Towards Zero Net Presence

Terence Lau, University of Dayton
TOWARDS ZERO NET PRESENCE

TERENCE J. LAU *

You have zero privacy anyway. Get over it.
— Scott McNealy, Former CEO, Sun Microsystems

The fantastic power and convenience of digital life has led us to change what we consider private in ways that we can only begin to understand.
— L. Gordon Crovitz, columnist, Wall Street Journal

We cannot make a national privacy policy based on the current pledge of the current CEO of a company.
— Rep. Edward Markey (D-MA)

A snarky insult, embedded in a story or a post, quickly gets traffic; it gets linked to other blogs; and soon it has spread like a sneezy cold through the vast kindergarten of the Web.
— David Denby

Now, those are the two questions that I am very bothered about. I don’t know what the rules ought to be there. That is, do you think that a person can put anything on the Internet? Do you think they can put anything on television even if it attacks, say, the most private things of a private individual?
— Justice Steven Breyer

* Associate Professor, University of Dayton; J.D., Syracuse University.


3 Leslie Cauley, Feel Like Someone’s Watching You? Google’s G1 Makes it Easy to Track Surfing Habits, USA TODAY, Feb. 9, 2009, at 1B.

4 DAVID DENBY, SNARK 10 (2009).

On September 19, 2010, a Rutgers University student sent a message to his Twitter account: “Roommate asked for room till midnight. I went into Molly’s room and turned on my webcam. I saw him making out with a dude. Yay.” Later that night, eighteen-year-old Dharun Ravi turned on his webcam again, and used it to stream his roommate’s intimate encounter live on the Internet. Three days later, his roommate, eighteen-year-old first year student Tyler Clementi posted a note on his Facebook page: “Jumping off the gw bridge sorry.” Witnesses saw a man jump off the George Washington Bridge just before 9 p.m. on September 22, and responding officers discovered a wallet with Mr. Clementi’s identification.

A decade ago, Professor John Eger at San Diego State University warned that “[a]s we rush headlong into a new but uncertain age, it is becoming increasingly clear that in our zeal to promote the marvels of the Internet, we may be seriously eroding the fundamental rights of the average citizen and consumer.” “Abusive scavenging” for information took place long before the Internet existed, but “information of this kind and much more is becoming increasingly available to commercial enterprises in their relentless search for markets, and to governments to satisfy their thirst for personal information, all at the risk of undermining our fundamental rights.” What Eger could not have foreseen was that in ten short years, the Internet would become a place where reputations are damaged, gay teens are outed, outrageous slander is commonplace, and a Supreme Court Justice wonders out loud whether a church can thank God for dead soldiers on its website. The fundamental right to be left alone, even if one

pose a clear and present danger to the survival of America, exposing our nation to the wrath of God . . WBC has conducted . . [demonstrations] at . . over 400 military funerals of troops whom God has killed in Iraq/Afghanistan in righteous judgment against an evil nation.”). The Court ruled in favor of the Westboro Church’s right to protest, deciding the case on March 2, 2011. See Snyder v. Phelps, No. 09-751, 2011 WL 709517 (Mar. 2, 2011).

7 Id.
8 Id.
9 Id.
10 John M. Eger, The Precious Right to be Left Alone, SAN DIEGO UNION-TRIB., Aug. 6, 2000, at G1.
11 Id.
wishes to have nothing to do with the Internet, is as ethereal as morning mist.

In a campaign to warn the public about the implications of a “Total Surveillance Society” where private commercial databases are joined in one database so that information is gathered about American consumers, a few years ago the American Civil Liberties Union published an animation of a fictional phone call of a customer placing an order for pizza in 2010. When the hapless customer attempts to order double-meat special pizzas, he is assessed a $20 charge because medical records indicate high blood pressure and high cholesterol. An agreement with the health care provider allows the pizza company to sell him the meat pies, but he has to sign a liability waiver first. Delivery to an “orange” zone (a neighbor was robbed the day prior) yields a $15 delivery surcharge. When he protests the high charge, the pizza company pulls his credit card bill, and points out to him that he can probably afford the pizzas given his recent purchase of expensive airline tickets to Hawaii. The company then suggests a healthier alternative, since his records indicate he purchased a 42-inch waist pair of pants. Payment is by cash only since his credit cards are maxed out, but the helpful agent points out a coupon in a magazine the customer’s wife subscribes to.

Although 2010 is here and the ACLU’s Total Surveillance Society (or some version of it) has not materialized, much of the information required for it would be built through collection of data in electronic databases that do currently exist. In many instances these databases are built by consumers themselves when they use the Internet for banking, shopping, maintaining social networks, updating health records, and a growing myriad of other personal activity.

As we become more reliant on online services, privacy concerns about how the data collected is used become more

---

13 Id.
14 Id.
15 Id.
16 Id.
17 Id.
18 Id.
pressing. In 2008 alone, the number of data breaches of all kinds reached 656, affecting over 36 million records.\(^\text{19}\) As they tend to be widely reported,\(^\text{20}\) the privacy of financial and medical data tends to receive the bulk of attention from policymakers and academics.\(^\text{21}\)

This Article, on the other hand, traces the privacy concerns raised by the casual use of the Internet (for example, searching, web-based email, blogging, and social networking), an area that has received relatively less attention.\(^\text{22}\) How much does the right to privacy protect the right of citizens to be free of a presence on the Internet? How much liability should lie with citizens to ensure no presence on the Internet if they wish it? What role should website owners and Internet service providers play in censoring speech that infringes on the privacy rights of citizens?

Scholarly attention to these problems has tended to focus on existing remedies. Professor Brenner argues for new criminal laws to address cyberbullying\(^\text{23}\) (a position echoed by Schwartz\(^\text{24}\)), Jameson thinks that a criminal statute prohibiting cyberharassment is needed,\(^\text{25}\) while Moy believes that no new

---


\(^{22}\) Some see the “explosion in data collection” as a “trade-off for convenience and discounts.” Ellen Nakashima, Enjoying Technology’s Conveniences But Not Escaping Its Watchful Eyes, WASH. POST, Jan. 16, 2007, at A1 (listing the data collected on one fifty-six-year-old real estate agent as she moves through her normal day).


statutes are needed in this arena at all.\textsuperscript{26} Professor Lidsky argues that there are not actually any effective remedies for reputational torts such as defamation when the defamation takes place on the Internet,\textsuperscript{27} while Professor Kim believes that existing tort law might provide relief if sufficiently broadened.\textsuperscript{28} Gelman believes in a technological solution wherein anyone who uses the Internet can “express and exercise privacy preferences over uploaded content.”\textsuperscript{29} She believes that allowing users to tag content with preferences will allow existing privacy torts to evolve to “take account of individual privacy expectations.”\textsuperscript{30} In the school speech arena, Professor Backus concurs, arguing that schools should “embrace the teachable moment to stop cyberbullying and safeguard a vigorous First Amendment.”\textsuperscript{31} In a similar vein, Wells believes that a recalibration of Internet policing to incorporate lessons from the urban environment is in order.\textsuperscript{32} Kane argues that better-informed judges and rediscovering the “forgotten” tort of confidentiality is the best avenue for relief.\textsuperscript{33} Kay argues for the extension of the torts of misappropriation and

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{26} Jessica Moy, Note, Beyond ‘The Schoolhouse Gates’ and into the Virtual Playground: Moderating Student Cyberbullying and Cyberharassment After Morse v. Frederick, 37 HASTINGS CONST. L.Q. 565, 588 (2010) (arguing that revisiting and reexamining the Tinker standard is an appropriate alternative to cyberbullying regulation).
\item \textsuperscript{27} Lyrissa Barnett Lidsky, Anonymity in Cyberspace: What Can We Learn from John Doe?, 50 B.C. L. REV. 1373, 1389–90 (2009) (arguing that libel law only offers a partial remedy for cybersmears).
\item \textsuperscript{28} Nancy S. Kim, Web Site Proprietorship and Online Harassment, 2009 UTAH L. REV. 993, 1034 (arguing that tort liability should be imposed on website sponsors).
\item \textsuperscript{29} Lauren Gelman, Privacy, Free Speech, and “Blurry-Edged” Social Networks, 50 B.C. L. REV. 1315, 1342 (2009).
\item \textsuperscript{30} Id. at 1344.
\item \textsuperscript{31} Mary Sue Backus, OMG! Missing the Teachable Moment and Undermining the Future of the First Amendment—TISNF!, 60 CASE W. RES. L. REV. 153, 204 (2009); see also Mary-Rose Papandrea, Student Speech Rights in the Digital Age, 60 FLA. L. REV. 1027, 1028 (2008) (arguing that the primary approach schools should take is not to punish, but to educate students how to use digital media responsibly).
\item \textsuperscript{32} Philip A. Wells, Shrinking the Internet, 5 N.Y.U. J.L. & LIBERTY 531, 532 (2010).
\item \textsuperscript{33} Brian Kane, Balancing Anonymity, Popularity, & Micro-Celebrity: The Crossroads of Social Networking & Privacy, 20 ALB. L.J. SCI. & TECH. 327, 358 (2010).
\end{itemize}
\end{footnotesize}
right of publicity to social media websites. Professor Richards argues that existing federal law governing Internet service providers should be amended to curtail the current broad immunity they enjoy, Norby-Jahner believes the law should only be amended to permit hostile environment sexual harassment claims, and Dickinson believes the law should simply be more narrowly interpreted by the courts. What is missing from this literature, however, is an analysis of how dangerous the Internet has become to individual privacy and the right to be left alone, as well as a concerted examination into the role website operators can (and should) play in ensuring the protection of a fundamental privacy interest.

