THE COLUMBIA JOURNAL OF
LAW & the ARTS

A QUARTERLY JOURNAL OF LAW AND THE ARTS,
ENTERTAINMENT, COMMUNICATIONS AND INTELLECTUAL PROPERTY

A Declaration of the Dependence of Cyberspace
Alex Kozinski and Josh Goldfoot

Vol. 32, No. 4 ♦ Summer 2009

COLUMBIA UNIVERSITY SCHOOL OF LAW

A Declaration of the Dependence of Cyberspace

Alex Kozinski* and Josh Goldfoot**

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

That was the opening of "A Declaration of the Independence of Cyberspace."[1] The would-be Cyber-Jefferson who wrote it was John Perry Barlow, a co-founder of the Electronic Frontier Foundation, a noted libertarian and a Grateful Dead lyricist. He delivered the Declaration on February 8, 1996, the same day that President Clinton signed into law the Communications Decency Act. That Act was chiefly an early effort to regulate internet pornography. Many had concerns about that law, and, indeed, the Supreme Court would eventually declare most of it unconstitutional.[2]

Barlow's argument invoked what he believed was a more decisive criticism than anything the Supreme Court could come up with. Barlow saw the internet as literally untouchable by our laws. Extolling the power of anonymity, he taunted that "[o]ur identities have no bodies, so, unlike you, we cannot obtain order by physical coercion." Unlike the Declaration of Independence, this was not a declaration that cyberspace was newly independent; it was an observation that cyberspace had always been independent, and will always remain independent, because its denizens were beyond the law's reach.

Needless to say, the weary giants of flesh and steel did not take kindly to the Declaration. They fought back hard and won numerous battles: witness the fall of Napster, Grokster, Aimster and innumerable other file-sharing and child-pornography-trading sites and services. Ironically, the Department of Homeland Security now has a "National Strategy to Secure Cyberspace." Even the cyber-libertarians have shifted their focus: the organization Barlow co-founded is now a major proponent of what it calls "network neutrality" regulation, which is itself a form of regulation of how subscribers access the internet and how content reaches them.

---

* Chief Judge, United States Court of Appeals for the Ninth Circuit.

** B.A., Yale University; J.D., University of Virginia School of Law; Trial Attorney, Department of Justice, Criminal Division, Computer Crime & Intellectual Property Section. The views expressed in this article are the views of the authors and do not necessarily represent the views of the U.S. Department of Justice or the United States.

1. John Perry Barlow, A Declaration of the Independence of Cyberspace (Feb. 8, 1996), http://homes.eff.org/~barlow/Declaration-Final.html

2. Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

In other ways, the Declaration has proved prescient. As far back as 1996, Barlow had identified that the internet poses a significant problem for governments. Then, as now, people used the internet to break the law. The internet gives those people two powerful tools that help them escape the law's efforts to find and punish them. First, the internet makes anonymity easy. Today any 11-year-old can obtain a free e-mail account, free web page and free video hosting. The companies that provide these things ask for your name, but they make no effort to verify your answer; as a result, only boy scouts tell them the truth. You can be tracked through your internet protocol address, but it is not too tough to use proxies or some neighbor's open Wi-Fi connection to get around that problem. Thus, if your online conduct ever hurts someone, it will be difficult for the victim to ever find out who you are and sue you.

Second, the internet makes long-distance international communication cheap. This allows the world's miscreants, con-artists and thieves easy access to our gullible citizens. When people find out they've been had, they often find that they have no practical recourse because of the extraordinary difficulties involved in pursuing someone overseas. The internet's global nature makes it easy for people to hide from our courts.

These two advantages of internet law-breakers pose a serious and recurring problem. That problem has been particularly painful for intellectual property rights holders. It is common knowledge that instead of buying music or movies, you can use the internet to download perfect copies for free from individuals known only by their IP addresses. In some cases, wrongdoers have become so bold that they demand payment in exchange for the opportunity to download infringing material.

