, 8 Yale J L & Tech 201, 202 (2006) ("Since the creation of the first pre-Web Internet search engines in the early 1990s, search engines have become almost as important as email as a primary online activity. Arguably, search engines are among the most important gatekeepers in today's digitally networked environment."); Stephen E. Arnold, *Google: Search Becomes an Application Platform* 1 (2005) (unpublished position paper, on file with the U Chi Legal F) ("Just as calculations were one of the reasons for mainframes, search is one of the reasons why distributed, parallel, commodity-based network systems as the next computing platforms. The smartphone, the desktop computer, the Xbox game machine, and even the mainframe gain greater utility when linked to a computer similar to one built, owned, and operated by Google."); Memorandum from Deborah Fallows et al, Pew Internet & American Life Project, *The popularity and importance of Search Engines* 3 (Aug 2004), available at <[http://www.pewinternet.org/pdfs/PIP\\_Data\\_Memo\\_Searchengines.pdf](http://www.pewinternet.org/pdfs/PIP_Data_Memo_Searchengines.pdf)> (last visited Feb 24, 2008) ("The availability of reliable, easy-to-use search engines has transformed people's connection to information. For some, search engines are indispensable. Many people deeply rely on search engines to deliver vitally important information to them: 44% of searchers say that all or most of the searches they conduct are for information they absolutely need to find.").

<sup>104</sup> Pay-for-placement has existed from the early days of the Web's commercialization. See Jeff Pelline, *Pay-for-Placement Gets Another Shot*, CNET News.com (Feb 19, 1998), available at <[http://news.com.com/Pay-for-placement+gets+another+shot/2100-1023\\_3-208309.html](http://news.com.com/Pay-for-placement+gets+another+shot/2100-1023_3-208309.html)> (last visited Feb 24, 2008) (noting renewed attempts to establish pay-for-placement search engines in 1998). Until early 2007, Yahoo's search engine placed the highest bidders' ads before the most relevant ads. Yahoo, however, switched to ranking based on relevance only, a change driven by significant competitive pressures. See Sara Kehaulani Goo, *Yahoo Retools Ad Technology; Ranking System Ends Pay-for-Placement Ads in Search Results*, Wash Post D2 (Feb 6, 2007), ("The whole notion that I can buy my way to the top [of sponsored links] is something we do want to move beyond" (quoting Tim Cadogan, Vice President, Yahoo Search Marketing) (interpolation in original)). Of course, advertisers routinely pay for placement among sets of sponsored links included alongside search results in search engines like Yahoo and Google.

<sup>105</sup> See Hitslink, *Search Engine Market Share for January 2008*, available at

As mentioned earlier, a site popular with others—with lots of inbound links—is considered worthier of a high rank than an unpopular one, and thus search engines can draw upon the behavior of millions of other websites as they sort their search results.<sup>106</sup> Sites like Amazon.com deploy a different form of ranking, using the “mouse droppings” of customer purchasing and browsing behavior to make recommendations—so they can identify for customers that “people who like the Beatles also like the Rolling Stones.”<sup>107</sup> Search engines can also more explicitly invite the public to express its views on the items it ranks, so that users can decide what to view or buy on the basis of others’ opinions. Amazon users can rate and review the items for sale, and subsequent users then rate the first users’ reviews. Sites like Digg and Reddit invite users to vote for stories and articles they like, and tech news site Slashdot employs a rating system so complex that it attracts much academic attention.<sup>108</sup>

eBay uses reputation to help shoppers find trustworthy sellers. eBay users rate each others’ transactions, and this trail of ratings then informs future buyers how much to trust repeat sellers. These rating systems are crude but powerful. Malicious sellers can abandon poorly rated eBay accounts and sign up for new ones, but fresh accounts with little track record are often viewed skeptically by buyers, especially for proposed transactions involving expensive items. One study confirmed that established identities fare better than new ones, with buyers willing to pay, on average, over eight percent more for items sold by highly regarded, established sellers.<sup>109</sup> Reputation systems have many pitfalls and can be gamed, but the scholarship seems to indicate that they work reasonably well.<sup>110</sup> There are many ways reputa-

---

<<http://marketshare.hitslink.com/report.aspx?qprid=4>> (last visited Feb 24, 2008) (finding that Google and Yahoo! together enjoy nearly 90 percent market share).

<sup>106</sup> Benkler, *Wealth of Networks* 76 (cited in note 30) (“More fundamentally, the core innovation of Google, widely recognized as the most efficient general search engine during the first half of the 2000s, was to introduce peer-based judgments of relevance. . . . The engine treats links from other Web sites pointing to a given Web site as votes of confidence.”).

<sup>107</sup> A New York state legislator recently proposed a new law that would limit some online companies’ ability to track such mouse droppings. See Louise Story, *A Push To Limit the Tracking of Web Surfer’s Clicks*, NY Times C3 (March 20, 2008).

<sup>108</sup> Benkler, *Wealth of Networks* at 76–80 (cited in note 30) (describing the peer rating systems of various websites).

<sup>109</sup> See Paul Resnick, et al, *The Value of Reputation on eBay: A Controlled Experiment*, 9 *Experimental Econ* 79, 96 (2006) (“[B]uyers are willing to pay 8.1% more for lots sold by STRONG [reputation sellers] than NEW [sellers].”).

<sup>110</sup> See, for example, Paul Resnick, et al, *Reputation Systems: Facilitating Trust in Internet Interactions*, 43(12) *Commun ACM* 45, 46 (Dec 2000) (noting that reputation

tion systems might be improved, but at their core they rely on the fact that the number of people rating each other in good faith probably well exceeds the number of people seeking to game the system—and a way to exclude robots working for the latter. For example, eBay's rating system has been threatened by the rise of "1-cent eBooks" with no shipping charges; sellers can create alter egos to bid on these non-items and then have the phantom users highly rate the transaction.<sup>111</sup> One such "feedback farm" earned a seller a thousand positive reviews over four days. eBay intervenes to some extent to eliminate such gaming, just as Google reserves the right to exact the "Google death penalty" by de-listing any website that it believes is unduly gaming its chances of a high search engine rating.<sup>112</sup>

These reputation systems now stand to expand beyond evaluating people's behavior in discrete transactions or making recommendations on products or content, into rating people more generally. This could happen as an extension of current services: one's eBay rating could be used to determine trustworthiness on, say, another peer-to-peer service. Any downside to allowing its ratings to be deployed elsewhere (such as on competing auction sites), could be significantly outweighed by the benefits of serving as an authoritative purveyor of reputation information. Or, trustworthiness ratings could come directly from social networking: Cyworld is a social networking site that has twenty million subscribers; it is one of the most popular internet services in the

---

systems protect anonymity while fostering reliable transactions); Paul Resnick and Richard Zeckhauser, *Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System*, 11 *Advances Applied Microecon* 127 (2002), available at <<http://www.si.umich.edu/~presnick/papers/ebayNBER/RZNBERBodegaBay.pdf>> (last visited Feb 23, 2008) (noting that eBay's system and others appear to work, probably with help from norms drawn from outside the online context); Chrysanthos Dellarocas, *The Digitization of Word-of-Mouth: Promise and Challenges of Online Feedback*, 49 *Mgmt Sci* 1407, 1418–21 (2003) (noting several ways that users can game the system, including changing their user name after receiving a bad rating).

<sup>111</sup> Ina Steiner, *eBay "Feedback Farms" Planted with One-Cent eBooks*, Auction-Bytes.com (Oct 3, 2006), available at <<http://www.auctionbytes.com/cab/abn/y06/m10/i03/s02>> (last visited Feb 23, 2008).

<sup>112</sup> For example, at one point Google de-listed BMW for creating dummy web pages with key words in order to raise the ranking of its central website. See *BMW Given Google "Death Penalty"*, BBC News (Feb 6, 2006), available at <<http://news.bbc.co.uk/2/hi/technology/4685750.stm>> (last visited Feb 23, 2008). Google, however, quickly showed mercy and re-listed the site just three days later, casting some doubt on the effectiveness of the system when the perpetrator is an influential and important website. See Danny Sullivan, *Welcome Back to Google, BMW—Missed You These Past Three Days*, SearchEngineWatch.com (Feb 8, 2006), available at <<http://blog.searchenginewatch.com/blog/060208-104027>> (last visited Feb 23, 2008).

world, largely thanks to interest in South Korea.<sup>113</sup> The site has its own economy, with about \$100 million worth of “acorns,” Cyworld’s currency, sold in 2006.<sup>114</sup>

Not only does Cyworld have a financial market, but it also has a market for reputation. Cyworld includes rating and behavior monitoring systems that make it so that users can see a constantly updated score for “sexiness,” “fame,” “friendliness,” “karma,” and “kindness.” As people interact with each other, they try to maximize the kinds of behaviors that augment their ratings in the same way that many websites try to figure out how best to optimize their presentation for a high Google ranking.<sup>115</sup> People’s worth is defined and measured precisely, if not accurately, by the reactions of others. That trend is increasing as social networking takes off, partly due to the extension of online social networks beyond the people a user already knows personally as they “befriend” their friends’ friends’ friends.

