

New Public Spaces

John Palfrey⁼

Submission to Harvard Civil Rights–Civil Liberties Law Review’s
Inaugural Issue of *Amicus*
October, 2009

Digital environments are becoming the most important public spaces of the twenty-first century. These digital spaces are where many young people—and many older people, too—spend enormous amounts of time. These spaces are akin to the public parks, schoolyards, malls, and lecture halls of the physical world.¹ These are places where social lives take place, where nearly all information is found and republished, and where important functions like learning and participating in civic life occur. With every passing year, digital technologies are mediating more and more of the ways that we lead our lives.

In this essay, I explore several of the privacy and speech problems that arise in the context of lives partially mediated by digital technologies. I conclude by arguing that we should focus not just on the civil rights and civil liberties problems, but also on the opportunities afforded by life in these new public spaces online.

Risks Associated with Life in Online Public Spaces

Just as there are great things about life online, so, too, are there risks. Consider the prevalent behavior of those young Internet users who lead lives extensively mediated by digital technologies. Not all young people use technology the same way. There are important variations based on where one lives in the world, how much money one has, what age one is, one’s level of literacy, one’s gender, and so forth. Here, though, I focus on youth in developed countries, where Internet access is nearly ubiquitous and where the vast majority of young people go online multiple times per day.²

These wired young people do not distinguish much between life online and life offline—it is all just life. Teachers and parents, lawyers and law enforcement officers, technology companies and social networks: we all need to heed this lesson, too. And as we seek to protect our children in this hybrid world (as well as to live in it ourselves), we need to be sure not to trample on civil liberties like speech and privacy. Nowhere in today’s world

⁼ John Palfrey is the Henry N. Ess III Professor of Law and Vice Dean for Library and Information Resources at Harvard Law School. He is also Faculty Co-Director of the Berkman Center for Internet and Society at Harvard University. This overview draws upon research conducted with Urs Gasser and other colleagues at the Berkman Center, as well as many conversations with danah boyd, Dena Sacco, Jonathan Zittrain, and others about issues of civil rights and civil liberties on the Internet.

¹ See generally JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET—AND HOW TO STOP IT* (2008) (especially Chapter 9, “Meeting the Risks of Generativity: Privacy 2.0,” discussing public and private spaces and roles on the Internet).

² This argument draws heavily upon the research for a book by the author and Urs Gasser, entitled *BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES* (2008).

are people striking this balance well; nowhere in today's world do we yet see ample protection of safety and of civil liberties online. It is a noble and important goal, for our children and for all of us.

As we seek to understand emerging problems online—such as threats to safety and the privacy of our children—and to anticipate the future, we have to listen to our children and our grandchildren and seek to understand how their behaviors differ from those who are older.

Take the concept of identity, for instance. Identity formation is one of the ways in which young people often use technologies and relate to the world differently than those who came before.³ Young people shape their identities by what they wear and who their friends are, just as they always have. But they also shape their identities through the profiles that they create in online social networks, through the personalities that they develop while instant messaging and texting, and through blogs and LiveJournals and their avatars in games and virtual worlds. Identity is shaped in this converged space of online and offline.

Young people interact with both friends and strangers online. Their understanding of the word “friend” (as in, to “friend” someone on Facebook, for instance) is changing. They may consider someone they have never met, other than in an online chatroom, to be a close friend. They spend a great deal of time online with their friends—as they play games together, plan something that they might do later, share music and movies, or just chat—and chat, and chat (or: text, and text, and text). These are the spaces where growing up takes place.

Old Problems in New Spaces

Over the past fifteen years, the sharply growing use of the Internet by large numbers of people, including children, has given rise to a series of public policy issues. Threats to civil rights and civil liberties—not new threats, but rather familiar ones—arise frequently as a result. Sometimes these speech and privacy issues arise directly from the behavior of Internet users. In other cases, the issues arise as a result of the fixes to which we turn to protect Internet users from various harms that they may encounter online.