The situation seemed unsolvable to Barlow and others in 1996. Armed with anonymity and invulnerability, internet actors could ignore efforts to apply law to the internet. Barlow concluded that the internet's nature posed an insurmountable barrier to any effort at legal enforcement. Some scholars even began work on theorizing how the diverse denizens of cyberspace might join together and go about creating their own indigenous legal system.[3]

But over time, a solution to Barlow's problem appeared. Let us entertain, for a moment, the conceit that there is a "cyberspace," populated by people who communicate online. The denizens of cyberspace exist simultaneously in cyberspace and in the real flesh-and-steel world. Their cyberspace selves can be completely anonymous; their real-life selves are easier to identify. Their cyberspace selves have no physical presence; their real-life selves both exist and have base material desires for PlayStations, Porsche Boxsters and Battlestar Galactica memorabilia. Their physical selves can be found in the real world and made to pay in real dollars or serve real time behind real bars for the damage their cyber-selves cause.

The dilemma that online law-breakers face is that their cyberspace crimes have real-life motives and fulfill real-life needs. Therefore, they need some way to

3. *See, e.g.*, David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, J. OF ONLINE L., Article 3, June 1995. Available at SSRN: http://ssrn.com/ abstract=943456

translate their online misdeeds into offline benefits. The teenager downloads that MP3 so that he can listen to it. The con-artist asks for money to be wired to him so that he can withdraw it and buy things with it. The fringe activist who e-mails a death threat to a judge does so in the hopes that the judge will change his behavior in the real world.

These internet actors usually rely on real-world institutions to get what they want. They use Internet Service Providers and hosting companies to communicate, and they use banks and credit card companies to turn online gains into cash. Without these institutions, they either could not accomplish their online harms, or they would not be able to benefit from them in the real world. Unlike anonymous cyberspace miscreants, however, these institutions have street addresses and real, physical assets that can satisfy judgments in the United States. By placing pressure on those institutions to cut off service to customers who break the law, we can indirectly place pressure on internet wrong-doers. Through this pressure, we have a powerful tool to promote online compliance with the law.

In some cases, for some offenses, we have the legal tools to do this already. For intellectual property cases, the tool for holding those institutions liable is secondary liability: contributory and vicarious infringement. The Ninth Circuit has led the way in developing the law in this area. In *Perfect 10 v. Google*, the court noted the cases that had applied contributory infringement to internet actors, and summarized their holdings as saying that "a computer system operator can be held contributorily liable if it has actual knowledge that specific infringing material is available using its system . . . and can take simple measures to prevent further damage to copyrighted works . . . yet continues to provide access to infringing works."[4] In other words, if people are using your stuff to infringe copyrights, and you know about it, and you can easily stop them, but you do not, then you are on the hook.

The motive behind secondary liability is simple. Everyone agrees that the direct infringers ideally should be the ones to pay. But there might be too many of them to sue; or, they might be anonymous; or, they might be in Nigeria. This can make them apparently invulnerable to lawsuits. That invulnerability has a cause: someone is providing the tools to infringe and looking the other way. The doctrine of secondary liability says that such behavior is unacceptable. Those who provide powerful tools that can be used for good or evil have some responsibility to make sure that those tools are used responsibly.

Put more directly: with some changes to the law, the institutions that enable the anonymity and invulnerability of cyberspace denizens can be held accountable for what their anonymous and invulnerable customers do. The anonymity of cyberspace is as much a creation of men as it is a creation of computers. It is the result of policy choices. We have accepted, without serious examination, that it is perfectly fine for a business to grant free web space and e-mail to any schmuck who comes off the street with an IP address, and then either keep no record of that grant or discard the record quickly. Businesses that do this are lending their

4. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007) (quotations, citations and italics omitted).

powerful and potentially harmful capabilities and demanding little accountability in return. That arrangement has obvious benefits but also obvious costs. The victims of online torts and crimes bear these costs, and those victims are, overwhelmingly, third parties. They include big movie studios, middle-aged internet newbies and, unfortunately in some cases, young children.

If the legal rules change, and companies are held liable more often for what their users do, then the cost of anonymity would shift away from victims and toward the providers. In this world, providers will be more careful about identifying users. Perhaps online assertions of identity will be backed up with offline proof; providers will be more careful about providing potential scam artists in distant jurisdictions with the tools to practice their craft. All this would be expensive for service providers, but not as expensive as it is for injured parties today.