The whole-person ratings of social networks like Cyworld will eventually be available in the real world. Similar real world reputation systems already exist in embryonic form. Law professor Lior Strahilevitz has written a fascinating monograph on the effectiveness of “How’s My Driving” programs, where commercial vehicles are emblazoned with bumper stickers encouraging other drivers to report poor driving.<sup>116</sup> He notes that such programs have resulted in significant accident reductions, and analyzes

<sup>113</sup> Cyworld allows its users to decorate their pages by renting various digital accoutrements. While one’s home page has the metaphor of a physical home, every digital item within the home is rented rather than purchased. See Deborah Cameron, *Koreans Cybertrip to a Tailor-Made World*, *The Age* (May 9, 2005), available at <<http://www.theage.com.au/articles/2005/05/06/115092684512.html>> (last visited Feb 24, 2008) (“Instead of real money the Cyworld currency is dotori, which is Korean for acorn. An acorn costs 100 won (about 12 cents) . . . Something small from the online shop might cost three acorns but a more average purchase costs 10 acorns and something elaborate might set him back 20 acorns. The ‘rent’ for some items has to be paid each month or they disappear.”). This reasoning might similarly apply to Second Life, another popular Internet-based virtual world.

<sup>114</sup> Cho Jin-seo, *Cyworld Members Reach 20 Mil.*, *Korea Times* (Feb 5, 2007), available at <[http://search.hankooki.com/times/times\\_view.php?term=cyworld++&path=hankooki3/times/lpage/tech/200702/kt2007020519364411810.htm&media=kt](http://search.hankooki.com/times/times_view.php?term=cyworld++&path=hankooki3/times/lpage/tech/200702/kt2007020519364411810.htm&media=kt)> (last visited Feb 23, 2008) (stating sales of “100 billion won” in 2006, converting to approximately \$100 million).

<sup>115</sup> See Jennifer Park, *“I Was a Cyholic, a Cyworld Addict,”* *OhmyNews* (July 26, 2004), available at <[http://english.ohmynews.com/articleview/article\\_view.asp?menu=c10400&no=179108&rel\\_no=1&back\\_url](http://english.ohmynews.com/articleview/article_view.asp?menu=c10400&no=179108&rel_no=1&back_url)> (last visited Feb 23, 2008) (noting the incentive to buy decorations for your virtual room in hopes of increasing ratings such as “popularity” and “fame”).

<sup>116</sup> See Lior Jacob Strahilevitz, *“How’s My Driving?” for Everyone (and Everything?)*, 81 *NYU L Rev* 1699 (2006).



what might happen if the program were extended to all drivers.<sup>117</sup> A technologically sophisticated version of the scheme dispenses with the need to note a phone number and file a report; one could instead install transponders in every vehicle and distribute TiVo-like remote controls with “thumbs up” and “thumbs down” ratings buttons to drivers, cyclists, and pedestrians. If someone acts politely, say by allowing you to switch lanes, you can acknowledge such politeness with a digital thumbs-up that is recorded on that driver’s record. Cutting someone off in traffic earns a thumbs-down from the victim and other witnesses. Strahilevitz is supportive of such a scheme, and he surmises it could be even more effective than eBay’s ratings for online transactions since vehicles are registered by the government, making it far more difficult to escape poor ratings tied to one’s vehicle. He acknowledges some worries: people could give thumbs-down to each other for reasons unrelated to their driving—racism, for example. Perhaps a bumper sticker expressing support for Republicans would earn a thumbs-down in a blue state. Strahilevitz counters that the reputation system could be made to eliminate “outliers,” so presumably only well-ensconced racism across many drivers would end up affecting one’s ratings. According to Strahilevitz, this system of peer judgment would pass constitutional muster if challenged, even if the program is run by the state, because driving does not implicate one’s core rights. “How’s My Driving?” systems are too minor to warrant extensive judicial review. But driving is only the tip of the iceberg.

Imagine entering a café in Paris with one’s personal digital assistant or mobile phone, and being able to query: “Is there anyone on my buddy list within 100 yards? Are any of the ten closest friends of my ten closest friends within 100 yards?” Although this may sound fanciful, it could quickly become mainstream. With reputation systems already advising us on what to buy, why not have them also help us make the first cut on whom to meet, to date, to befriend? These are not difficult services to offer, and there are precursors today.<sup>118</sup> These systems can indicate who

---

<sup>117</sup> See *id.*

<sup>118</sup> For example, *dodgeball.com* combines online friend lists and cell-phone text messaging to allow users to advertise their whereabouts to friends, see when they are near friends of friends, and even see when their crushes are nearby. See <<http://www.dodgeball.com/>> (last visited Feb 23, 2008). *Loopt.com* offers a similar service. See *Loopt.com*, *Live in It*, available at <<https://loopt.com/loopt/sess/index.aspx>> (last visited Feb 23, 2008) (“[T]urn [ ] your mobile phone into a social compass”). *Meetro.com* helps users chat over the Internet and connect with other Meetro users who live nearby. See *Meetro*, *What Is Meetro?*, available at <<http://meetro.com/>> (last visited Feb 23, 2008).

has not offered evidence that he or she is safe to meet—as is currently solicited by some online dating sites—or it may use Amazon.com-style matching to tell us which of the strangers who have just entered the café is a good match for people who have the kinds of friends we do. People can rate their interactions with each other (and change their votes later, so they can show their companion a thumbs-up at the time of the meeting and tell the truth later on), and those ratings will inform future suggested acquaintances. With enough people adopting the system, the act of entering a café can be different from one person to the next: for some, the patrons may shrink away, burying their heads deeper in their books and newspapers. For others, the entire café may perk up upon entrance, not necessarily knowing who it is but having a lead that this is someone worth knowing. Those who do not participate in the scheme at all will be as suspect as brand new buyers or sellers on eBay.

Increasingly, difficult-to-shed indicators of our identity will be recorded and captured as we go about our daily lives and enter into routine transactions. Our fingerprints may be used to log into our computers or verify our bank accounts, our photo may be snapped and tagged many times a day, or our license plate may be tracked as people judge our driving habits. The more our identity is associated with our daily actions, the greater opportunities others will have to offer judgments about those actions. A government-run system like the one Strahilevitz recommends for assessing driving is the easy case. If the state is the record-keeper, it is possible to structure the system so that citizens can know the basis of their ratings, such as where (if not by whom) various thumbs-down clicks came from. The state can give a chance for drivers to offer an explanation, excuse, or follow up. The state's formula for meting out fines or other penalties to poor drivers would be known ("three strikes and you're out," for whatever other problems it has, is an eminently transparent scheme), and it could be adjusted through accountable processes the way that legislatures already determine what constitutes illegal acts and what range of punishment they should earn.

Generatively-grown but comprehensively popular unregulated systems are much trickier. The more that we rely upon the judgments offered by these private systems, the more harmful mistakes can be.<sup>119</sup> Correcting or identifying mistakes can be

---

<sup>119</sup> One prominent recent example is found in the Seattle-based start-up Avvo, which provides ratings for attorneys. An opaque system that generated low ratings for some

difficult if the systems are operated entirely by private parties and their ratings formulas are closely held trade secrets. Search engines are notoriously resistant to discussing how their rankings work, in part to avoid gaming—a form of security through obscurity.<sup>120</sup> The most popular engines reserve the right to intervene in their automatic rankings processes, such as by administering the Google death penalty, but otherwise suggest that they do not manually adjust results. Hence a search in Google for “Jew” returns an anti-Semitic website as one of its top hits,<sup>121</sup> as well as a separate sponsored advertisement from Google itself explaining that its rankings are automatic.<sup>122</sup> But while the observance of such policies could limit worries of bias to search algorithm design rather than to the case-by-case prejudices of search-engine operators, it does not address user-specific biases that may emerge from personalized judgments.

Amazon’s automatic recommendations also make mistakes; for a period of time the *Official Lego Creator Activity Book* was paired with a “perfect partner” suggestion: *American Jihad: The Terrorists Living Among Us Today*.<sup>123</sup> If such mismatched pairings happen when discussing people rather than products, rare mismatches could have broader effects while being no more noticeable since they are not universal. The kinds of search systems that say which people are worth getting to know and which should be avoided, tailored to the users querying the system, present a set of due process problems far more complicated than a state-operated system or, for that matter, any system operated by a single party, since there is no public entity to hold to account. The generative capacity to share data and to create mash-

---

prompted offended lawyers to consider pressing for damages to their practices. See John Cook, *Avvo’s Attorney Rating System Draws Fire*, *Seattlepi.com* (June 8, 2007), available at <<http://blog.seattlepi.nwsource.com/venture/archives/116417.asp#extended>> (last visited Feb 24, 2008).