The behaviors of young people in these new public spaces are sometimes perfectly healthy and sometimes risky, just as in physical space. Sometimes people meet others who do terrible things to them, whether online or in physical environments. Sometimes, people are cruel to one another in ways that they would not be in real space, when face-to-face. After all, it is much easier to leave a hard conversation online than it is offline. It is no surprise that this should be so: these are places where kids are spending a great

³ See generally YOUTH, IDENTITY, AND DIGITAL MEDIA (David Buckingham ed., 2008).

deal of time, where they are playing and learning and just hanging out.⁴ They leave a lot of personally identifiable information about themselves around these places. And they are often experimenting with who they are and how they want to interact with other people.

Research tells us that bullying online, for instance, is a growing concern for young people, parents, and teachers.⁵ Young people do more harm to one another—peer to peer—than adults do to them. This is a very important point. We need to think in terms of how “friends” act toward one another just as we think about how strangers might reach our children. The problems that can occur are terrible here, too, and they are increasingly being reported as common. The psychological harm done to young people by their peers online can be devastating.

Also, young people can access much more content—information, imagery, and just about any kind of media one can imagine—online than they ever could before. Sometimes, that level of access is terrific. Sometimes, they are accessing information that helps them to learn about their world—to expand their horizons, to help them to think more critically, to give them a way into a public discourse where they can contribute their own voices, to find things that could never be housed in a single library. For some young people, learning on their own online is a big part of their growing up, and it’s a good thing for the individual and for society at large. But it is also easy to access pornography. Young people may also create (wittingly or unwittingly) child pornography in the course of leading social lives mediated by digital technologies. Parts of this problem are not entirely new: of course, young people have sought out pornography in the past, or a friend, an older cousin, or a sibling has presented it. The difference today is the ease with which pornography can be created and accessed online, from anywhere at any time.

We are not necessarily seeing bigger problems or more crime in the era of the Internet, but we are seeing some old problems become much trickier. It is imperative that we figure out how to get these skills, tools, and partnerships to our teachers, parents, mentors, and to young people themselves so that we can cooperate in meeting these challenges together, rather than relying upon one-size-fits-all approaches that will not resolve the core issues at stake.

We often turn first to the idea that technology can solve the problems that technology has wrought. This is a mistake. First, we need to be careful not to see these as problems “created by” technology. Digital technologies do not have a nature; these are tools and media that allow human beings to do what we want to do.⁶ In this spirit, it is essential to recognize that the underlying behavior is the key place to focus. Second, while

⁴ See Mizuko Ito et al., *Living and Learning with New Media: Summary of Findings from the Digital Youth Project* (John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning, Nov. 2008), <http://digitalyouth.ischool.berkeley.edu/report>.

⁵ See ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES: FINAL REPORT OF THE INTERNET SAFETY TECHNICAL TASK FORCE 14-21, app. (John Palfrey et al. eds., 2009), <http://cyber.law.harvard.edu/pubrelease/isttf/> (literature review summarizing the findings of the most credible studies on risks to children online, such as bullying).

⁶ See generally LAWRENCE LESSIG, CODE 2.0 (2008), available at <http://codev2.cc/>.

technologies can sometimes help address problems online, these approaches are rarely a panacea. And sometimes, using technologies to solve such problems can cause more harm than good—certainly when one factors in the costs to civil liberties. Technical online filtering is a primary example of such a technology, which can be helpful to parents of young children when used in the home, but which does not scale well to usage on the broader network or in many institutional settings.

These problems of online life—such as child safety—are not easily or quickly solved. They are so complex as to defy easy, one-off answers. We cannot just expect that a single technology—such as online filtering—will keep our kids from danger. We cannot just “pass a law” against these things and imagine that we can enforce that law in the way we have always enforced the law and hope that all will be well. The problems do not lend themselves to such easy answers.

That is not to say that the law has no place in solving these enduring online problems. We can and should pass laws against the crimes—whether committed online or offline—and we should enforce them with great vigor. Most of the time, we already have laws against harming children or stealing from other people. The trick is to ensure that the laws and legal infrastructure enables enforcement, and then figure out how best to enforce them in these new environments. These are primarily prevention and enforcement issues, not issues where we need extensive new legislation or technological systems in place to solve them (though technology and resources for law enforcement can play very helpful roles). And as we adapt the law or the technology to address these concerns, we need to be cognizant of the risks to civil rights and civil liberties of the fixes that we bring to bear on the problems.