Secondary liability should not reach every company that plays any hand in assisting the online wrong-doer, of course. Before secondary liability attaches, the plaintiff must show that the defendant provided a crucial service, knew of the illegal activity, and had a right and a cost-justified ability to control the infringer's actions. This rule will in almost every case exclude electrical utilities, landlords, and others whose contributions to illegal activity are minuscule.

While we have come a long way from Barlow's Declaration of the Independence of Cyberspace, the central idea behind it—that the internet is a special place, separate somehow from the brick and mortar world, and thus subject to special rules and regulations, or no rules and regulations—lingers. The name itself has a powerful influence: we don't speak of "telephone-space" or "radio-space" or "TV-space"—though we do have Television City in Hollywood. Prior technological advances that aided in connecting people were generally recognized as tools to aid life in the real world; no one claimed that they made up a separate dimension that is somehow different and separate from the real word. Every time we use the term "cyberspace" or the now-outmoded "Information Superhighway," we buy into the idea that the world-wide network of computers that people use for electronic commerce and communication is a separate, organic entity that is entitled to special treatment.

This idea of cyberspace as a separate place subject to a different set of rules—one where courts ought to tread lightly lest they disturb the natural order of things and thereby cause great harm—still arises in many court cases.[5]

The first of these is *Perfect 10 v. Visa*—a case where one of the authors of this

5. Some disclaimers: One of the authors of this piece (Chief Judge Kozinski) sat on the panel that decided some of the cases given as examples here. He wants to make it clear that he won't re-argue the cases here. Both involved split decisions, and his views as to how those cases should have come out is set out in his opinions in those cases. His colleagues on the other side are not present to argue their positions and, in any event, it's unseemly to continue a judicial debate after the case is over. Furthermore, despite his disagreement with his colleagues, he respects and appreciates their views. The judges that came out the other way are some of dearest of his colleagues, and some of the finest judges anywhere. The disagreement is troubling, because they bring a wealth of intelligence, diligence, talent, experience and objectivity to the problem, and he can't quite figure out why they see things so differently.

piece was in the dissent.[6] The facts are simple: plaintiff produces and owns pictures of scantily-clad young women, which it sells online. It alleged that unknown parties had copied the pictures and were selling them online, at a lower price, using servers in remote locations where the legal system was not hospitable to copyright and trademark lawsuits, and, moreover, they could fold up their tents and open up business elsewhere if anyone really tried to pursue them. So the plaintiff didn't try to sue the primary infringers; instead, it went after the credit card companies that were processing the payments for what they claimed were pirated photographs.

This was by far not the first case that applied the doctrine of secondary infringement to electronic commerce. The cases go back at least to the 1995 case of *Religious Technology Center v. Netcom*,[7]—a case involving the liability of an ISP for damage caused when it posted copyrighted Scientology documents to USENET, at the direction of one of its users. And, of course, the *Napster*, *Aimster* and *Grokster* cases all dealt with the secondary liability of those who assist others in infringement.[8] *Perfect 10*, though, presented a novel question: how do you apply the doctrine of secondary infringement to people who help the transaction along, but never have any physical contact with the protected work?

Two excellent and conscientious Ninth Circuit jurists, Judges Milan Smith and Stephen Reinhardt, said there was no liability, whereas the dissenting judge concluded that there was. Visa, the dissent argued, was no different from any other company that provided a service to infringers, knew what it was doing, and had the ability to withdraw its service and stop the infringement, but did nothing.

This debate fits within a larger context. In the majority's rejection of contributory liability, it cited a public policy decision that found that the internet's development should be promoted by keeping it free of legal regulation. Relatedly, the majority distinguished some precedent by saying that its "tests were developed for a brick-and-mortar world" and hence "do not lend themselves well to application in an electronic commerce context."[9]

This argument channels Barlow's declaration that users of the internet are entitled to special treatment (or, as he would have it, entitled to *no* treatment). The chief justification for this argument is that the internet is so new, exotic and complicated that the imposition of legal rules will chill, stifle, discourage or otherwise squelch the budding geniuses who might otherwise create the next Google, Pets.com, or hamster dance. For example, the Electronic Frontier Foundation argued to the Supreme Court during the *Grokster* case that if the Ninth Circuit's opinion were reversed, the effect would "threaten innovation by subjecting product design to expensive and indeterminate judicial second-

6. Perfect 10, Inc. v. Visa Intern. Service Ass'n, 494 F.3d 788 (9th Cir. 2007).

7. Religious Technology Center v. Netcom, 907 F.Supp. 1361 (N.D. Cal. 1995)

8. *See* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002); In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003); Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

9. *Perfect 10*, 494 F.3d at 798 n.9.

guessing."[10] The Ninth Circuit *was* reversed, and if that decision slowed the pace of product design, no one seems to have noticed.