Part I of this Article reviews the problem of Internet intrusion into personal privacy. The Internet is unlike any other media heretofore known to humanity. Its reach is worldwide, its speed is instant and its permanence means scrubbing content becomes more and more difficult as time progresses and the content replicates. Part II reviews existing remedies to protect individual privacy, both legislative and common law, and highlights the shortcomings in such remedies. Finally, Part III of the Article argues that the time has come for a re-thinking of the parameters of online privacy, and calls for the adoption of an individual right, Zero Net Presence. If the right to privacy is to remain meaningful in the hurricane of technological advance, an immovable shelter must be built now, and it must be constructed in law.

I. THE PROBLEM OF INTERNET INTRUSION

On October 2, 2008, popular South Korean Choi Jin-sil, a

34 Bradley Kay, Note, Extending Tort Liability to Creators of Fake Profiles on Social Networking Websites, 2010 CHI.-KENT J. INTELL. PROP. 1, 4.
mother of two and one of South Korea’s hottest movie stars, locked herself in her bathroom and hanged herself in the shower. Authorities believe she was driven to suicide by rumors posted on Internet chat rooms that she was a ruthless loan shark who caused the suicide of another popular actor, Ahn Jae-hwan. The case follows a string of high-profile celebrity suicides caused by Internet bulletin board rumors, such as popular singer Yuni, who hanged herself after online accusations that she had received cosmetic surgery, and the suicides of a transsexual celebrity and openly gay actor days after Choi’s suicide after they were “bombarded with hate e-mail and Web posts.”

South Koreans even have a name for this phenomenon, translated as “cyberviolence.” Nearly 200,000 cases were reported in 2007, up almost fifty percent from a year earlier.

While South Korea struggled early in its Internet renaissance with the problems associated with online smear campaigns that left victims feeling powerless and hopeless enough to commit suicide, the phenomenon is not limited to South Korea. All around the world, online targeting of individuals for scorn, ridicule, or simply bullying has risen with the rise of social networking websites. Users typically use these websites to keep in touch with friends and family, and to make new friends. The voluntary use of the Internet to maintain relationships and interact with other human beings is limited only by imagination.

This phenomenon is best exemplified in the meteoric rise of social media giant Facebook. Founded in 2004 by CEO Mark Zuckerberg in his Harvard University dorm room, the site allows its 500 million users to share photos, videos, short messages, applications, and other information for free. It was the fourth most visited website in the United States in 2009, lagging only

---

39 Id.
41 Id.
42 Id.
behind Google, Yahoo!, and Microsoft. Although it does not charge users, the privately-held company is hugely profitable, driven by advertising revenue. Its biggest advertisers boosted advertising by a factor of ten in 2009 alone, which may help the company break its $800 million sales record set in 2009 with over $1.4 billion in 2010. “More than 1 in 4 people who browse the Internet not only have a Facebook account but have returned to the site within the past 30 days.”

The site’s soaring popularity made it especially vulnerable to accusations that it failed to respect its users’ privacy. In 2007, for example, it launched Facebook Beacon, which sent a user’s friends automatic updates about purchases that user made on certain third-party websites. In early 2009, the company updated its terms of service to delete a provision that said users could remove their content at any time, and added new language that the company could retain users’ content and licenses even after an account was terminated. Later in 2009 it bungled an attempt to change its default privacy settings. Even after a public backlash forced the company to publicly apologize and once again re-examine its privacy settings, the company continues to quietly create easier ways for strangers to track its users, such as the creation of a “de-facto” follow feature in late 2010. Even with a privacy policy in place, the site does not always have the ability to enforce privacy settings—an investigation recently revealed that many popular application on Facebook transmitted identifying information about millions of users’ names and their friends’ names, even when the users set

44 Id.
45 Id.
46 Id.
47 Dan Fletcher, How Facebook is Redefining Privacy, TIME, May 31, 2010, at 32.
48 Id.
52 MG Siegler, Facebook Has Quietly Implemented a De-Facto Follow Feature, TECHCRUNCH (Sept. 20, 2010), http://techcrunch.com/2010/09/20/facebook-not-now-follow/.
their profiles to the strictest privacy settings. Most users do not realize, however, that the information they post on social media websites can sometimes yield unintended consequences. Jury consultants, for example, claim that with “information online—newspaper letters to the editor, petition signatures, club memberships, campaign contributions—retrievable with a couple of keystrokes, Internet surfing can produce a detailed picture of how an individual votes, spends money and sounds off on controversial issues.” In one case, a jury consultant caught a potential juror in a lie when the juror denied knowing a potential fellow juror (his Facebook page revealed they were in fact cousins). In another case, a potential juror who wrote on his Facebook page that he was “sitting in hell . . . aka jury duty” was removed from a prominent civil trial and prompted motions for a mistrial. In England, a juror on a child abduction and sex assault case held a poll on her Facebook page, inviting her friends to help her decide the case. After a court official received an anonymous tip, she was dismissed from the case.

A particularly troubling trend lies in a new generation of

---

55 Id.
57 Urmee Khan, *Juror Dismissed from a Trial After Using Facebook to Help Make a Decision*, TELEGRAPH (U.K.) (Nov. 24, 2008, 10:01 AM), http://www.telegraph.co.uk/news/newstopics/lawreports/3510926/Juror-dismissed-from-a-trial-after-using-Facebook-to-help-make-a-decision.html. The problem of jurors discussing trials on the Internet is not isolated, and is not going away. One commenter pointed out that in one random search on Twitter, she found 108 updates in one eight-hour period involving “jury duty.” See *If We Strike All the Facebook Jurors, Who’s Left?*, WIS. L.J. (Feb. 9, 2009, 1:00 AM), http://www.wislawjournal.com/article.cfm/2009/02/09/If-We-Strike-All-The-Facebook-Jurors-Whos-Left. Even if jurors refrain from discussing their roles on their social networking sites, courts are beginning to grapple with the very real, and very troublesome, problem of jurors who conduct independent research using internet-enabled mobile devices. See John Schwartz, *As Jurors Turn to Google and Twitter, Mistrials Are Popping Up*, N.Y. TIMES, Mar. 18, 2009, at A1.
58 Khan, supra note 57.
social networking built upon wireless platforms with Global Positioning System (GPS) technology. Social media networking sites are now using these GPS receivers to allow users to physically see where their friends are. Facebook’s “Places” application, for example, allows users to [check in] at a restaurant, bar or museum, alerting their friends on Facebook of their presence. They will then be able to see, using the service, any friends that are nearby, as well as other people who have checked in at the same location and have agreed to have their location broadcast widely. Known as “geolocation” devices, these offerings have grown dramatically. One interesting service, Ratio Finder, aggregates data from other geolocation services to create maps that show places where “social media savvy guys tend to congregate, the places where social media savvy girls tend to congregate, and the sad places where no one congregates at all.”

Real time maps display pink bubbles where more women congregate and blue bubbles show where more men congregate. Curiously, Americans seem to have hit a privacy wall with these services, opting out more often than opting in. Only four percent of Americans have tried location-based services, and only one percent use them weekly. Eighty percent who have tried them are men, and seventy percent are between age nineteen and thirty-five.