<sup>120</sup> Gasser, *Regulating Search Engines*, 8 Yale J L & Tech at 232–33 (cited in note 103) (observing that search algorithms are often trade secrets).

<sup>121</sup> See Judit Bar-Ilan, *Web Links and Search Engine Ranking: The Case of Google and the Query “Jew,”* 57 J Am Socy for Info Sci & Tech 1581, 1582 (2006) (“the top result for the query “Jew” on Google was a highly anti-Semitic site called Jew Watch”).

<sup>122</sup> See Google, *An Explanation of Our Search Results*, available at <<http://www.google.com/explanation.html>> (last visited Feb 24, 2007) (“If you recently used Google to search for the word ‘Jew,’ you may have seen results that were very disturbing. We assure you that the views expressed by the sites in your results are not in any way endorsed by Google.”).

<sup>123</sup> See <<http://www.amazon.co.uk/exec/obidos/ASIN/1566868351/026-5666135-0354819>> (last visited March 24, 2003).

ups means that ratings and rankings can be far more emergent and far more inscrutable.

#### IV. SOLVING THE PROBLEMS OF PRIVACY 2.0

Cheap sensors generatively wired to cheap networks with cheap processors are transforming the nature of privacy. How can we respond to the notion that nearly anything we do outside our homes can be monitored and shared? How do we deal with systems that offer judgments about what to read or buy, and whom to meet, when they are not channeled through a public authority or through something as suable, and therefore as accountable, as Google?

The central problem is that the organizations creating, maintaining, using, and disseminating records of identifiable personal data are no longer just “organizations”—they are collections of far-flung 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. These databases are becoming as powerful as the ones large institutions populate and centrally define. Yet the sorts of administrative burdens we can reasonably place on established firms exceed those we can place on individuals—at some point, the burden of compliance becomes so great that the administrative burdens are tantamount to an outright ban. That is one reason why so few radio stations are operated by individuals: it need not be capital intensive to set up a radio broadcasting tower—a low-power neighborhood system could easily fit in someone’s attic—but the administrative burdens of complying with telecommunications law are well beyond the abilities of a regular citizen. Similarly, we could create a privacy regime so complicated as to frustrate generative developments by individual users.

The 1973 U.S. government report on privacy crystallized the template for Privacy 1.0, suggesting five elements of a code of fair information practice:

- There must be no personal data record keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose

from being used or made available for other purposes without his consent.

- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.<sup>124</sup>

These recommendations present a tall order for distributed, generative systems. It may seem clear that the existence of personal data record-keeping systems ought not to be kept secret. However, this issue was easier to address in 1973, when such systems were typically large consumer credit databases or government dossiers about citizens, which could more readily be capable of being disclosed and advertised by the relevant parties. It is harder to apply the anti-secrecy maxim to distributed personal information databases. We live in an age in which many of us privately maintain records or record fragments on one another. Through peer-produced social networking services like Facebook or MySpace, we share these records with thousands of others, or allow them to be indexed to create powerful mosaics of personal data. In this age, exactly what the database *is* changes from one moment to the next—not simply in terms of its contents, but its very structure and scope. Such databases may be generally unknown while not truly “secret.”<sup>125</sup>

Further, these databases are ours. It is one thing to ask a corporation to disclose the personal data and records it maintains; it is far more intrusive to demand such a thing of private citizens. Such disclosure may itself constitute an intrusive search upon the citizen maintaining the records. Similarly, the idea of mandating that an individual be able to find out what an information gatherer knows—much less to correct or amend the information—is categorically more difficult to implement when what is known is distributed across millions of people’s technological outposts. To be sure, we can Google ourselves, but this

---

<sup>124</sup> Advisory Committee, *Records, Computers, and the Rights of Citizens* § III (cited in note 2).

<sup>125</sup> See Pamela Samuelson, *Five Challenges for Regulating the Global Information Society*, in Chris Marsden, ed., *Regulating the Global Information Society* 316, 321–22 (Routledge 2000) (describing how technological developments threaten existing means for protecting traditional values such as “privacy, innovation, and freedom of expression”).

does not capture those databases open only to “friends of friends”—a category that may not include us but may include thousands of others. At the same time, we may have minimal recourse when the information we thought we were circulating within social networking sites merely for fun and, say, only among fellow college students, ends up leaking to the world at large.<sup>126</sup> What to do?

#### A. The Power of Code-Backed Norms

The Web is disaggregated. Its pieces are bound together into a single virtual database by private search engines like Google. Google and other search engines assign digital robots to crawl the Web as if they were peripatetic Web surfers, clicking on one link after another, recording the results, and placing them into a concordance that can then be used for search.<sup>127</sup>

Early on, some wanted to be able to publish material to the Web without it appearing in search engines. In the way a conversation at a pub is a private matter unfolding in a public (but not publicly owned) space, these people wanted their sites to be private but not secret. The law could offer one approach to vindicate this desire for privacy but not secrecy. It could establish a framework delineating the scope and nature of a right in one’s website being indexed, and providing for penalties for those who infringe that right. An approach of this sort has well-known pitfalls. For example, it would be difficult to harmonize such doctrine across various jurisdictions around the world,<sup>128</sup> and there would be technical questions as to how a website owner could signal his or her choice to would-be robot indexers visiting the site.

The internet community, however, fixed most of the problem before it could become intractable or even noticeable to mainstream audiences. A software engineer named Martijn Koster was among those discussing the issue of robot signaling on a

---

<sup>126</sup> It does not just happen on social networking sites; constitutional law scholar Laurence Tribe was distressed when a statement he posted on a family Web site became the subject of public attention. See Jeffrey Rosen, *Unwanted Gaze* 164–65 (cited in note 48).

<sup>127</sup> Nancy Blachman and Jerry Peek, *How Google Works*, available at <[http://www.googleguide.com/google\\_works.html](http://www.googleguide.com/google_works.html)> (last visited Feb 24, 2008) (“Googlebot is Google’s web crawling robot, which finds and retrieves pages on the web and hands them off to the Google indexer.”).

<sup>128</sup> See Samuelson, *Five Challenges* at 323–24 (cited in note 125) (arguing that given the tediously slow nature of the harmonization process, nations may generally be better off seeking not complete harmonization, but “policy interoperability,” broad agreement on goals that allow room for flexible implementation of those goals at a later date).

public mailing list in 1993 and 1994. Participants, including “a majority of robot authors and other people with an interest in robots,” converged on a standard for “robots.txt,” a file that web-site authors could create that would be inconspicuous to Web surfers but in plain sight to indexing robots.<sup>129</sup> Through robots.txt, site owners can indicate preferences about what parts of the site ought to be crawled and by whom. Consensus among some influential Web programmers on a mailing list was the only blessing this standard received:

It is not an official standard backed by a standards body, or owned by any commercial organisation. It is not enforced by anybody, and there [sic] no guarantee that all current and future robots will use it. Consider it a common facility the majority of robot authors offer the WWW community to protect WWW server [sic] against unwanted accesses by their robots.<sup>130</sup>

Today, nearly all Web programmers know robots.txt is the way in which sites can signal their intentions to robots, and these intentions are voluntarily respected by every major search engine across differing cultures and legal jurisdictions.<sup>131</sup> On this potentially contentious topic—search engines might well be more valuable if they indexed everything, *especially* content marked as something to avoid—harmony was reached without any application of law. The robots.txt standard did not address the legalities of search engines and robots; it merely provided a way to defuse

---

<sup>129</sup> Martijn Koster, *A Standard for Robot Exclusion*, available at <<http://www.robotstxt.org/wc/norobots.html>> (last visited Feb 24, 2008) (detailing the genesis of robots.txt).