Restraints on Free Expression

In the interest of protecting children (and adults, in some cases) from harmful people and harmful content in these new public spaces, policy-makers—whether legislators, school superintendents, or those who run corporate networks—have turned to a range of strategies that often threaten to restrict free expression. A familiar initial approach is to implement technical filtering software that disallows an Internet user from accessing material online that appears on a “blacklist” of blocked sites. Most of the time, that involves deploying off-the-shelf software programs that technology companies such as Secure Computing sell. These for-profit corporations make decisions about which sites ought to be blocked or permitted, based on various criteria that relate to categories of speech those seeking to censor disfavor. In the context of home computing, many parents use these systems to keep their children in safe areas of the Internet. The issue grows more complicated when this same approach is applied to keep adults from accessing online content. While much Internet filtering is geared toward protecting children from unwanted content online, adults, too, often encounter Internet filtering. This filtering takes place in some libraries, schools, and workplaces.

Technical Internet filtering is controversial. One reason is that it rarely works particularly well: users can circumvent these filters without too much trouble. Another is that it is rarely very accurate: the censor must choose between a list of sites to block that is either overbroad (i.e., too many sites are blocked) or underbroad (i.e., too few sites are blocked), especially as content online changes quickly. And it takes on complicated international dimensions. More than three dozen countries around the world—including China, Iran, and Uzbekistan—censor the Internet to keep information from their citizens. As of 2009, the web is increasingly not a “world wide web” but rather a series of networks that are connected to one another, where users see different things in different countries—a “China Wide Web,” an “Iran Wide Web,” an “Uzbek Wide Web.”⁷

Further restraints on free expression take place in virtual worlds and social network sites. The restriction of speech that occurs online takes place often within private spaces, such as social network sites (Facebook, MySpace) and virtual worlds (Second Life). These constraints on expression may be crucial to the protection of certain shared values. But the First Amendment does not ordinarily govern these decisions to restrict speech, as these companies are not “state actors.”⁸ The extent to which life is now taking place in these new public spaces owned by companies is giving rise to another round of questions about speech restrictions by private actors, as we saw with company towns (e.g., *Marsh v. Alabama*⁹) and, more recently, with shopping malls (e.g., *Pruneyard Shopping Center v. Robins*¹⁰).

The complete list of speech-related disputes on the Internet, often but not always prompted by safety concerns, is too long for this short article. But a particularly current dispute is worth highlighting: one of the hottest policy issues on technology matters before the Congress and the Federal Communications Commission (FCC) is “network neutrality.” This issue relates to whether Internet Service Providers (ISPs) and others between a person and the information she seeks can or should block certain information based upon its form or its content. All ISPs block some information for one reason or another, including “reasonable network management,” but some ISPs have blocked more content than others for policy reasons. The Obama administration’s new FCC chair, Julius Genachowski, has made this matter a priority.¹¹ Debates over speech online, seen through the lenses of child safety and network neutrality, will rage for years to come.

⁷ See generally ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING (Ronald Deibert, John Palfrey, Rafal Rohozinski & Jonathan Zittrain eds., 2008). Visit <http://opennet.net> online for detailed analyses of Internet filtering by country and by region.

⁸ See generally 2 RONALD D. ROTUNDA & JOHN E. NOWAK, TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND PROCEDURE § 16.1(a) (4th ed. 2007).

⁹ *Marsh v. Alabama*, 326 U.S. 501 (1946); see also Molly Shaffer Van Houweling, Sidewalks, Sewers, and State Action in Cyberspace, <http://cyber.law.harvard.edu/is02/readings/stateaction-shaffer-van-houweling.html> (last visited Oct. 15, 2009) (unpublished draft) (considering the legal issues to which private ownership of online spaces gives rise).

¹⁰ *Pruneyard Shopping Center v. Robins*, 447 U.S. 74 (1980).

¹¹ See Farhad Manjoo, *I Heart the New FCC Chairman*, SLATE, Oct. 9, 2009, <http://www.slate.com/id/2231917/>.

Threats to Individual Privacy

Privacy is just as substantial a concern as speech in online debates. Two basic facts give rise to this concern. First, these new public spaces are, by and large, owned and controlled by private parties. These private entities often make their money by rendering advertisements to their customers based on perceived preferences. As a result, these companies have an incentive to collect and retain more, not less, information about their customers in order to target these advertisements effectively. Second, many Internet users share more information about themselves in these digitally mediated environments than perhaps they would in other environments. Young people enjoy extensive use of social networks, where they relate to one another across their respective Facebook and MySpace pages. Older people, too, share a great deal of information about themselves in online environments such as dating sites like Match.com and JDate.com. Vast amounts of information about what Internet users are seeking on the web are stored in the log files of search engines, including the runaway search leader, Google.