Combining social media and geolocation, Twitter has become a social force in its own right. The service allows users to constantly broadcast, or “tweet,” their thoughts and whereabouts in short messages from their computers, any web browser, or mobile phones. Companies are using Twitter to

61 Id.
63 Id.
64 Id.
market their products and understand their customers. Politicians use Twitter to communicate their thoughts directly to constituents. A Japanese journalist, kidnapped in Afghanistan and facing execution, tricked his captors into using Twitter, which he then used to tweet his location to rescuers. As of January 2009, Twitter had over 3.5 million users worldwide. By April 2009, that number was up to 14 million users. By the end of 2010, that number had exploded to 160 million. The number of active users is now more than ten times the number twelve months ago. The company recently announced it raised an additional $35 million in financing, bringing its total financing to $55 million even though it has not earned a single dollar in profit.

Another big name in technology, with far more users than Twitter, is Google. Google dominates web searching, drawing sixty percent of all searches worldwide, with Yahoo at fourteen percent and Microsoft at four percent. The company, founded
by Stanford University students Larry Page and Sergey Brin, burst onto the scene in 1998 with its groundbreaking search capability, an uncanny ability to find relevant information among the billions of webpages its robots crawl and index.\textsuperscript{75} Unlike many of its peers, Google quickly developed a model for making money through paid searches.\textsuperscript{76} In essence, the company sold advertisements to appear along with search results.\textsuperscript{77} The advertisements would be targeted to each user, depending on what the user was searching for.\textsuperscript{78} Advertisers, keen to reach web users interested in their product or service, would pay Google each time a user clicked on their advertisement.\textsuperscript{79} The business model has resulted in a revenue explosion for Google. The company earned $3 billion in profit in 2006, $4.2 billion in 2007, and $4.2 billion in 2008.\textsuperscript{80} More than eighty percent of the company’s profits are from the advertisements that Google displays on search results pages.\textsuperscript{81} In spite of an economic downturn, Google’s advertising revenue rose eighteen percent in the final three months of 2008, yielding a $382 million profit.\textsuperscript{82}

Google’s success, however, has created new breaches in the firewall against privacy. In one recent case, a French citizen appealing his conviction for corruption of a minor found that Google’s search engine automatically linked the man’s identity to search terms including “rapist” and “prison.”\textsuperscript{83} Since French law provides all citizens with the presumption of innocence until all

\textsuperscript{77} See id.
\textsuperscript{78} See id.
\textsuperscript{79} See id.
\textsuperscript{81} Freedman, supra note 74.
appeals are exhausted, he successfully sued Google for defamation. In the United States, these concerns reached the level of a national conversation with the launch of Google’s free email service, Gmail, in beta form in 2004 and later to the public in early 2007. At its launch, Gmail offered users an unprecedented amount of storage, and encouraged users to never “delete another message again” since there was so much storage space available. The catch is that the service displays targeted advertisements to users. In order to generate the advertisements, the service “reads” the user’s email, and decides what ads to display based on that email’s content. The advertisements are generated by the same technology that generates advertisements when a user executes a search using Google’s search engine, generating “similar” links. The idea that Google would be reading users’ emails quickly generated a wave of backlash. Privacy advocacy groups sent Google an open letter urging the company to abandon the idea of targeting ads based on the content of the emails. A California state senator went further, introducing legislation to outlaw services like Gmail. Advertisers and marketing firms now want to push the envelope of targeted ads even further beyond context-sensitive ads: they are now exploring ways to target ads to users

---

84 Id.
88 Id.
89 Id. Only ads classified as “Family-Safe” are shown, the service avoids “targeting ads to messages about catastrophic events or tragedies.” Id.
90 Walker, supra note 86.
91 Id.
92 Id. See also CREEPY GMAIL, http://www.gmail-is-too-creepy.com/ (last visited Feb. 2, 2009) (website dedicated to encouraging users to reply to any email from a Gmail account with boilerplate language: “Dear Gmail user: Due to privacy considerations, we cannot respond unless you resend your email from a different account.”).
based on data about a user’s interests, habits, and location.\(^{93}\)

In 2005, Google introduced Google Maps,\(^{94}\) allowing web users to search for local businesses, obtain directory information, and plan driving routes.\(^{95}\) The service has been enhanced with the addition of street-level photos taken by roving vans (called Street View), which allows anyone in the world to see actual images of streets.\(^{96}\) Google claims that since all photos are taken from public property, “[i]t’s not unlike what you see while walking down the street.”\(^{97}\) Potentially embarrassing or incriminating photos have already surfaced,\(^{98}\) and multiple websites are dedicated to posting funny or interesting photos,\(^{99}\) as well as potential criminal activity,\(^{100}\) captured on the service. One woman using Street View was startled to see her cat, Monty, perched in the living room window of her apartment in Oakland.\(^{101}\) In an interview, she said, “[T]he next step might be seeing books on my shelf. If the government was doing this, people would be outraged.”\(^{102}\) Using Google Earth, a related


\(^{94}\) *Google History*, supra note 85.

\(^{95}\) Maps are nothing new, of course. Google Maps, however, changes the way that people access and use maps through the use of innovations such as phone number map lookup.


\(^{97}\) Janet Kornblum, *Street View Clicks, Captures Everyday Antics But Not Everyone Caught is Smiling*, USA TODAY, July 10, 2007, at 8D.

\(^{98}\) Id.


\(^{102}\) Id.
service that provides satellite imagery of the earth, police in Switzerland found a two-acre marijuana plantation and arrested sixteen people while seizing more than a ton of marijuana.

One town in New York used Google Earth images to determine if properties had swimming pools, and then compared those homes to records of home with pool permits. Violators were told to get a permit, or face stiff fines and penalties. In Brazil, startled citizens logging on to Google’s Brazilian site saw gruesome scenes of murder and traffic accidents captured on Street View. A British mother was stunned to see a photo of her three-year-old son, naked, on Street View after a Street View car captured an image of him on the family driveway after running out of the house.

Controversy and indignation over Street View is felt worldwide. In Canada, Street View faced a firestorm of criticism when Google began taking images without complying with the country’s Personal Information and Electronic Documents Act. Lawmakers demanded to understand the
implications of the feature on the privacy rights of Canadian citizens. The company relented, and after agreeing to blur out all faces and car license plates, as well as making it easy for users to flag images for removal, Street View was launched in Canada in late 2009. In the United Kingdom, angry residents formed a human chain when a Street View van tried to take pictures of their neighborhood, claiming that the images might facilitate break-ins and other crimes. Within weeks of Street View’s U.K. launch in March 2009, watchdog groups began complaining of invasions of privacy, including one from a woman photographed outside a home she was living in to escape a violent former partner. In South Korea, police raided Google’s Korean offices as part of an investigation into whether Street View cars illegally collected and stored personal wireless information. The admission by Google that Street View cars contained antennas that sniffed out data on open wireless networks including the MAC addresses of computers, and data included in documents, emails, video, and audio over the networks the vehicles encountered, led to class action lawsuits in the U.S. and an investigation by the U.K.’s Information Commissioner Office and French authorities. Protests over

110 Bill Curry, Google Vows to Protect Privacy After Camera Exposes Nude Man, GLOBE & MAIL (Can.), June 18, 2009, at A7.
118 Google Cleared of Wi-Fi Snooping, BBC NEWS (July 29, 2010),
Street View were perhaps loudest in Germany, where “there was an outcry louder than anywhere else on the planet.” Privacy concerns prompted Google to permit Germans, at least for a limited time, to exclude their physical properties from Street View. These measures were not enough to stop the German government from considering privacy legislation that would specifically address services such as Street View.

Google’s other products and services have not fared any better when it comes to consumer privacy. When Google introduced its own smartphone, the G1, Jeffrey Chester, the executive director of the Center for Digital Democracy, described it as a “walking surveillance device.” As a customer uses the phone, data such as the user’s name, contacts, instant messages, emails, calendars, social networking site visits, and videos downloaded are all collected. The user cannot see what specific data is collected, and there is no way to expunge the data. “It’s Google’s for as long as it wants to hold onto it.”

When Google released its web browser, Chrome, it came under heavy attack for the End User License Agreement (it turns out that most Google products carried the same language), which provided Google with “a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and


121 Alexia Tsotsis, If German Homes Can Now Opt Out of Google, Then How About People?, TECHCRUNCH (Aug. 17, 2010), http://techcrunch.com/2010/08/17/if-german-houses-can-now-opt-out-of-google-then-how-about-people/. By late September, over 100,000 Germans had requested their homes be excluded from Street View. Low Visibility Ahead? More than 100,000 Germans Ask Google to Blur Their Homes, SPIEGEL ONLINE (Sept. 20, 2010), http://www.spiegel.de/international/germany/0,1518,718374,00.html.