<sup>130</sup> *Id.*

<sup>131</sup> See, for example, Yahoo!, *How Do I Prevent You from Indexing Certain Pages*, available at <<http://help.yahoo.com/l/us/yahoo/search/webcrawler/slurp-04.html>> (last visited Feb 24, 2008) (showing how to prevent indexing on Yahoo by alerting robots through directives like robots.txt); MSN Search, *Site Owner Help: Control Which Pages of Your Website Are Indexed*, available at <[http://search.msn.com.sg/docs/siteowner.aspx?t=SEARCH\\_WEBMASTER\\_REF\\_RestrictAccessToSite.htm](http://search.msn.com.sg/docs/siteowner.aspx?t=SEARCH_WEBMASTER_REF_RestrictAccessToSite.htm)> (last visited Feb 24, 2008) (showing how to prevent indexing on MSN Search by using a robots.txt file); Baidu, <<http://www.baidu.com/search/robots.html>> (last visited Feb 24, 2008) (showing use of robots.txt on foreign search engines); Google, *How Do I Request that Google Not Crawl Parts or All of My Site?*, available at <<http://www.google.com/support/webmasters/bin/answer.py?answer=33570&topic=8846>> (last visited Feb 24, 2008) (“[R]obots.txt is a standard document that can tell Googlebot not to download some or all information from your web server.”). For a general discussion, see Google, *Controlling How Search Engines Access and Index Your Website*, available at <<http://googleblog.blogspot.com/2007/01/controlling-how-search-engines-access.html>> (last visited Feb 24, 2008) (explaining robots and metatags).

many conflicts before they could even begin. The apparent legal vulnerabilities of robots.txt, namely its lack of ownership, its want for the backing of a large private standards-setting organization (let alone official backing), and the absence of private enforcement devices, may have been essential to its success. Scholars have written about the increasingly important role played by private organizations in the formation of standards across a wide range of disciplines and the ways in which some organizations incorporate governmental notions of due process in their activities.<sup>132</sup> Many internet standards have been forged much less legalistically but still cooperatively.<sup>133</sup>

The questions not preempted or settled by such cooperation tend to be clashes between firms with some income stream in dispute—and where the law has then partially weighed in. For example, eBay sued data aggregator Bidder's Edge for using robots to scrape its site even after eBay clearly objected both in person and through robots.txt.<sup>134</sup> eBay won in a case that has made it singularly into most cyberlaw casebooks and even into a few general property casebooks—a testament to how rarely such disputes enter the legal system.<sup>135</sup>

Similarly, the safe harbors of the Digital Millennium Copyright Act of 1998 give some protection to search engines that point customers to material that infringes copyright,<sup>136</sup> but they

---

<sup>132</sup> See Jody Freeman, *The Private Role in Public Governance*, 75 NYU L Rev 543, 547 (2000) (exploring the increase in private participation in traditionally public governance, where "[n]ongovernmental actors perform 'legislative' and 'adjudicative' roles, along with many others, in a broad variety of regulatory contexts"). See also Pamela Samuelson, *Questioning Copyright in Standards*, 48 BC L Rev 193, 193 (2007) (describing the uniform standards underpinning the information society as "an integral part of the largely invisible infrastructure of the modern world," and offering a thorough analysis of why and how courts should resist placing these standards under the scope of U.S. copyright protection); Mark A. Lemley, *Intellectual Property Rights and Standard-Setting Organizations*, 90 Cal L Rev 1889, 1901 (2000) (noting the importance of standard-setting organizations, or private industry groups, in adopting, or failing to adopt, standards covered by intellectual property rights based on formal and informal rules).

<sup>133</sup> See A. Michael Froomkin, *Habermas@Discourse.net: Toward a Critical Theory of Cyberspace*, 116 Harv L Rev 749, 777–96 (2003) (discussing the evolution of internet standards setting).

<sup>134</sup> See *Ebay, Inc v Bidder's Edge*, 100 F Supp 2d 1058, 1063 (N D Cal 2000) ("eBay now moves for preliminary injunctive relief preventing BE from accessing the eBay computer system . . .").

<sup>135</sup> See *id* at 1073 ("[Bidder's Edge] are hereby enjoined pending the trial of this matter, from using any automated query program, robot, web crawler or other similar device, without written authorization, to access eBay's computer systems or networks, for the purpose of copying any part of eBay's auction database.").

<sup>136</sup> 17 USC § 512(d) (2000) (shielding service providers from monetary liability upon certain conditions).



do not shield the actions required to create the search database in the first place. The act of creating a search engine, like the act of surfing itself, is something so commonplace that it would be difficult to imagine deeming it illegal. Nevertheless, this is not to say that search engines rest on any stronger of a legal basis than the practice of using robots.txt to determine when it is and is not appropriate to copy and archive a website.<sup>137</sup> Only recently, with Google's book scanning project, have copyright holders really begun to test this kind of question.<sup>138</sup> That challenge has arisen over the scanning of paper books, not websites, as Google prepares to make them searchable in the same way Google has indexed the Web.<sup>139</sup> The longstanding practice of website copying, guided by robots.txt, made that kind of indexing uncontroversial even as it is, in theory, legally cloudy.

The lasting lesson from robots.txt is that a simple, basic standard created by people of good faith can go a long way toward resolving or forestalling a problem containing strong ethical or legal dimensions. The founders of Creative Commons created an analogous set of standards to allow content creators to indicate how they would like their works to be used or reused. Creative Commons licenses purport to have the force of law behind them: one ignores them at the peril of infringing copyright. Yet the main force of Creative Commons as a movement has not been in the courts, but in cultural mindshare: alerting authors to basic but heretofore hidden options they have for allowing use of the photos, songs, books, or blog entries they create, and alerting those who make use of the materials to the general orientation of the author.

Creative Commons is robots.txt generalized. Again, the legal underpinnings of this standard are not particularly strong. For example, one Creative Commons option is "noncommercial," which allows authors to indicate that their material can be re-

---

<sup>137</sup> Google prevailed, on a particularly favorable fact pattern, against one author-plaintiff challenging the search engine's copying and distribution of his copyrighted works. See *Field v Google*, 412 F Supp 2d 1106, 1118–19 (D Nev 2006) (finding Google's copying and distribution of the copyrighted works through cached links to be a fair use on grounds that offering access through its cache serves important social purposes and transforms rather than supersedes the original authors' uses).

<sup>138</sup> See Complaint, *McGraw-Hill Companies, Inc. v Google*, No 05-CV-8881, 2005 WL 2778878, at \*2 (S D NY Oct 19, 2005) (alleging that Google's Library Project is violating plaintiffs' copyrights of the scanned books).

<sup>139</sup> See Complaint, *Author's Guild v Google*, No 05-CV-8136, 2006 WL 4058866, at \*2 (S D NY Dec 20, 2005) (alleging that Google's contracting to create digital archives of libraries' collections is massive copyright infringement).

used without risk of infringement so long as the use is noncommercial. But the definition of noncommercial is a model of vagueness, the sort of definition that could easily launch a case like *eBay v Bidder's Edge*.<sup>140</sup> If one aggregates others' blogs on a page that has banner ads, is that a commercial use? There have been only a handful of cases over Creative Commons licenses, and none testing the meaning of noncommercial.<sup>141</sup> Rather, people seem to know a commercial (or derivative) use when they see it: the real power of the license may have less to do with a threat of legal enforcement and more to do with the way it signals one's intentions and asks that they be respected. Reliable empirical data is absent, but the sense among many of those using Creative Commons licenses is that their wishes have been respected.<sup>142</sup>

---

<sup>140</sup> See Creative Commons Legal Code, available at <<http://creativecommons.org/licenses/by-nc-sa/2.5/egalcode>> (last visited Feb 24, 2008) ("You may not exercise any of the rights granted to You . . . in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation.")

<sup>141</sup> In a case brought by Adam Curry against a Dutch tabloid after the tabloid attempted to republish several CC-licensed photos that Curry had posted on Flickr, the District Court of Amsterdam found that "[i]n case of doubt as to the applicability and the contents of the License, [Audax, the tabloid,] should have requested authorization for publication from the copyright holder of the photos (Curry). Audax has failed to perform such a detailed investigation, and has assumed too easily that publication of the photos was allowed. Audax has not observed the conditions stated in the [Attribution-Noncommercial-Sharealike] License . . ." Groklaw, *Creative Commons License Upheld by Dutch Court* (Mar 16, 2006), available at <<http://www.groklaw.net/article.php?story=20060316052623594>> (last visited Feb 24, 2008). However, American law is not nearly so clear. Some commentators have suggested that in the interest of clarifying the enforceability of these rights in the United States, Creative Commons licensors, when faced with some infringement of the rights they have chosen to retain, should file cease and desist letters and force a legal decision on this issue. See Posting of John Palfrey, *Following up on the RSS/Copyright Debate*, available at <<http://blogs.law.harvard.edu/palfrey/2006/07/28/following-up-on-the-rsscopyright-debate>> (last visited Feb 24, 2008). Until then, content publishers may have no way to grapple with the "widespread abuse" and piracy of works published under Creative Commons licenses. See Posting of Ethan Zuckerman to My Heart's in Accra, *Can Creative Commons and Commercial Aggregators Learn to Play Nice?*, available at <<http://www.ethanzuckerman.com/blog/?p=900>> (last visited Feb 24, 2008) ("Unless these licenses get enforced, they won't have teeth."). But see Posting of Mia Garlick to Creative Commons Weblog, *Creative Commons Licenses Enforced in Dutch Court* (Mar 16, 2006), available at <<http://creativecommons.org/weblog/entry/5823>> (last visited Feb 24, 2008) (questioning whether the legitimacy of Creative Commons licenses should depend on judicial validation instead of voluntary recognition of rights between private parties).