In addition to information individuals share and companies collect, states are able to collect more information today about their citizens than ever before. The Internet is a “surveillance-ready” technology. Digital information about individuals may be searched in the form of bits of data that flow through rivers and into oceans of data. These rivers are full of information that passes by a given point, or series of points, in a network and can be intercepted; these oceans are stocked with information that can be searched after the fact; and the rivers arise from springs that can be watched at the source. The data subject to search by states may be held in private hands as well as public. The Fourth Amendment by and large does not protect Americans from the search by the state of information held in private hands, the so-called “third-party data problem.”¹²

The net result is that both young people and adults are living their lives in new public spaces that we have not yet determined how to regulate without setting ourselves up for large-scale privacy concerns in the future. No generation has lived cradle-to-grave with so much of their lives recorded for posterity, searchable by other people, by corporations, and by the state. Those who study online privacy worry a great deal about the combination of three factors: the aggregate effect of this pattern of behavior online; the incentives for companies to collect, store, and use data about individuals; and the extent to which the law has not kept pace with changes in behaviors and practices associated with these new public spaces.

From Problems to Opportunities: Speech in New Public Spaces

The *Harvard Civil Rights–Civil Liberties Law Review* (“CR–CL”) (<http://harvardcrcl.org/>) is launching *Amicus* (<http://harvardcrcl.org/amicus>) at a propitious time. Just as social lives are moving in part to these new public spaces, much of our public discourse, too, is moving to online venues. There is a palpable need to establish new venues and formats for serious, constructive discussion of the important

¹² See Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1085–86 (2002).

issues of the day. CR–CL and other law journals have a terrific opportunity: to design and to build these venues in cyberspace, to build them out with reflections on the important matters of the day, and to iterate in their form and content as they go.

These new public spaces offer ways to build original connections between topics and arguments that have not yet been made. The greatest opportunity presented by these new digital technologies is the potential of the networked public sphere, described in compelling fashion by Yochai Benkler in his pathbreaking work, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. (Link to http://cyber.law.harvard.edu/wealth_of_networks/Main_Page) Benkler prompts us to consider new modes of information production about the way we talk — individually and collectively—about the most important issues of our day, and about the effects of these changes on modern complex democracies.¹³ *Amicus*, and efforts like it by other law reviews, can contribute to the creation of the networked public spheres heralded by Benkler.

The theory is sound. But how will we know in practice whether these new forms and modes of scholarly publishing online are a success?

First, and, in a way, most important: the ordinary metrics of success need to apply online, just as they do offline. The content of the publication, and the discourse to which it gives rise, must meet traditional, high standards of quality, novelty, relevance, and so forth. The discourse will need to contribute to the record of scholarship and knowledge. It must find and engage a readership.

For a new mode or form of scholarly publishing to succeed, though, these basic metrics are necessary but not sufficient. There will need to be something more to justify a shift in time, cost, and emphasis from the current model to a new model, even if the new model is a supplement rather than a replacement for the old. We—as prospective authors, readers, and commenters—have a finite amount of time, energy, and attention. This “something more” might sensibly take advantage of the special qualities of the online medium and the changing processes by which some people (and many young people) are creating, accessing, and responding to information.

The editors of *Amicus* no doubt have many ideas on this score, but here are a few possibilities for this “something more.” A new form might allow for new connections to be developed between and across existing arguments about scholarly matters in law. These connections might be built using a combination of footnotes and hypertext links on the open web, much as proprietary databases do (Lexis and Westlaw, for instance) for the professionals. The process of building these connections, though, might be carried out both by the author and by readers, perhaps with an editing function retained by the publisher of the journal to ensure quality (or perhaps left in the hands of the community at large, in the spirit of Wikipedia).

¹³ See YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* (2006).