123 Cauley, supra note 3.

124 Id.

125 Id.

126 Id.
distribute any Content which you submit, post or display on or through, the Services.” Under fire from many technology bloggers, the company rescinded the provision within a few days of the browser’s release. When Google released its social networking platform, Buzz, it led to a “ferocious backlash from users concerned about intrusions of privacy” because the service automatically created a circle of friends based on people they frequently emailed. The default setting when it was released meant that “the people you follow and the people that follow you are made public to anyone who looks at your profile.” Google eventually agreed to pay $8.5 million to settle a privacy class-action lawsuit stemming from Buzz’s disastrous launch. Another free product, Google Analytics, can be installed on any web server connected to the Internet to provide information about traffic and users. A survey by Austrian computer scientist Hermann Maurer at Graz University revealed that Google Analytics is installed on eighty-three percent of servers, which means that even if a user does not use any Google product, “by doing anything on the internet, four out of five servers automatically pass on every conversation a customer has with the server on to Google.”

Finally, a new service to allow consumers to keep track of health records, Google Health, was revealed by the company

---

recently with the Cleveland Clinic as its launch partner.\textsuperscript{135} The service allows “outside doctors to send information through Google that the Cleveland Clinic can merge with existing files.”\textsuperscript{136} Privacy advocates are worried because while Google has announced a privacy policy for Google Health, since Google is not a health care provider the provisions of the Health Insurance Portability and Accountability Act (HIPAA) do not apply.\textsuperscript{137} For now, voluntary promises by Google (and the competing Microsoft service, Vault) are the only privacy safeguards.

As our lives become more and more imprinted online, it is important to make a distinction between voluntary and involuntary presence on the Internet. Many people voluntarily do stupid things on the Internet and get caught for it, such as the thirteen cabin crewmembers for Virgin Atlantic who posted Facebook updates insulting passengers and making jokes about faulty engines.\textsuperscript{138} An involuntary presence on the Internet, however, gives rise to serious privacy concerns. What happens when someone suffers real harm because of content accessible on the Internet that is not the result of that individual’s voluntary action? The Internet is unlike any bulletin board, building side, bathroom wall, newspaper, radio show, or book. In fact, it is unlike any other media in the history of humanity. The three characteristics that make the Internet so appealing—its speed, reach, and permanence—also make it a devastatingly effective tool to ruin the lives of innocent citizens.

\textbf{A. Speed}

\textit{A lie can travel halfway round the world while the truth is still putting on its shoes.}

\begin{flushright}
— Mark Twain\textsuperscript{139}\end{flushright}

The Internet is fast. It is as fast as people can type, because

\begin{footnotesize}
\bibliography{file}
\end{footnotesize}
Unlike virtually any other media, publication is instant. There are no presses to run, shows to tape, canvasses to be prepped, or film to be developed. For example, in early October 2008, a false report submitted by a viewer to CNN that Apple CEO Steve Jobs had been rushed to the hospital sent Apple’s stock downwards by five percent.\textsuperscript{140} In September 2008, United Airlines lost more than $1 billion in market capitalization based on a six-year-old bankruptcy announcement mistaken by traders as fresh news.\textsuperscript{141} A false report on September 5, 2008 on the Drudge Report website that Oprah Winfrey had refused to invite then vice-presidential candidate Sarah Palin to her show resulted in widespread attention, even drawing a question about it from debate moderator Tom Brokaw during the sole vice-presidential debate of the 2008 election season.\textsuperscript{142} More recently, a city councilman in Texas pleading with gay teens not to commit suicide at a council meeting attended by a small group of citizens on a Tuesday evening “rocketed into cyberspace prominence” on YouTube after a video of his speech was watched more than 500,000 times only three days later.\textsuperscript{143}

Once that content is instantly published, it becomes accessible to billions of people all over the planet. This speed is easily harnessed in social networking sites to achieve a communal goal quickly. In early February 2009, a twenty-two-year-old Facebook user saw a TV commercial for cell phone service provider T-Mobile and was inspired to invite his friends to Liverpool Street, a major train station in London, for a “little dance.”\textsuperscript{144} He posted the event on Facebook and, within hours, 14,000 people had joined the Facebook group “Liverpool Street Station Silent Dance.”\textsuperscript{145} “Videos posted on the social-networking site showed [the station] completely filled with

\textsuperscript{141} Id.
\textsuperscript{142} Id.
\textsuperscript{145} Id.
people, counting down the seconds until the clock showed 7 p.m., then dancing to music on their mp3 players as the hour struck.”

This phenomenon has generated a new word: “flashmob.”

Another group on Facebook encourages users to participate in various “No Pants” subway rides in major cities such as Boston, New York, and Washington, D.C. Flashmobs sound innocent enough, and the use of social media sites to organize spontaneous community expressions of creativity may even sound attractive or appealing. That same community can quickly turn ugly, however, when it is used against innocent citizens.

Stories of Internet users startled by the quick and long-reaching spread of their postings are nearly everyday occurrences. In New York, a police officer who fantasized about being a “devious” character on his MySpace website found himself confronted with those postings when he was accused of planting evidence on a suspect. In 2007, Kevin Colvin, an intern at Anglo Irish Bank’s North American branch, told his manager by email that he would be missing work because “something came up at home,” but then posted a picture of himself dressed in a fairy costume holding a beer. The manager found the picture on Facebook and replied to the whole office, attaching the picture, with the wry message, “Thanks for letting us know—hope everything is ok in New York.”

---

146 Id.
147 Id.
149 One example site, Improv Everywhere, seeks to cause “scenes of chaos and joy in public places.” IMPROV EVERYWHERE, http://improveverywhere.com/ (last visited Feb. 2, 2011). For instance, its latest “mission” involves over 3000 participants downloading a particular MP3 file and pressing play simultaneously while in retail stores in midtown Manhattan. See Charlie, The MP3 Experiment Seven, IMPROV EVERYWHERE (Oct. 12, 2010), http://improveverywhere.com/2010/10/12/the-mp3-experiment-seven/. The participants then took part in a series of fun activities, culminating in a huge “mummy dance party” in Bryant Park. Id.
150 See infra Part I.B.
At Duke University, recent graduate Karen Owen compiled a mock thesis, comparing and rating her sexual partners in a forty-two-page PowerPoint presentation. She emailed the file to a few close friends, and before long the file had “gone viral”—passed among millions of people and posted widely on blogs and news sites.

B. Reach

*People think what they say won’t have repercussions, and they don’t have to soften their comments.*

— Lesley Withers, Communication Professor

In addition to being fast, the Internet is ubiquitous. With remarkably few resources, content can be replicated over and over again, the number of copies increasing exponentially as it travels through the Internet. By its very nature, the Internet was designed to be an open network, open to anyone with a web browser. Along with that reach comes anonymity, as no authentication process is required before someone posts content to the Internet.

The anonymous nature of the Internet permits people to engage in invectives and vitriol that they might normally never think about. In the early days of the Internet, frustrated consumers quickly found a way to voice their frustration at poor customer service through websites. Now, a valid complaint is no longer a pre-requisite to venting. There are websites that are dedicated to simply venting, such as Justrage.com (which bills itself as “The Internet Anger Sponge”) and mybiggestcomplaint.com (proudly proclaiming it is “Where the World Comes to Complain”).

153. *Id.*
158. MY BIGGEST COMPLAINT, http://www.mybiggestcomplaint.com (last
classified listings website, Craigslist.org, is dedicated purely to rants. Some Internet users have taken this anonymity to perfect the drive-by shooting on an emotional level, proudly collecting “lulz” (from the acronym LOL for “laughing out loud”) as evidence of their ability to “disrupt[] another’s emotional equilibrium.” Nothing appears to be too depraved for these users, including an episode where several of them harassed the family of a seventh-grader who had killed himself. In other episodes, they target random strangers and hit the phones, sending taxis, pizzas, and escorts to their homes. As lulz are collected, they are displayed proudly on Encyclopædia Dramatica (its tagline is “In Lulz We Trust”), an online archive of their exploits. Many other examples of websites that specialize in allowing users to smear other citizens exist—dontdatehimgirl.com, dontdateherdude.com, whosararat.com, and whosarrested.com are past and current examples, and future websites are currently limited only by imagination.

The Internet’s reach takes an ugly turn in the phenomenon widely known as cyberbullying. The term includes instances wherein an individual, or group of individuals, target and bully another person or group through private online communications. The case involving Megan Meier, for


160 Id.

161 Id.


163 Writing PIs, Don’t Date Him Girl! and Other “Bad Rep” Sites, GUNS, GAMS AND GUMSHOES (Mar. 26, 2010), http://writingpis.wordpress.com/2010/03/26/dont-date-him-girl-and-other-bad-rep-sites/.