<sup>142</sup> To be sure, it may be easy for the wishes expressed in a Creative Commons license to be respected, since nearly every variant of the license is designed to emphasize sharing among peers rather than restrictions. Variants that do not contemplate such sharing—for example, the Founder's Copyright that asserts regular copyright protection but only for a limited term, or Developing Nations, which only relaxes copyright's restrictions for certain states—are used hardly at all. See Creative Commons, *License Statistics*, available at <[http://wiki.creativecommons.org/License\\_statistics](http://wiki.creativecommons.org/License_statistics)> (last visited Feb 24, 2008).

## B. Applying Code-Backed Norms to Privacy: Data Genealogy

As people put data on the internet for others to use or re-use—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. Law professor Pamela Samuelson has proposed that in response to the technical simplicity of collecting substantial amounts of personal information in cyberspace, a person should have a protectable right to control this personal data.<sup>143</sup> She notes that a property-based legal framework is more difficult to impose when one takes into account the multiple interests a person might have in her personal data, and suggests a move to a contractual approach to protecting information privacy based in part on enforcement of website privacy policies.<sup>144</sup> Before turning to law directly, we can develop tools to register and convey authors' privacy-related preferences unobtrusively.

On today's internet, copying and pasting of information takes place with no sense of metadata.<sup>145</sup> It is difficult enough to make sure that a Creative Commons license follows the photograph, sound, or text to which it is related as those items circulate on the Web. But there is no standard at all to pass along for a given work and who recorded it, with what devices,<sup>146</sup> and most important, what the subject is comfortable having others do with it. If there were, links could become two-way. Those who place information on the Web could more readily canvass the public uses to which that information had been put and by whom. In turn, those who wish to reuse information would have a way of getting in touch with its original source to request permission.

---

<sup>143</sup> See, for example, Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stan L Rev 1125, 1172 (2000) (concluding that a contractual approach to protecting privacy is a flexible and realistic solution, especially in cyberspace since websites already have privacy policies that can become "the basis of a contractual understanding between the user and the Web site").

<sup>144</sup> See id at 1170–73.

<sup>145</sup> See Wikipedia, *Metadata*, available at <<http://en.wikipedia.org/wiki/Metadata>> (last visited Feb 25, 2008) ("Metadata are data about data.").

<sup>146</sup> Flickr allows users to record data such as camera-type used, shutter speed, exposure, date, photographer, geotagging data, and viewer comments, see, for example, <<http://www.flickr.com/cameras>> (last visited March 20, 2008). However, no convenient process exists for ensuring that this metadata remains attached to a photo when someone saves it to a hard drive or reposts it on a different site.

Some Web 2.0 outposts have generated promising rudimentary methods for this. Facebook, for example, 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.

The Web is a complex social phenomenon with information contributed not only by institutional sources like *Britannica*, CNN, and others that place large amounts of structured information on it, but also by amateurs like Wikipedians, Flickr contributors, and bloggers. Yet a Google search intentionally smoothes over this complexity; each linked search result is placed into a standard format to give the act of searching structure and order. Search engines and other aggregators can and should do more to enrich users' understanding of where the information they see is coming from. This approach would shadow the way that Ted Nelson, coiner of the word "hypertext," envisioned "transclusion," a means not simply to copy text, but also to reference it to its original source.<sup>147</sup> Nelson's vision was drastic in its simplicity: information would repose primarily at its source, and any quotes to it would simply frame that source. If it were deleted from the original source, it would disappear from its subsequent uses. If it were changed at the source, downstream uses would change with it. This is a strong version of the genealogy idea, since the metadata about an item's origin would actually be the item itself. For the purposes of privacy, we do not need such a radical reworking of the copy-and-paste culture of the Web. Rather, we need ways for people to signal whether they would like to remain associated with the data they place on the Web, and to be consulted about unusual uses.

This weaker signaling-based version of Nelson's vision does not answer the legal question of what would happen if the originator of the data could not come to an agreement with someone who wanted to use it. But as with robots.txt and Creative Commons licenses, it could forestall many of the conflicts that still

---

<sup>147</sup> See Wikipedia, *Transclusion*, available at <<http://en.wikipedia.org/wiki/Transclusion>> (last visited Feb 25, 2008) ("Nelson coined the term 'transclusion,' as well as 'hypertext' and 'hypermedia', in his 1982 book, *Literary Machines*. Part of his proposal was the idea that micropayments could be automatically exacted from the reader for all the text, no matter how many snippets of content are taken from various places."). Consider Ted Nelson, *Literary Machines: The Report on, and of, Project Xanadu Concerning Word Processing, Electronic Publishing, Hypertext, Thinkertoys, Tomorrow's Intellectual Revolution, and Certain Other Topics Including Knowledge, Education and Freedom* (Nelson 1981).

await us in the absence of any standard at all.<sup>148</sup> Most importantly, it would help signal authorial intention not only to end users but also to the intermediaries whose indices provide the engines for invasions of privacy in the first place. One could indicate that photos were okay to index by tag but not by facial recognition, for example. If search engines of today are any indication, such restrictions could be respected even without a definitive answer as to the extent of their legal enforceability. Indeed, by associating one's online identity—if not one's physical identity—with the various bits of data that are constantly mashed up as people copy and paste what they like around the Web, it becomes possible for people to get in touch with one another more readily to express thanks, suggest collaboration, or otherwise interact as people in communities do. Similarly, projects like reCAPTCHA could seek to alert people to the extra good their solving of CAPTCHAs is doing—and even let them opt out of solving the second word in the image, the one that is not testing whether they are human but instead is being used to perform work for someone else. Just as *Moore v Regents of the University of California*<sup>149</sup> struggled with the issue of whether a patient whose tumor was removed should be consulted before the tumor is used for medical research, we will face the question of when people ought to be informed when their online behaviors are used for ulterior purposes, including beneficial ones.

Respect for robots.txt, Creative Commons licenses, and privacy “tags,” coupled with an opportunity to alert people and allow them to opt in to helpful ventures with their routine online behavior like CAPTCHA-solving, require and promote a sense of community. Harnessing some version of Nelson's vision is a self-reinforcing community-building exercise, bringing people closer together while engendering further respect for people's privacy choices. It should be no surprise that people tend to act less charitably in today's online environment than they would act in the physical world.<sup>150</sup> In today's online environment, there are

---

<sup>148</sup> Consider, for example, the Internet Archive. Proprietor Brewster Kahle has thus far avoided what one would think to be an inevitable copyright lawsuit as he archives and makes available historical snapshots of the Web. He has avoided such lawsuits by respecting Web owners' wishes to be excluded as soon as he is notified. See Internet Archive FAQ, available at <<http://www.archive.org/about/faqs.php>> (last visited Feb 25, 2008) (stating that they are “not interested in preserving or offering access to Web sites or other Internet documents of persons who do not want their materials in the collection,” and providing a notice and takedown exclusion policy).

<sup>149</sup> *Moore v Regents of the University of California*, 793 P2d 479, 480 (Cal 1990).

<sup>150</sup> Daniel Goleman, *Normal Social Restraints Are Weakened in Cyberspace*, Intl Her-

few perceived rules, but there are also few ways to receive, and therefore respect, cues from those whose content or data someone might be using.<sup>151</sup> By devising tools and practices to connect distant individuals already building upon one another's data, we can promote the feedback loops found within functioning communities and build a framework to allow Benkler's ideal of "sharing nicely" to blossom.<sup>152</sup>

### C. Enabling Reputation Bankruptcy

As biometric readers become more commonplace in our end-point machines, it will be possible for online destinations routinely to demand unsheddable identity tokens rather than disposable pseudonyms from internet users. Many sites could benefit from asking people to participate with real identities known at least to the site, if not to the public at large. eBay, for one, would certainly profit by making it harder for people to shift among various ghost accounts. One could even imagine Wikipedia establishing a "fast track" for contributions if they were done with biometric assurance, just as South Korean citizen journalist newspaper OhmyNews keeps citizen identity numbers on file for the articles it publishes.<sup>153</sup> These architectures protect one's identity from the world at large while still making it much more difficult to produce multiple false "sock puppet" identities. When we participate in other walks of life—school, work, PTA meetings, and so on—we do so as ourselves, not wearing Groucho mustaches, and even if people do not know exactly who we are,

---

ald Trib (Feb 20, 2007), available at <<http://www.iht.com/articles/2007/02/20/business/email.php>> (last visited Feb 25, 2008) (explaining the psychological basis for less stringent standards of behavior on cyberspace). For a somewhat contrary view of online behavior, see Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 Va L Rev 505, 549–75 (2003) (discussing how cooperation and the social norm of reciprocity impact online behavior).