This argument became particularly central in a second case, *Fair Housing Council of San Fernando Valley v. Roommates.com*.[11] The case involved a claim that the commercial website Roommates.com violated state and federal fair housing laws by helping to pair up roommates according to their personal preferences, the exercise of which is allegedly prohibited by law. Again, one of the authors of this piece was a judge on that case, and was in the majority at both the panel and the en banc level—despite the efforts of some conscientious and brilliant dissenting judges, of whose intellectual rigor and commitment to the rule of law no one can doubt.

The majority mostly held that Roommates.com *could* be held liable, if the plaintiff's allegations were proven true. The court held essentially that an online business had to be held to the same substantive law as businesses in the brick-and-mortar world. The dissenters saw things quite differently; to them, the majority placed in jeopardy the survival of the internet. Here is a taste of the dissent:

> On a daily basis, we rely on the tools of cyberspace to help us make, maintain, and rekindle friendships; find places to live, work, eat, and travel; exchange views on topics ranging from terrorism to patriotism; and enlighten ourselves on subjects from "aardvarks to Zoroastrianism." . . . The majority's unprecedented expansion of liability for Internet service providers threatens to chill the robust development of the Internet that Congress envisioned. . . . [W]e should be looking at the housing issue through the lens of the Internet, not from the perspective of traditional publisher liability.[12]

And finally, the unkindest cut of all: "The majority's decision, which sets us apart from five circuits, . . . violates the spirit and serendipity of the Internet."[13]

The argument that a legal holding will bring the internet to a standstill makes most judges listen closely. Just think of the panic that was created when the Blackberry server went down for a few hours. No one in a black robe wants to be responsible for anything like that, and when intelligent, hard-working, thoughtful colleagues argue that this will be the effect of one of your rulings, you have to think long and hard about whether you want to go that way. It tests the courage of your convictions.

Closely related is the argument that, even if you don't bring down the existing structure, the threat of liability will stifle innovation, so that the progress we have seen in recent years—and the gains in productivity and personal satisfaction—will stop because the legal structure has made innovation too risky or expensive. The innovation argument is partly right but mostly wrong. Certainly, some innovators

---

10. *See* Brief for Respondents, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., No. 04-480 (9th Cir. Mar. 1, 2005), *available at* 2005 WL 508120 *and at* http://w2.eff.org/IP/P2P/MGM_v_Grokster/20050301_respondents_brief.pdf .

11. Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157 (9th Cir. 2008).

12. *Id.* at 1176-77 (footnote omitted).

13. *Id.* at 1177.

will shy away from legally murky areas. It's hard to think of a worse recipe for creativity than having a lawyer attend every engineering meeting. But promoting innovation alone cannot be a sufficient justification for exempting innovators from the law. An unfortunate result of our complex legal system is that almost everyone is confused about what the law means, and everyone engaged in a business of any complexity at some point has to consult a lawyer. If the need to obey the law stifles innovation, that stifling is just another cost of having a society ruled by law. In this sense, the internet is no different than the pharmaceutical industry or the auto industry: they face formidable legal regulation, yet they continue to innovate.

There is an even more fundamental reason why it would be unwise to exempt the innovators who create the technology that will shape the course of our lives: granting them that exemption will yield a generation of technology that facilitates the behavior that our society has decided to prohibit. If the internet is still being developed, then we should do what we can to guide its development in a direction that promotes compliance with the law.