164 For an excellent review of cyberbullying and state legislative responses to it, as well as criticism of those responses, see Backus, supra note 31; Colleen Barnett, Note, Cyberbullying: A New Frontier and a New Standard: A Survey of and Proposed Changes to State Cyberbullying Statutes, 27 QUINNIPAC L. REV. 579 (2009); Kevin Turbert, Note, Faceless Bullies: Legislative and Judicial Responses to Cyberbullying, 33 SETON HALL LEGIS. J. 651 (2009); and Schwartz, supra note 159.

165 See Brenner & Rehberg, supra note 23; Shannon L. Doering, Tinkering With School Discipline in the Name of the First Amendment: Expelling a Teacher’s Ability to Proactively Quell Disruptions Caused by Cyberbullies at the Schoolhouse, 87 NEB. L. REV. 630 (2009); Papandrea,
example, drew worldwide attention when Lori Drew, a suburban mother whose daughter was a former friend of Meier’s, created a fake online profile of a boy named Josh Evans.\textsuperscript{166} Drew used that profile to lure Meier into a month-long flirtation that suddenly turned nasty when “Josh” sent Meier a message saying, “I don’t like the way you treat your friends, and I don’t know if I want to be friends with you.”\textsuperscript{167} On October 16, 2006, Meier hanged herself.\textsuperscript{168} Drew was eventually convicted of minor misdemeanors in federal court, but her conviction was overturned on appeal.\textsuperscript{169}


\textsuperscript{166} Christopher Maag, MySpace Hoax Draws No Charges, N.Y. TIMES, Dec. 4, 2007, at A22.

\textsuperscript{167} \textit{Id.}

\textsuperscript{168} \textit{Id.}

\textsuperscript{169} Rebecca Cathcart, Conviction Is Tossed Out In MySpace Suicide Case, N.Y. TIMES, July 3, 2009, at A14. For critical scholarly analysis of
Of course, online bullying isn’t limited just to suburban mothers. In Michigan, Andrew Shirvell, an assistant attorney general, was put on administrative leave after he attacked the student body president at the University of Michigan by calling him a racist with a “radical homosexual agenda.” The smears were made on a website Shirvell set up to directly attack the student. After a national uproar, Shirvell made the website private.

It is when that bullying goes public for thousands or millions to witness that truly horrific consequences can follow. In 2009, Hope Witsell, a thirteen-year-old Florida middle school student, took a photo of her breasts with her cell phone camera and sent it to a boy that she liked. Someone else stumbled upon a copy, and the photo went viral. Classmates used the photo to bully and torment Hope, even creating a MySpace page to humiliate her. On September 12 that year, Hope committed suicide.

Call it cyber-lynching, cybersmearing, cyberbullying, or cyber-stoning—it is the modern day equivalent of a drumhead trial, and the consequences can be startling. In 2008, anyone who

---


171 Id.
172 Id.
Googled “Morgan Shaw-Fox” would have learned that he was accused of rape at Lewis & Clark University.\(^{177}\) The charge came on Facebook, when several women launched a Facebook group titled, “Morgan Shaw-Fox is a piece of shit rapist.”\(^{178}\) The group was supposed to be private, but within a week eighty students had joined, bloggers had picked up the story, and Shaw-Fox’s name was all over the Internet.\(^{179}\) A local paper picked up the story and published details of the alleged rape on its website.\(^{180}\) Shaw-Fox, meanwhile, was neither arrested nor charged in the case.\(^{181}\) Even the group’s organizers were surprised by the consequences of their actions, saying “[n]one of us wanted to bring him down. . . . I didn’t think it was going to be this big. We had no idea the can of worms we were opening.”\(^{182}\)

Yale Law School students Brittan Heller and Heide Iravani found themselves in a similar nightmare when they became the targets of a cybersmear campaign on the website Autoadmit.com. Prospective employers, friends, classmates or family who Googled them would find postings such as “[i]s Brittan Heller a lying bitch?”\(^{183}\) Another said, “Heide Iravani deserves to be raped.”\(^{184}\) Yet others wrote falsely that Heller had herpes and bribed her way into Yale with a secret lesbian affair with the dean of admissions and that Iravani had gonorrhea, was addicted to heroin, and had exchanged oral sex with Yale’s dean for a passing grade in civil procedure.\(^{185}\)

If the victims of these cases of cybersmearing had been targeted through traditional media such as a book or even a bathroom wall, there are physical ways to limit the extent to


\(^{178}\) Id.

\(^{179}\) Id.


\(^{181}\) Ross, supra note 177.

\(^{182}\) Id.


\(^{184}\) Id.

\(^{185}\) Id.
which the smears are spread. Whereas physical media can ultimately be controlled through distribution, the Internet has one other trick up its sleeve to ensure that once content is generated, it becomes difficult to scrub clean—permanence.

C. Permanence

People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.

— Mark Zuckerberg, CEO, Facebook

In an interview with the Wall Street Journal, Google’s CEO Eric Schmidt suggested that one day, every young person will be “entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends’ social media sites” (as paraphrased by the Journal). Later, in an interview with Stephen Colbert, Schmidt was asked about his idea “that someday, young people instead of having privacy for the things that they put up on Facebook, being able to expunge that, since once they put it up there, it exists forever, that one day they’ll just erase their histories, and change their names, and they’ll be scot free.” Although Schmidt claimed “it was just a joke,” he also stated flatly: “[J]ust remember when you post something that the computers remember forever . . . . [I]t’s actually on the web. Google just collects it. It’s all out there on the web somewhere . . . . And if it’s really juicy, there will be copies everywhere.”

That is certainly the case with content on Facebook. Facebook provides a “delete this” option on its social media site. While clicking “delete this” may remove the link to the picture from someone’s Facebook page, the picture itself remains available on Facebook’s servers, in some cases for

189 Id.
years. Anyone with the direct link to the picture, including Google and other search engines, can still locate the picture.

In litigation, deleted websites can be revived to haunt litigants in discovery, as one personal injury plaintiff in New York found out when the defendant successfully retrieved pictures of the plaintiff enjoying herself away from home in historical Facebook and MySpace pages, in spite of the plaintiff’s claims that she was bedridden and housebound.

Even when Internet users believe they are being anonymous because they have not entered any identifiable information such as their name or email address, computers and network servers continue to collect information about them. The use of “cookies,” for example, allows web browsers to track users’ web browsing habits, from how often they visit a web site to how long they stay on a particular site. Sometimes this information can be used for a public good, such as Google’s recent effort, Google FluTrends, to correlate searches about the flu with a user’s geographic location to “detect regional outbreaks of the flu a week to ten days before they are reported by the Centers for Disease Control and Prevention.”

Sometimes user search data can be quite interesting, and reveal trends in popular culture as evidenced by Google’s annual “Zeitgeist” list of top search terms, broken down by country and region. According to

---

191 Id.
Google, the list is compiled after Google “anonymises” the data by deleting the last two digits of the user’s Internet Protocol address, much like how credit card numbers are blanked out on credit card receipts.\(^{196}\) Such efforts to anonymize data, however, are dependent wholly on the corporation’s magnanimous sense of preserving privacy. There is no legal obligation to do so, at least not yet. Among the major web search engines, Google retains use search and Internet Protocol data for nine months, Microsoft for eighteen months, and Yahoo for three months.\(^{197}\)

Some courts are already recognizing that the public and permanent nature of the Internet make it unique and can expose citizens, particularly those accused of crime, to “limitless and eternal notoriety.”\(^{198}\) In Nassau County, New York, for example, Judge William LaMarca ordered the county to remove a woman’s mug shot and name from the county’s “Wall of Shame” website.\(^{199}\) In his opinion holding that the website violates due process, Judge LaMarca observed that “[t]he Internet has no sunset and postings on it will last and be available until some person purges the Web site, perhaps in decades to come.”\(^{200}\) The county has since revised the website to only include the names of those convicted, not merely arrested, of drunk driving.\(^{201}\) The revision came too late for at least one New York citizen, falsely accused of drunk driving and posted to the website, when in fact

---


\(^{199}\) Id.

\(^{200}\) Id.

she was driving erratically due to diabetes-induced hypoglycemia.202

From middle schoolers to law students to student body presidents to virtually anyone alive, the Internet provides new and previously unimaginable ways to hurt and destroy. Regrettably, while the pain and anguish that accompanies cyber-smearing are every bit as real as a case where the smears are made in traditional channels, the law has fallen woefully behind in providing victims with meaningful remedies.