<sup>151</sup> See John Suler, *The Online Disinhibition Effect*, 7 CyberPsych & Beh 321, 322 (2004) (noting how not having facial feedback with those we are addressing online allows us to ignore negative emotional responses to our statements).

<sup>152</sup> See Yochai Benkler, *Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production*, 114 Yale L J 273, 279 (2004) (noting the economic significance of sharing between weakly-related private parties as an alternative to market-based production and the desirability of preserving this social practice).

<sup>153</sup> See Jonathan L. Zittrain, *Private is the New Public*, in Ed Richards, Robin Foster, and Tom Kiedrowski, eds, *Communications: The Next Decade* 51, 61 (Ofcom 2006) (identifying the trend of having "anonymous" contributors be partially identifiable through a method like Ohmynew's national identity number—if not by name—to allow for reputation systems).

they can recognize us from one meeting to the next. The same should be possible for our online selves.

As real identity grows in importance on the Net, the intermediaries demanding it ought to consider making available a form of reputation bankruptcy. Like personal financial bankruptcy, or the way in which a state often seals a juvenile criminal record and gives a child a “fresh start” as an adult,<sup>154</sup> we ought to consider how to implement the idea of a second or third chance in our digital spaces. People ought to be able to express a choice to deemphasize if not entirely delete older information that has been generated about them by and through various systems: political preferences, activities, youthful likes and dislikes. If every action ends up on one’s “permanent record,” the press conference effect can set in. Reputation bankruptcy has the potential to facilitate desirable, experimental social behavior and break up the monotony of static communities online and offline.<sup>155</sup> As a safety valve against excess experimentation, perhaps the information in one’s record could not be deleted selectively; if someone wants to declare reputation bankruptcy, we might want it to mean throwing out the good along with the bad.<sup>156</sup> The blank spot in one’s history would indicate a bankruptcy has been declared. This blank spot would be the price one pays for eliminating unwanted details.

The key is to realize that we can make design choices now that work to capture the nuances of human relations far better than our current systems, and that online intermediaries might well embrace such new designs even in the absence of a legal mandate to do so.

#### D. More, Not Less, Information

Reputation bankruptcy provides for the possibility of a clean slate. It works best within hermetic systems that generate their own data through the activities of their participants, such as social networking sites that record who is friends with whom, or

---

<sup>154</sup> See, for example, Va Code Ann § 16.1-306 (Michie 2008); CRSA §19-1-306.

<sup>155</sup> Compare, for example, *Local Loan Co v Hunt*, 292 US 234, 244 (1934) (noting that providing debtors with a clean slate is “[o]ne of the primary purposes of the Bankruptcy Act”); Thomas H. Jackson, *The Fresh-Start Policy in Bankruptcy Law*, 98 Harv L Rev 1393 (1985) (arguing that a nonwaivable right of discharge is justified).

<sup>156</sup> For example, eBay might allow users to delete their full feedback histories, but prohibit selective deletion of negative reviews.

that accumulate the various thumbs-up and thumbs-down arrays that could be part of a "How's My Driving" style judgment.

But the use of the internet more generally to spread real-world information about people is not amenable to reputation bankruptcy. Once injected into the Net, an irresistible video of an angry teacher, or a drunk and/or racist celebrity, cannot be easily stamped out without the kinds of network or endpoint control that are both difficult to implement and, if implemented, unacceptably corrosive to the generative internet. What happens if we accept this as fact, and also assume that legal proscriptions against disseminating sensitive but popular data will be largely ineffective?<sup>157</sup> We might turn to contextualization: the idea, akin to the tort of false light, that harm comes from information plucked out of the rich thread of a person's existence and expression.<sup>158</sup> We see this in political controversies: even the slightest misphrasing of something can be extracted and blown out of proportion. It is the reason that official press conferences are not the same as bland conversation; they are even blander.

Contextualization suggests that the aim of an informational system should be to allow those who are characterized within it to augment the picture provided by a single snippet with whatever information, explanation, or denial that they think helps frame what is portrayed. Civil libertarians have long suggested that the solution to bad speech is more speech while realizing the difficulties of linking the second round of speech to the first without infringing the rights of the first speaker.<sup>159</sup> Criticisms of the "more speech" approach have included the observation that a retraction or amendment of a salacious newspaper story usually appears much less prominently than the original. This is particularly true for newspapers, where those seeing one piece of infor-

---

<sup>157</sup> Such proscriptions may also prove difficult to reconcile with constitutional frameworks. See, for example, Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan L Rev 1049, 1051 (2000) ("While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.").

<sup>158</sup> See Jeffery Rosen, *Unwanted Gaze* 158 (cited in note 48) (stating that "we have fewer opportunities to present ourselves publicly in all of our complexity. Therefore, as more of our private lives are recorded in cyberspace, the risk that we will be unfairly defined by isolated pieces of information that have been taken out of context has increased dramatically.").

<sup>159</sup> See, for example, Richard Delgado and Jean Stefancic, *Understanding Words That Wound* 207 (Westview 2004) (noting that while some have argued that "[t]he cure for bad speech is more speech," a problem arises from the fact that "hate speech is rarely an invitation to dialogue; it is like a slap in the face").



mation may not ever see the follow-up. There is also the worry that the fog of information generated by a free-for-all is no way to have people discern facts from lies. Generative networks invite us to find ways to reconcile these views. We can design protocols to privilege those who are featured or described online so that they can provide their own framing linked to their depictions. This may not accord with our pre-Web expectations: it may be useful for a private newspaper to provide a right of reply to its subjects, but such an entity would quickly invoke a First Amendment style complaint of compelled speech if the law were to provide for routine rights of reply in any but the narrowest of circumstances.<sup>160</sup> And many of us might wish to discuss Holocaust deniers or racists without giving them a platform to even link to a reply. The path forward is likely not a formal legal right but a structure to allow those disseminating information to build connections to the subjects of their discussions. In many cases those of us disseminating may not object, and a properly designed system might turn what would have otherwise been one-sided exchanges into genuine dialogues.

We already see some movement in this direction. The Kennedy School's Joseph Nye has suggested that a site like urban legend debunker snopes.com be instituted for reputation, a place that people would know to check to get the full story when they see something scandalous but decontextualized online.<sup>161</sup> The subjects of the scandalous data would similarly know to place their answers there, perhaps somewhat mitigating the need to link it formally to each instance of the original data. Google in-

---

<sup>160</sup> This kind of compelled speech would not be unprecedented. For much of the twentieth century, the FCC's Fairness Doctrine forced broadcasters to air controversial public interest stories and provide opposing viewpoints on those issues. See Steve Rendall, *The Fairness Doctrine: How We Lost It and Why We Need It Back*, Extra! (Jan/Feb 2005), available at <<http://www.fair.org/index.php?page=2053>> (last visited Feb 25, 2008) (outlining the history, rationale, and workings of the Fairness Doctrine). Under President Reagan, the FCC repealed this doctrine in 1987. *Id.* Despite this administrative change, the Supreme Court has consistently interpreted the First Amendment to include the right *not* to speak in a line of compelled speech cases. See, for example, *Keller v State Bar of California*, 496 US 1, 15–16 (1990) (holding that lawyers could not be forced to pay bar association fees to support politicians supporting purely ideological messages with which they disagreed); *Abood v Detroit Board of Education*, 431 US 209, 235–36 (1977) (holding that teachers could not be forced to pay union fees to support political messages with which they disagreed).

<sup>161</sup> Joseph Nye, *Davos Day 3: Internet Privacy and Reputational Repair Sites*, Huffington Post (Jan 26, 2007), available at <[http://www.huffingtonpost.com/joseph-nye/davos-day-3-internet-pri\\_b\\_39750.html](http://www.huffingtonpost.com/joseph-nye/davos-day-3-internet-pri_b_39750.html)> (last visited Feb 25, 2008) ("the virtual world could provide a site where anyone who felt that a quote or picture was out of context or misrepresented, their views could say so for the record.").

vites people quoted or discussed within news stories to offer addenda and clarification directly to Google, which posts it prominently near its link to the story when it is a search result within Google News. Services like reputationdefender.com will, for a fee, take on the task of trying to remove or, failing that, contextualize sensitive information about people online.<sup>162</sup> ReputationDefender uses a broad toolkit of tactics to try to clear up perceived invasions of privacy, mostly moral suasion rather than legal threat.

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 help much. Values of privacy may be implacably in tension with some of the fruits of generativity. Just as the digital copyright problem could be solved if publishers could find a way to profit from abundance rather than scarcity, the privacy problem could be solved if we could take Sun Microsystems CEO McNealy's advice and simply get over it. This is not a satisfying rejoinder to someone whose privacy has been invaded, but, amazingly, this may be precisely what is happening: people are getting over it.