For example, what use is "innovation" in creating a job hunting site if the innovators produce a site that invites employers automatically to reject any applicant from a particular race? Perhaps the job site is a bold new innovation that makes hiring far easier and more efficient than it has ever been. But if this site is used widely, it will facilitate racial discrimination in hiring—conduct that society has already decided it must prohibit. Similarly, is a file-sharing service such as Grokster worth the harm it causes by offering no built-in tools for identifying participants or establishing they have the right to "share" the files they copy? Far from *exempting* this growing industry from the law, we should vigorously *enforce* the law as the industry grows, so that when it is mature its services won't guide behavior toward conduct that society has decided to discourage. As difficult as it might be for innovators today, it is easier than the alternatives: forcing them to rebuild everything ten years down the road, or grudgingly accepting that we have surrendered key aspects of our ability to govern our society through law.

It is Barlow who is generally credited with taking the word "cyberspace" from the science fiction of William Gibson and applying it to the internet. In doing so, he launched the conceit that such a "space" exists at all. This was wholly unjustified. It is a mistake to fall into Barlow's trap of believing that the set of human interactions that is conducted online can be neatly grouped together into a discrete "cyberspace" that operates under its own rules. Technological innovations give us new capabilities, but they don't change the fundamental ways that humans deal with each other. The introduction of telephones and cars did create new legal questions. Those questions all revolved around what the acceptable uses of the new technologies were. How closely can you follow the car in front of you on the highway? Can you repeatedly dial someone's phone to annoy them? Can you tap into a phone conversation or put a tape recorder in a phone booth? Over time, courts and legislatures answered these questions with new legal rules. They had to; the essence of the controversy arose from the new technological abilities. But no one thought that telephones and cars changed the legal rules surrounding what was said on a telephone or where a car traveled. Can an oral contract be formed with a

telephone call? Of course; it is still two people speaking. Is it trespassing to drive across my neighbor's front yard? Of course; you are on his land.

Like cars and telephones, the internet prompts new questions about the acceptable uses of the new technology. Is port-scanning a form of hacking? When does title to a domain name legally transfer? While analogies to settled legal rules are helpful in answering these questions, they are not conclusive. Answers to these questions will look like new legal rules.

But when the internet is involved in a controversy only because the parties happened to use it to communicate, new legal rules will rarely be necessary. When the substance of the offense is that something was *communicated*, then the harm occurs regardless of the tools used to communicate. If an attorney betrays a client's confidence, the duty to the client is breached regardless of whether the attorney used a telephone, a newspaper, a radio station, or the internet. The choice of communication medium might affect the magnitude of the harm, but if it is illegal for A to communicate X to B without C's permission, there is no reason to fashion new rules of liability that depend on the mode of communication used.

There are *some* ways that the internet might require courts to re-think legal rules. The internet makes long-distance communication cheaper than it was before. To the extent that existing legal rules were premised on the assumption that communications were expensive, the internet might require a reappraisal. Courts are already reevaluating, for example, what it means to do business within a state, for purposes of the long-arm statute, when the defendant's "business establishment" is a server located in Uzbekistan.

Yet the vast majority of internet cases that have reached the courts have not required new legal rules to solve them. It has been fifteen years since America Online unleashed its hordes of home computing modem-owners on e-mail and the internet and fifteen years since the release of the Mosaic web browser. After all that time, we have today relatively few legal rules that apply to the internet only. Using the internet, people buy stocks, advertise used goods and apply for jobs. All those transactions are governed by the exact same laws as would govern them if they were done offline.

Those who claim the internet requires special rules to deal with these ordinary controversies have trouble explaining this history. Despite this dearth of internet-specific law, the internet is doing wonderfully. It has survived speculative booms and busts, made millionaires out of many and, unfortunately, rude bloggers out of more than a few. The lack of a special internet civil code has not hurt its development.

The internet, it turns out, was never so independent or sovereign as early idealists believed. It was an astounding social and technological achievement, and it continues to change our lives. But it has not proven to be invulnerable to legal regulation—at least, not unless we choose to make it invulnerable. As intriguing as Barlow's Declaration of Independence was, the original 1776 Declaration is more profound in its understanding of the purpose and abilities of government: men have rights of "Life, Liberty and the pursuit of Happiness," and "to secure these rights, Governments are instituted among Men." The government that we have

instituted retains its purpose of securing those rights, and it accomplishes that purpose through the law. We have seen that our government has many tools at its disposal through which it can bring law to the internet's far reaches. The internet might pose obstacles toward that job, but those obstacles can be overcome. The question is whether we will do it.