II. EXISTING REMEDIES

Googling someone’s name has become the modern-day equivalent of asking a friend, neighbor, or past employer about someone’s reputation. Whatever results show up on Google’s first page becomes the professional or personal image of someone for the world to see. If that image is not the result of voluntary self-disclosure, then a person loses a critical part of what it means to be left alone. When faced with the speed at which false, defamatory, or ruinous information can spread around the Internet, citizens are left with little recourse. Engaging an online reputation scrubber—a company that generates positive content, buries negative content, or negotiates to remove negative content—is an option, but it is expensive and time-consuming.203 One journalist who tried to change the results of her Search Engine Results Page, found that the process can take a lot of time, and can be undone in an instant because of the (unpublished) way that search engine algorithms work.204 Taking steps to limit disclosure of information through safe surfing options such as encrypted email and managing web

204 Julia Angwin, It’s a New Me (As Seen on Google), WALL ST. J., Feb. 5, 2009, at D1.
cookies helps, but does not solve the problem of users who are victims of cybersmearing or cyberbullying.

The problems described in this Article beg for a more effective solution. Surveying the legal landscape for existing remedies, however, leaves one thirsty for more. Privacy torts, of course, are familiar to most practitioners but are of limited utility when applied to the Internet. In his article, Brian Kane addresses the problem with privacy torts on the Internet: the “disconnect between privacy interests and information sharing” makes “privacy regulation particularly difficult online.” Users do not take adequate steps to protect their information, and online providers like Facebook actively seek to solicit and disseminate information. Among traditional privacy torts, appropriation is commonplace on the Internet, but difficult to establish because of the damages requirement. Intrusion into seclusion offers some hope for relief, but is also rarely successful. Casting someone in a false light happens as well, but it may be difficult to meet the legal standard of showing that a reasonable person would be offended in an online setting. Publication of embarrassing private facts does not provide any protection if one is observed in a public place (like the Internet).

Ultimately, Kane concludes, the tort of confidentiality “resets the privacy field appropriately because its critical analysis point is the relationship between the person about whom information is being shared and the person sharing the information,” but recognizes courts are reluctant to find the requisite duty underlying this tort. Professor Kim also believes that current tort law can be rescued to protect privacy, if courts adopt certain reforms such as the imposition of proprietorship liability upon website sponsors.

---

205 See Eric Griffith, How to Reclaim Your Online Privacy, PCMag (Feb. 1, 2009), http://www.pcmag.com/article2/0,2817,2334782,00.asp.
206 Kane, supra note 33, at 344.
207 See id. at 345.
208 Id. at 348. See also Kay, supra note 34, at 23–24 (arguing that legislative enactments to buttress the misappropriation tort may be necessary to make it effective in the context of cyberspace).
209 See Kane, supra note 33, at 349.
210 Id.
211 Id. at 350.
212 Id. at 359.
213 Kim, supra note 28, at 1045.
The law of defamation is equally ineffective in combating defamation on the Internet, primarily because of inadequate remedies. “An angry lover, a disgruntled employee, or simply a mischievous character assassin can start a campaign of lies, and often the victim will have little meaningful recourse.” Lidsky traces the inadequacies of defamation in the AutoAdmit case, where several law school students attempted to bring defamation cases against the operators of an admission website and anonymous posters on the website. Even if an effective remedy were available, courts, including the California Supreme Court, have held that website operators have broad immunity from tort liability for defamatory remarks made on their sites (under the Communications Decency Act of 1996). This leaves victims with “only one legal recourse: To go after the author, which can be difficult, time consuming, expensive, or simply impossible. The lack of effective remedies for harms suffered by victims of cybersmears is the direct result of the nature of the Internet, and is further evidence of the need for a stronger and legislated privacy right.

The limitation of tort law in protecting someone from having a presence on the Internet is exemplified in Aaron and Christine Boring’s case against Google. In 2008, the Borings sued Google for sending a Street View car onto their property, photographing their residence in spite of a sign that said “Private Road, No Trespassing,” and posted the photographs on the Internet. The Borings sued in Pennsylvania State court; Google then removed to federal court under diversity jurisdiction.

---

214 Lidsky, supra note 27, at 1390–91.
215 Id. at 1386–87. See also Jameson, supra note 25, at 248 (outlining why current defamation law is inadequate to protect against harassment on the Internet).
216 Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006) ("In the Communications Decency Act of 1996, Congress declared: ‘No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. . . . These provisions have been widely and consistently interpreted to confer broad immunity against defamation liability for those who use the Internet to publish information that originated from another source.’ (quoting 47 U.S.C. § 230(c)(1))).
218 Id. at 276.
dismissed the invasion of privacy claim because the Borings could not establish that Google’s conduct was “highly offensive to a person of ordinary sensibilities.”

The negligence claim was dismissed because the court found that Google did not owe the Borings a duty of care. The trespass claim was dismissed because the Borings could not establish damages. The unjust enrichment claim was dismissed for lack of contract privity. The claims for injunctive relief and punitive damages were also dismissed.

Although the Borings sued for Google’s Street View feature, the legal analysis is the same in a case of cyber-smearing or other invasion of privacy. If a citizen wishes to be left alone on the Internet, and takes no steps to be on the Internet, the law does not provide any meaningful remedy for when a third party publishes information about that citizen on the Internet.

The use of criminal law to protect online privacy is equally problematic. A network of state laws preventing stalking has been used with varying degrees of success against harassment on the Internet. A federal law to address cyber harassment does not yet exist, although scholars have suggested language that may be included in such a law. Others have suggested states adopt a tiered approach to these crimes to include cyberstalking, cyberharassment, and cyberbullying with attendant punishment for malicious and less-malicious conduct.

The Megan Meier case illustrates the difficulty in prosecuting these types of crimes. In that case, Lori Drew was convicted of a violation of the Computer Fraud Abuse Act for

\[\text{id. at 277.}\]
\[\text{id.}\]
\[\text{id.}\]
\[\text{id.}\]
\[\text{id.}\]

For a discussion on how difficult it is to prosecute online crimes from a prosecutor’s perspective, see Stephen Treglia, *The Clash of Titanic Paradigms—The American Criminal Justice System Versus Modern Computer Technology: The Greatest Unresolvable Conflict Between a Square Peg and Round Hole?*, 20 ALB. L.J. SCI. & TECH. 407 (2010).

\[\text{Jameson, supra note 25, at 258–60. See also Brenner & Rehberg, supra note 23, at 15–78.}\]

\[\text{Jameson, supra note 25, at 265.}\]

\[\text{See Schwartz, supra note 24, at 429.}\]
essentially violating MySpace’s terms of service by posing as a fictional teenage boy in order to bully a neighbor’s daughter.\textsuperscript{228} The district court overturned the conviction, holding that a federal law that makes violating a website’s terms of service a crime is unconstitutionally vague.\textsuperscript{229} The Constitution requires laws to contain “relatively clear guidelines as to prohibited conduct.”\textsuperscript{230}

Turning from common law to statutory law yields no relief. State regulation of online privacy can be summarized as meager and pitiful. Minnesota\textsuperscript{231} and Nevada\textsuperscript{232} require Internet service providers to keep certain information about their customers private unless customers consent to disclosure. Delaware\textsuperscript{233} and Connecticut\textsuperscript{234} require employers to give notice to employees before monitoring employee email or Internet communications. Direct regulation of website privacy policies is limited to a handful of states. California, for example, which has one of the nation’s only online privacy laws, only requires Internet merchants to post a privacy policy on their website.\textsuperscript{235} Connecticut requires any site operator that collects Social Security numbers to create a privacy protection policy to protect the confidentiality and disclosure of Social Security numbers.\textsuperscript{236} Nebraska makes knowingly making a false statement in a privacy policy on the Internet illegal, but says nothing about making those statements elsewhere on a website.\textsuperscript{237} Finally, Pennsylvania makes including false statements in privacy policies a deceptive business practice.\textsuperscript{238}

Of course, state regulation of the Internet poses all kinds of practical and constitutional Commerce Clause problems. Federal regulation of the Internet, however, is much easier to envision.