#### E. The Generational Divide: Beyond Informational Privacy

The values animating our concern for privacy are themselves in transition. Many have noted an age-driven gap in attitudes about privacy perhaps rivaled only by the 1960's generation gap on rock and roll.<sup>163</sup> Surveys bear out some of this perception.<sup>164</sup> Fifty-five percent of online teens have created profiles on sites

---

<sup>162</sup> See <<http://www.reputationdefender.com>> (last visited Feb 25, 2007). ReputationDefender was started by a former student of mine, and I once served on its advisory board. The firm has itself been the subject of some controversy. See, for example, Posting of Ann Bartow to Feminist Law Professors, *Well, Those "ReputationDefender" Guys Certainly are Well Connected, Anyway*, (Apr 8, 2007), available at <<http://feministlawprofs.law.sc.edu/?p=1671>> (last visited Feb 25, 2008) (questioning the decision to not invite a representative of AutoAdmit to a ReputationDefender conference at Harvard, where AutoAdmit was specifically mentioned as a topic).

<sup>163</sup> Emily Nussbaum, *Say Everything*, NY Magazine 1-2 (Feb 12, 2007), available at <<http://nymag.com/news/features/27341/>> (last visited Feb 25, 2008) (comparing the modern generation gap between young and old in attitudes on privacy to the differential reception of rock and roll).

<sup>164</sup> People aged fifty to sixty-four are almost twice as likely as young people to worry about privacy online. Pew Research Center for the People and the Press, *Online Newcomers More Middle-Brow, Less Work-Oriented: The Internet News Audience Goes Ordinary* 24 (1999), available at <<http://people-press.org/reports/pdf/72.pdf>> (last visited Feb 25, 2008) ("Young people show the least concern about their privacy (only 17% worry a lot), those aged 50-64 the most (32% worry a lot).").

like MySpace, though sixty-six percent of those use tools that the sites offer to limit access in some way.<sup>165</sup> Teens are more than twice as likely as adult internet users to have a blog.<sup>166</sup> Interestingly, while young people appear eager to share information online, they are more worried than older people about government surveillance.<sup>167</sup> Some also see that their identities may be discovered online, even with privacy controls.<sup>168</sup>

A large part of the personal information available on the Web about those born after 1985 comes from the subjects themselves. People routinely set up pages on social networking sites—in the United States, more than eighty-five percent of university students are said to have an entry in facebook.com—and they impart reams of photographs, views, and status reports about their lives, updated to the minute. Friends who tag other friends in photographs cause those photos to be automatically associated with everyone mentioned, a major step toward the world in which simply showing up to an event is enough to make one's photo and name permanently searchable online in connection with the event.

Worries about such a willingness to place personal information online can be split into two categories. The first is explicitly paternalistic: children may lack the judgment to know when they should and should not share their personal information. As with other decisions that could bear significantly on their lives—signing contracts, drinking, or seeing movies with violent or sexual content—perhaps younger people should be protected from

---

<sup>165</sup> Memorandum from Amanda Lenhart and Mary Madden, Research Fellows, Pew Internet and American Life Project, on Social Networking Websites and Teens: An Overview 5 (Jan 7, 2007), available at <[http://www.pewinternet.org/pdfs/PIP\\_SNS\\_Data\\_Memo\\_Jan\\_2007.pdf](http://www.pewinternet.org/pdfs/PIP_SNS_Data_Memo_Jan_2007.pdf)> (last visited Feb 25, 2008). See also Amanda Lenhart and Mary Madden, *Teens, Privacy & Online Social Networks: How Teens Manage Their Online Identities and Personal Information in the Age of Myspace*, at v (Apr 18, 2007), available at <[http://www.pewinternet.org/pdfs/PIP\\_Teens\\_Privacy\\_SNS\\_Report\\_Final.pdf](http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf)> (last visited Feb 25, 2008) (noting that fifty-three percent of parents of online teens have installed filtering software on home computers to protect their children).

<sup>166</sup> Amanda Lenhart and Mary Madden, *Teen Content Creators and Consumers* 5 (Nov 2, 2005), available at <[http://www.pewinternet.org/pdfs/PIP\\_Teens\\_Content\\_Creation.pdf](http://www.pewinternet.org/pdfs/PIP_Teens_Content_Creation.pdf)> (last visited Feb 25, 2008) ("While one teen in five keeps a blog, about 7% of adult internet users say the same.").

<sup>167</sup> See Justin Berton, *The Age of Privacy: Gen Y Not Shy Sharing Online—But Worries About Spying*, SanFran Chron A1 (May 20, 2006) ("On the one hand, she and millions of citizens under 30 are actively engaging in online exhibitionism without fear of consequences. On the other hand, they seem more concerned than their parents about government eavesdropping in the name of U.S. security.").

<sup>168</sup> Lenhart and Madden, *Teens, Privacy & Online Social Networks* (cited in note 165) (finding that "40% of teens with profiles online think that it would be hard for someone to find out who they are from their profile, but that they could eventually be found online.").

rash decisions that facilitate infringements of their privacy. The second relies more on the generative mosaic concern expressed earlier: people might make rational decisions about sharing their personal information in the short term, but underestimate what might happen to that information as it is indexed, reused, and repurposed by strangers. Both worries have merit, and to the extent that they do we could deploy the tools of intermediary gatekeeping to try to protect people below a certain age until they wise up. This is just the approach of the U.S. Children's Online Privacy Protection Act of 1998 ("COPPA").<sup>169</sup> COPPA fits comfortably but ineffectually within a Privacy 1.0 framework, as it places restrictions on operators of websites and services that knowingly gather identifiable information from children under the age of thirteen: they cannot do so without parental consent. The result is discernable in most mainstream websites that collect data; each now presents a checkbox for the user to affirm that he or she is over thirteen, or asks outright for a birthday or age. The result has been predictable; kids quickly learn simply to enter an age greater than thirteen in order to get to the services they want.<sup>170</sup> It will take levels of intervention that so far seem to exceed the willingness of any jurisdiction to achieve effective limits on the flow of information about kids.<sup>171</sup> The most common scheme to separate kids from adults online is to identify individual network endpoints as used primarily or frequently by kids and then limit what those endpoints can do: PCs in libraries and

---

<sup>169</sup> 15 USC §§ 6502–06 (2000) (regulating the "collection and use of personal information from and about children on the Internet").

<sup>170</sup> The FTC provides updates on COPPA enforcement on its Web page. The agency has filed twelve cases since COPPA was enacted, and only one in the past three years. See FTC, *Privacy Initiatives*, available at <[http://www.ftc.gov/privacy/privacyinitiatives/childrens\\_enf.html](http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html)> (last visited Feb 25, 2008). According to one source, seventy-seven percent of children aged eight to seventeen who were surveyed said they would lie about their age in order to do something they were restricted from doing on a Web site. Isabel Walcott, *Online Privacy and Safety Survey*, available at <<http://web.archive.org/web/20001202110700/http://www.smartgirl.com/press/privacyfindings.html>> (last visited Feb 25, 2008).

<sup>171</sup> The U.S. Children's Online Protection Act and its predecessors also struggled with how to protect kids from receiving information that could be harmful to them, such as pornography that adults have a right to see. The most restrictive approach has been to ask providers of information online to assume that kids are receiving it unless each person accessing can demonstrate possession of a valid credit card. See 47 USC § 231(c)(1) (2000) (shielding providers if they restrict access to harmful materials "by requiring use of a credit card . . ."). This approach was struck down as unconstitutional. *ACLU v Ashcroft*, 322 F3d 240 (3d Cir 2003), *affd and remanded*, 542 US 656 (2004).

public schools are often locked down with filtering software, sometimes due to much-litigated legal requirements.<sup>172</sup>

A shift to tethered appliances, those for which their vendors are privileged to change how they work long after they have left the factory, could greatly lower the costs of discerning age online. Many appliances could be initialized at the time of acquisition with the birthdays of their users, or sold assuming use by children until unlocked by the vendor after receiving proof of age. This is exactly how many tethered mobile phones with internet access are sold,<sup>173</sup> and because they do not allow third-party code they can be much more securely configured to only access certain approved websites. With the right standards in place, PCs could broadcast to every website visited that they have not been unlocked for adult browsing, and such websites could then be regulated through a template like COPPA to restrict the transmission of certain information that could harm the young users. This is a variant of Lessig's idea for a "kid enabled browser,"<sup>174</sup> made much more robust because a tethered appliance is difficult to hack.