This new mode might also support the growing interdisciplinarity of the study of law. *Amicus* might enable us to draw tighter linkages between legal arguments and the social science scholarship on which we occasionally draw. It might enable authors to point more directly into data sets from the census or from economists. For instance, Stephen Churchill's article on discrimination in the workplace in this inaugural issue of *Amicus* cites to several studies, many of which have presumably not been conducted by lawyers. Over time, as more and more scholarship from various disciplines is published online, an article such as Churchill's might be linked to those studies to which he cites, such that a reader might easily move from the law article to the data and back again. We see glimpses of this promise in databases such as Lexis-Nexis and Westlaw. But the next-generation version of these linkages might be freely available on the web at large and across disciplinary boundaries, not confined to professionals and to a single field of inquiry.

A new form might also allow for ideas developed in the academy to reach broader, or at least different, audiences. There are no doubt some potential followers of legal scholarship who are less likely to read a bound law review volume in a law library (or in Hein Online) than they are to come across arguments online, in open formats that are indexed well by Google and other search engines (in ways that even PDFs of law review articles online often are not). William Yeomans' essay on the widely-followed discrimination case involving New Haven's firefighters, *Ricci v. DeStefano*,¹⁴ might well appeal to a broader audience in *Amicus* than it would in a traditional law review article published only in hard-copy and in its traditional long form. The effective curation of these materials might help address the problem of credibility and information overload on the web, as Internet users often struggle to know whom to trust when it comes to online information. The brands of well-run law reviews might well serve a helpful signaling function in the online environment, much as they have offline. The tone of this discourse, too, might be adapted so as to draw readers in, rather than to discourage them, as I fear we in the legal academy do from time to time.

A final positive difference might be that a format that is less rigid than the classic, heavily footnoted law review article might lead to the development and publication of new arguments that could then be vetted and refined as a result of criticism from a wide online audience. These arguments, if they withstand the feedback, might then be developed further over time, in the best case into full-blown articles or books that will themselves stand the test of time. There are of course other formats today, such as working paper series and blogs, that already allow for the floating of such trial balloons. But new formats, such as *Amicus* and its kin, might lead to additional arguments being developed in these ways, with different kinds of constructive feedback. An example of another such effort, called *Publius*, is curated by the Berkman Center for Internet & Society at Harvard University with the purpose of drawing out the arguments related to how the networked public sphere is governed. (Link to <http://publius.cc>) These new formats can be developed at low cost and low risk and adapted—ideally, optimized over time to serve this scholarly purpose.

¹⁴ 129 S. Ct. 2658 (2009).

Last, it's worth noting that CR–CL is launching this new initiative at a time when there is massive upheaval in the publishing industry. This upheaval is already changing how we communicate, inside and outside the scholarly community. Within the academic setting, these changes take the form of debates over whether to publish our work on an open access basis¹⁵; whether to grant copyright interests in academic work at all¹⁶; and whether and how to credit (or punish) scholars for work published in non-traditional, online formats.¹⁷ Should, for instance, a tenure review committee recognize works that meet traditional standards for scholarly contribution (novel, constructive, well-argued, well-researched, and so forth), but not published as long-format, well-footnoted articles in prominent journals or as monographs published by well-regarded university presses? The success or failure of *Amicus*, along with other initiatives in scholarly publishing, may help us to answer these questions over time.

Discourse online will not be uplifting and constructive just because some of us happen to have high hopes for the democratizing power of new digital technologies. As more and more public discourse moves online with each passing year, it is crucial that we structure serious conversations into the fabric of the net, into these new public spaces. In some cases, merely digitizing materials and moving them online where people can find them may be enough. In other cases, we will need to design and build entirely new venues and link arguments within them to one another. With commitment and a bit of daring, *Amicus* will, before too long, become an important, trusted venue for discussion of some of our most pressing issues in Benkler's networked public sphere.

¹⁵ See, e.g., Open Access News, <http://www.earlham.edu/~peters/fos/fosblog.html> (last visited Oct. 15, 2009).

¹⁶ See, e.g., Steven Shavell, Should Copyright of Academic Works be Abolished?, <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Copyright%207-17HLS-2009.pdf> (last visited Oct. 15, 2009) (unpublished draft).

¹⁷ See Paul L Caron, *Are Scholars Better Bloggers?—Bloggership: How Blogs are Transforming Legal Scholarship*, 84 WASH. U. L.Q. 1025 (2006).