\textsuperscript{229} Id. at 464.
\textsuperscript{230} Id. at 463.
\textsuperscript{231} MINN. STAT. ANN. §§ 325M.01–09 (West 2004).
\textsuperscript{232} NEV. REV. STAT. § 205.498 (2009).
\textsuperscript{233} DEL. CODE ANN. tit. 19, § 705 (LexisNexis 2005).
\textsuperscript{234} CONN. GEN. STAT. ANN. § 31-48d (West 2003).
\textsuperscript{235} Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2008).
\textsuperscript{236} CONN. GEN. STAT. ANN. § 42-471 (West Supp. 2010).
\textsuperscript{237} NEB. REV. STAT. § 87-302(14) (Supp. 2010).
\textsuperscript{238} 18 PA. CONS. STAT. ANN. § 4107(a)(10) (West Supp. 2009).
On the federal level, however, efforts to protect online privacy have also fallen short. Financial privacy is subject to some protection. Health records are also subject to fairly strict privacy protections. The Electronic Communications Privacy Act regulates government access to computer records through wiretaps. The CAN-SPAM Act of 2003 establishes rules for companies that govern the use of email marketing, including requirements for consumers to easily opt-out of such communication.

In the past, Congress has recognized that Americans are interested in preserving their privacy from prying eyes. In 1988, Congress made it illegal in the Video Privacy Protection Act for video rental stores to disclose any information about the videos customers were renting. The Act was passed in reaction to Judge Robert Bork’s confirmation hearings for a seat on the Supreme Court, during which a reporter for the Washington City Paper published Judge Bork’s video rental records. Similar state laws have passed in Connecticut, Maryland, and Michigan. These laws only protect video rental records, however, meaning extending their protections to online privacy is problematic. For example, when Facebook’s Beacon program began automatically broadcasting Blockbuster Online video subscriptions, multiple class-action lawsuits based on the federal Video Privacy Act ensued. Most of these suits remain tied up in litigation over procedural issues. In a similar case, Netflix ran into trouble when it ran a $1 million competition to improve

---

244 Michael deCourcy Hinds, Personal but Not Confidential: A New Debate Over Privacy, N.Y. TIMES, Feb. 27, 1988, at 56.
245 CONN. GEN. STAT. ANN. § 53-450 (West 2007).
246 MD. CODE ANN., CRIM. LAW § 3-907 (LexisNexis 2002).
249 See id.
its movie recommendation algorithm. As part of the contest, Netflix released datasets to 50,000 contestants that included movie subscription information that was supposed to be anonymized. Enterprising programmers quickly found a way to reveal the identity of reviewers by comparing their renting patterns to reviews posted on Netflix’s website. An in-the-closet lesbian mother sued Netflix, alleging the company made it possible for her to be outed against her will. The Video Privacy Protect Act, therefore, is of extremely limited utility in protecting online users’ privacy interests.

A proposed federal law, the Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act (BEST PRACTICES Act), would levy fines of up to $5 million on businesses and individuals unless they comply with a complex set of new regulations to be administered by the Federal Trade Commission. The bill provides comprehensive guidelines for the collection, storage, and handling of consumer and sensitive data by covered businesses. The bill faces a tough road to passage, with Internet marketing and other business groups vowing to fight against it. Even if it passed, however, the bill does not address cybersmearing and other problems associated with it.

In the absence of common law or statutory law to address the problem, the industry has made some efforts to self-regulate. These efforts largely surround standards for online behavioral

---


251 Id.

252 Id.

253 Id.


advertising. Most technology companies back self-regulation, fearing that congressional regulation would “stifle the growth of digital advertising.”

An industry group representing various Internet companies such as Yahoo!, Google, and AOL eschews a one-size-fits-all regulatory environment as unworkable given the many different forms that digital advertising can take.

The problem with industry policing (besides the fact that standards are completely voluntary) is that companies do not face any real sanction for failing to uphold their own privacy policies. In addition, companies like Google and Facebook make money from advertising, and advertisers need viewers. It is in these companies’ best interests to keep privacy laws at bay so that they can continue to grow their user base. In Google’s own words: “Today’s satellite-image technology means that even in today’s desert, complete privacy does not exist.”

Google, for example, currently has more than two dozen privacy policies, including one just for its mobile phone product, the G1. The policies are so hard to decode that Google publishes videos on its YouTube subsidiary to explain them. In recent congressional testimony, AT&T, Time Warner, and Verizon all promised to support an opt-in system for tracing user web movement and using that data to target advertisements to them. These efforts, however, only target online advertising.

---


258 Emily Steel, AT&T Backs Privacy Rules, WALL ST. J., Apr. 23, 2009, at B7.

259 Id.


261 Cauley, supra note 3, at 1B.


They do nothing to relieve concerns about other forms of privacy breaches. A more comprehensive solution, if it is implemented, is the recently announced Global Network Initiative, a “global code of conduct” that commits member companies to “avoid or minimize the impact of government restrictions on freedom of expression.” Member companies also promise to try to “resist overly broad demands for restrictions on freedom of speech and overly broad demands that could compromise the privacy of their users.”

Another problem with industry policing is that the industry itself has failed to grasp the extent of the problem of privacy intrusion. Too often, “online privacy” is used to encompass only privacy of consumer shopping and banking transactions and behavior. If left to the industry, it would argue that notification (telling consumers what the site’s privacy policy is) and consent (requiring consumers to click to agree to the site’s terms and conditions) are enough to discharge their responsibilities to consumer privacy. Neither of these actions do anything in the case where a citizen has not participated in or interacted with that site in any manner, and yet becomes a victim of vicious cybersmearing. In that event, nothing short of a new right will protect citizens.

III. ZERO NET PRESENCE

[The founders] conferred, as against the government, the right to be left alone—the most comprehensive of rights and the right most valued by civilized men.

—Justice Louis Brandeis

Professor Gelman argues that social norms should guide net privacy. She believes:

Internet users will respect the social force of a plea for privacy

---

265 Id.
267 Gelman, supra note 29, at 1343. See also Brian Kane & Brett DeLange, A Tale of Two Internets: Web 2.0 Slices, Dices, and Is Privacy Resistant, 45 IDAHO L. REV. 317, 345 (2009) (arguing that Internet users should become more responsible).
if they are faced with such a request at the time they access online content. The best way to counteract the erosion of privacy that results when content of a personal nature is shared online is not to deploy gate-keeping measures and an inflexible hierarchy that privileges certain speakers, subjects, or expressed preferences. It is to let simple social signals exert their own force across forums.  

While Professor Gelman may be right about situations where web users voluntarily interact with each other such as on social networking sites, there are limits to this argument. Tyler Clementi’s suicide demonstrates that certain actors, on certain subject matter, simply disregard social norms of neighborliness and consideration.

For law students smeared on a gossip website, gay college students outed by their roommates with hidden webcams, men and women accused of being bad dates (or worse), partygoers who wish only others at the party know they were there, or simply homeowners who do not want their houses shown on the Internet, the reach, speed and permanence of the Internet is a nightmare. It can and does cause severe emotional distress and rather than simply accept it as a price for living in an information society, society should demand that fundamental notions of privacy and decency are more important than the right of nosy neighbors to know. The only solution that suffices is to declare that for individual citizens who involuntarily have a presence on the Internet to demand “Zero Net Presence” (ZNP). ZNP means that a citizen who does not otherwise contribute to a particular incident should have the right to demand a website operator or Internet service provider remove and scrub all traces of their name or identity if they wish. Tyler Clementi might have used ZNP, for example, to demand that Twitter and YouTube remove the material referencing his intimate encounter immediately and permanently, before any lasting damage could be wreaked.

A proposed federal law, the Megan Meier Cyberbullying Prevention Act, would criminalize the transmittal of any content online “with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person... to support severe, repeated, and hostile behavior.”  

---

268 Gelman, supra note 29, at 1343.
269 Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong.
advocates are sounding panic alarms over the language contained in this law.\textsuperscript{270} They seem to forget our courts already interpret similar language in other contexts such as workplace sexual harassment, and can fashion rules and balancing tests that can protect speech while still protecting the likes of Megan Meier and Tyler Clementi. ZNP goes further than the proposed law, because if the right to be left alone means anything, it must mean that any identifying information should be removed from websites. It also does not go as far as the proposed law, because it does not focus on criminal sanctions, but on prevention—getting the content off servers as quickly as possible before the Internet’s speed, reach, and permanence make scrubbing impossible.

Other countries have already started to examine this problem in earnest, and their experiences can be instructive. In South Korea, the law requires websites with more than 300,000 visits a day to require posters give their real names, while smaller sites are exempt.\textsuperscript{271} Legislators are proposing laws that would allow prosecutors to file charges for online libel without the victims’ consent.\textsuperscript{272} Their aim is to “keep cyberspace from becoming a public toilet wall.”\textsuperscript{273} In the European Union, meanwhile, European Consumer Commissioner Meglena Kuneva has proposed a “Digital Agenda” to address problems raised by the use of personal consumer data by consumers surfing the web and conducting online shopping.\textsuperscript{274} European regulators have laid out some preliminary rules for privacy for social networking


\textsuperscript{271} Lee, \textit{supra} note 40, at 51.