These paternalistic interventions assume that people will be more careful about what they put online once they grow up. And even those who are not more careful and regret it have exercised their autonomy in ways that ought to be respected. But the generational divide on privacy appears to be more than the higher carelessness or risk tolerance of kids. Many of those growing up with the internet appear not only reconciled to a public dimension to their lives—famous for at least fifteen people—but eager to launch it. Their notions of privacy transcend the Privacy 1.0 plea to keep certain secrets or private facts under control. In-

---

<sup>172</sup> Children's Internet Protection Act ("CIPA"), Pub L No 106-554, §§ 1701-1741, 114 Stat 2763, 2763A-335 to 2763A-352 (2000), codified as amended at 20 USC § 9134 and 47 USC § 254 (requiring certain schools and libraries to provide internet safety). While one federal court held that the CIPA is unconstitutional, see *American Library Association, Inc v United States*, 201 F Supp 2d 401 (E D Pa 2002), the Supreme Court subsequently reversed that decision and affirmed the Act's constitutionality. See *United States v American Library Association, Inc*, 539 US 194 (2003).

<sup>173</sup> See, for example, Vodafone, *Content Control*, available at <[http://online.vodafone.co.uk/dispatch/Portal/appmanager/vodafone/wrp?\\_nfpb=true&\\_pageLabel=template11&pageID=PAV\\_0024&redirectedByRedirectsImplServletFlag=true](http://online.vodafone.co.uk/dispatch/Portal/appmanager/vodafone/wrp?_nfpb=true&_pageLabel=template11&pageID=PAV_0024&redirectedByRedirectsImplServletFlag=true)> (last visited Feb 25, 2008) (providing an overview of the content control service, limiting access to online content for those under 18 but allowing those over 18 to lift content control by proving their age).

<sup>174</sup> Posting to Furd Log, *Lessig and Zittrain—Pornography and Jurisdiction*, available at <<http://msl1.mit.edu/furdlog/?p=383>> (last visited Feb 25, 2008) ("How about a kid-enabled browser? Parents could set up children's computers, so parents have the burden, instead of the porn consumer.").

stead, by digitally furnishing and nesting within publicly-accessible online environments, they seek to make such environments their own. MySpace, currently the third most popular website in the United States and sixth most popular in the world,<sup>175</sup> is evocatively named: it implicitly promises its users that they can decorate and arrange their personal pages to be expressive of themselves. Nearly every feature of a MySpace home page can be reworked by its occupant, and that is exactly what occupants do, drawing on tools provided by MySpace and developers.<sup>176</sup> This is generativity at work: MySpace programmers creating platforms that can in turn be directed and reshaped by users with less technical talent but more individualized creative energy. The most salient feature of privacy for MySpace users is not secrecy so much as autonomy: a sense of control over their home bases, even if what they post can later escape its confines. Privacy is about establishing a locus which we can call our own without undue intervention or interruption—a place where we can vest our identities. That vesting can happen most directly in a particular location—“your home is your castle”—and, as law professor Margaret Radin explains, it can also happen with objects.<sup>177</sup> She had in mind a ring or other heirloom, but an iPod containing one’s carefully selected music and video can fit the bill as well. Losing such a thing hurts more than the mere pecuniary value of obtaining a fresh one. MySpace pages, blogs, and similar online outposts can be repositories for our identities for which personal control, not secrecy, is the touchstone.

---

<sup>175</sup> Alexa, *Traffic Rankings for Myspace.com*, available at <[http://www.alexa.com/data/details/traffic\\_details?q=&url=myspace.com/](http://www.alexa.com/data/details/traffic_details?q=&url=myspace.com/)> (last visited Feb 25, 2008).

<sup>176</sup> See MySpace.com, *How Do I Add Color, Graphics, & Sound to My Profile Page?*, available at <<http://www.myspace.com/Modules/Help/Pages/HelpCenter.aspx?Category=4&Question=7>> (last visited Feb 25, 2008) (showing how to modify your personal profile on MySpace); David F. Carr, *Inside MySpace.com*, Baseline Magazine (Jan 16, 2007), available at <<http://www.baselinemag.com/c/a/Projects-Networks-and-Storage/Inside-MySpacecom/>> (last visited Feb 25, 2008) (reviewing the history of MySpace.com and its customizability).

<sup>177</sup> See Margaret J. Radin, *Property and Personhood*, 34 Stan L Rev 957, 959–60 (1982) (“Most people possess objects they feel are almost part of themselves. These objects are closely bound up with personhood because of the way we constitute ourselves as continuing personal entities in the world. They may be different as people are different, but some common examples might be a wedding ring, a portrait, an heirloom, or a house . . . The opposite of holding an object that has become part of oneself is holding an object that is perfectly replaceable with other goods of equal market value. One holds such an object for purely instrumental reasons.”).

## V. CONCLUSION

The 1973 U.S. government privacy report observed:

An agrarian, frontier society undoubtedly permitted much less personal privacy than a modern urban society, and a small rural town today still permits less than a big city. The poet, the novelist, and the social scientist tell us, each in his own way, that the life of a small-town man, woman, or family is an open book compared to the more anonymous existence of urban dwellers. Yet the individual in a small town can retain his confidence because he can be more sure of retaining control. He lives in a face-to-face world, in a social system where irresponsible behavior can be identified and called to account. By contrast, the impersonal data system, and faceless users of the information it contains, tend to be accountable only in the formal sense of the word. In practice they are for the most part immune to whatever sanctions the individual can invoke.<sup>178</sup>

Enduring solutions to the new generation of privacy problems brought about by the generative internet will have as their touchstone tools of connection and accountability among the people who produce, transform, and consume personal information and expression: tools to bring about social systems to match the power of the technical one. Today's internet is an uncomfortable blend of the personal and the impersonal. It can be used to build and refine communities and to gather people around common ideas and projects.<sup>179</sup> In contrast, it can also be seen as an impersonal library of enormous scale: faceless users perform searches and then click and consume what they see. Many among the new generation of people growing up with the internet are enthusiastic about its social possibilities. They are willing to put more of themselves into the network and are more willing to meet and converse with those they have never met in person. They may not experience the same divide that Twain observed between our public and private selves. Photos of their drunken exploits on

---

<sup>178</sup> Advisory Committee, *Records, Computers, and the Rights of Citizens* § II (cited in note 2).

<sup>179</sup> PledgeBank, for example, encourages people to take action by exchanging commitments to undertake an activity. See <<http://www.pledgebank.com/>> (last visited Feb 25, 2008) (allowing people to make commitments to act if others join them or otherwise help). Meetup helps people find and arrange events with others who share common interests. See <<http://www.meetup.com/>> (last visited Feb 25, 2008).

facebook.com might indeed hurt their job prospects,<sup>180</sup> but soon those making hiring decisions will themselves have had Facebook pages. The differential between our public and private selves might be largely resolved as we develop digital environments in which views can be expressed and then later revised. Our missteps and mistakes will not be cause to stop the digital presses. Instead the good along with the bad will form part of a dialogue with both the attributes of a small town and a “world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.”<sup>181</sup> Such an environment will not be perfect: there will be Star Wars Kids who wish to retract their private embarrassing moments and who cannot. But it will be better than one without powerful generative instrumentalities, one where the tools of monitoring are held and monopolized by the faceless institutions anticipated and feared in 1973.

---

<sup>180</sup> Similarly, see Alison Doyle, *To Blog or Not to Blog?*, available at <<http://jobsearch.about.com/od/jobsearchblogs/a/jobsearchblog.htm>> (last visited Feb 25, 2008) (“Employees have been fired when their employer construed their blog posts as sharing confidential information, making inappropriate comments about the company, or both.”); Ellen Goodman, Editorial, *The Perils of Cyberbaggage*, Truthdig (Feb 21, 2007), available at <[http://www.truthdig.com/report/item/20070221\\_the\\_perils\\_of\\_cyberbaggage/](http://www.truthdig.com/report/item/20070221_the_perils_of_cyberbaggage/)> (last visited Feb 25, 2008) (noting the resignation of two political campaign volunteers based on comments they made on their blogs); Ellen Goodman, *Two Worlds, Two Women: Bloggers Get Caught Between the Real and the Cyber*, Pittsburgh Post-Gazette B7 (Feb 23, 2007) (same); *MySpace Is Public Space When It Comes to Job Search: Entry Level Job Seekers – It’s Time to Reconsider the Web*, CollegeGrad.com (July 26, 2006), available at <<http://www.collegegrad.com/press/myspace.shtml>> (last visited Feb 25, 2008) (“47% of college grad job seekers who use social networking sites such as MySpace and Facebook have either already changed or plan to change the content of their pages as a result of their job search.”).

<sup>181</sup> John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb 8, 1996), available at <<http://homes.eff.org/~barlow/Declaration-Final.html>> (last visited Feb 25, 2008).