\textsuperscript{272} Id.

\textsuperscript{273} Id.

sites, including offering privacy-friendly default settings, advising users that pictures should only be uploaded with the individual’s consent, setting a maximum period on retaining data on inactive users, and allowing pseudonyms.\textsuperscript{275} While these rules are somewhat tougher than those in the United States, they are still somewhat “vague”\textsuperscript{276} and do not address the right to be invisible from the Internet if one so chooses.

Noted privacy expert Professor Daniel Solove suggests what is the most comprehensive solution to these problems so far. He writes:

\begin{quote}
We should expand the law’s recognition of privacy so that it covers more situations. We must abandon the binary view of privacy, which is based on the archaic notion that if you’re in public, you have no claim to privacy. Instead, we must recognize that privacy involves accessibility, confidentiality, and control . . . . More broadly, the law should afford people greater control over their personal information.\textsuperscript{277}
\end{quote}

ZNP would allow the law to rebalance privacy interests so that people can actually control their presence on the Internet if they wish.

Federal law already provides a mechanism by which content owners can send takedown notices to website operators and Internet service providers to demand they remove copyrighted content from their websites and networks.\textsuperscript{278} Some scholars have suggested a similar law permitting victims of defamation to issue takedown notices to websites and Internet Service Providers to remove false and damaging user posts in return for legal immunity.\textsuperscript{279} Of course, most network operators and site owners are already immune under the Communications Decency Act (CDA),\textsuperscript{280} but that fact alone should not preclude a re-

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{276}] Id.
\item[\textsuperscript{280}] See infra text accompanying notes 281–84.
\end{itemize}
\end{footnotesize}
examination of that immunity and whether it ought to come with a higher price in protecting consumer privacy.

The CDA provides immunity to website operators, including social media websites, from defamation liability for content submitted by users. \[^{281}\] Although this immunity has been criticized, \[^{282}\] it is clear that the Act is meant to promote a robust First Amendment-based approach to the Internet. One proposal to reform the Act calls for a “pragmatic” revision “in such a way as to require a heightened standard on the part of those seeking redress, yet leave open the opportunity for recourse in situations where complainants meet the high threshold.” \[^{283}\] Another proposal suggests amending the Act to permit hostile environment sexual harassment claims. \[^{284}\] Even if these proposals were adopted, however, they would only address the remedial stage of privacy violations, not the critical pre-viral stage when real harm can be averted.

In making this argument, I am cognizant of concerns that commercial enterprises become de-facto censors. Companies like Google already face pressures to act as censors daily when governments request certain types of videos (typically those deemed to be insulting to local leaders) be removed from YouTube. \[^{285}\] Censorship, whether by government or private actors, is not the focus here. \[^{286}\] Rather, the focus is on the ability of citizens to demand their presence be removed from a website because of their right to be left alone.

Legislators who ignore this problem do so at their own political peril. In a survey of one thousand Americans by TRUSTe, an organization that monitors privacy policies on the

---


\[^{282}\] See John E. D. Larkin, Criminal and Civil Liability for User Generated Content: Craigslist, A Case Study, 15 J. TECH. L. & POL’Y 85, 111 (2010); Auerbach, supra note 165, at 1646; Dickinson, supra note 37, at 882; Jameson, supra note 25, at 248; Kim, supra note 28, at 1041–42.

\[^{283}\] Richards, supra note 35, at 184, 215–16.

\[^{284}\] Norby-Jahner, supra note 36, at 259.

\[^{285}\] See Jeffrey Rosen, Google’s Gatekeepers, N.Y. TIMES, Nov. 30, 2008, at MM50, for an excellent essay on Google’s role as censor.

Web, more than ninety percent called online privacy a “really” or “somewhat” important issue. A recent poll of four hundred teens aged fifteen to eighteen showed that ninety-two percent believed they should be able to request the deletion of all their personal information held by a search engine, social network, or marketing company. Another online poll asked, “Should there be laws allowing people to remove data about themselves from companies that compile profiles online?” More than ninety-three percent of survey respondents answered “yes.”

I am not arguing that someone who voluntarily posts information on the Internet, freely available without restriction, should not have an expectation that the material may “go viral” even if the intent was to reach a limited audience. In Moreno v. Hartford Sentinel Inc., a California appellate court held that an individual who published information on the Internet could not have a reasonable expectation that it would remain private. By posting information on MySpace, a person opens that information to the public at large. In another California case, a jury convicted a defendant accused of vehicular manslaughter with gross negligence when the defendant claimed innocence in a traffic accident, but had posted on her MySpace page: “If you find me on the freeway and you can keep up I have a really bad habit of racing random people.” The question of whether employers may sanction employees who use employer-owned equipment to communicate non work-related matters or post on social media sites, is also a developing area of law and most

287 Stephanie Clifford, Many See Privacy on Web as Big Issue, Survey Says, N.Y. TIMES, Mar. 16, 2009, at B5.
290 Id.
292 Id.
cases are leaning towards the employer.\footnote{294 See Dionne Searcey, Employers Watching Workers Online Spurs Privacy Debate, WALL ST. J., Apr. 23, 2009, at A13.} In a case involving the right of a police chief to read private text messages of a subordinate using city-owned equipment, the Supreme Court found no constitutional violation in a 9–0 decision.\footnote{295 City of Ontario v. Quon, 130 S. Ct. 2619, 2621, 2624 (2010).} These are correct outcomes, because all Internet users bear some responsibility for knowing how the Internet works, especially the three characteristics of reach, speed, and permanence. On the other hand, a user who uses the Internet with wisdom and takes precautions (such as requiring a password to access sensitive information) should not be subject to the same analysis.

There is already some precedent for allowing the government to place restrictions on the Internet. Legislation currently pending in Congress would create blacklists of Internet domain names to allow content owners unprecedented control to deny access to sites that allegedly infringe copyrights.\footnote{296 David Segal & Aaron Swarz, Congress Has Plans for an Internet Blacklist in the Works—Let’s Stop This Now, ALTERNET (Oct. 1, 2010), http://www.alternet.org/story/148377/congress_has_plans_for_an_internet_blacklist_in_the_works_%28__let%27s_stop_this_now.} Other legislation would require all communications on the Internet to allow wiretapping by authorities.\footnote{297 Charlie Savage, U.S. Is Working to Ease Wiretaps on the Internet, N.Y. TIMES, Sept. 27, 2010, at A1.} Corporations are engaged in a heavy lobbying effort to permit traffic shaping in order to better manage their networks and maximize revenue, an effort fiercely opposed by Net Neutrality advocates.\footnote{298 See, e.g., Joe Nocera, The Struggle For What We Already Have, N.Y. TIMES, Sept. 4, 2010, at B1.} These initiatives place a premium on national security and corporate profits. As a society, are we willing to say that individual privacy is not at least as important as either national security or corporate profit?

\section*{IV. Conclusion}

Technologies evolve. Web services such as Facebook and Twitter have taken off in ways few imagined possible during the height of the dot com boom in the late 1990’s. Already, a new version of web programming known as HTML5 brings the promise of tremendous power and ease for web users, while
simultaneously “open[ing] the Pandora’s box of tracking [on] the Internet.”299 The city of Leon, Mexico, is creating a database of irises of its more than one million citizens, and installing large scale iris scanners that can snap up to fifty people per minute in motion, without their knowledge or consent.300 The scanners will allow residents to catch a train or bus, or take money from an ATM, using only an iris scan.301 Future applications include the ability to track a person from the point they are “browsing on Google and find[] something they want to purchase, to the point they cross the threshold in a Target or Walmart and actually make the purchase.”302 Tomorrow’s privacy threats have not even been thought of yet.

The Internet is a wonderful tool that has brought the world closer, facilitated commerce, and opened the world to new ideas and paradigms. It can also be a tool for destruction and pain, and no current laws protect the right of a citizen to have zero presence on the Internet. The Internet has no media equivalent, and should be treated differently. Its reach, speed, and permanence mean that the only way to avert wholesale wrecking of someone’s life is to create a new right that would allow citizens who meet certain qualifying conditions to demand the virtual eradication of any presence of their life on the Internet. Zero Net Presence, if properly implemented, can preserve the essential functions of the Internet while rebalancing privacy interests in favor of the right to be left alone.

301 _Id._
302 _Id._