

1-1-2014

## The Internet and the Constitution: A Selective Retrospective

M. Margaret McKeown

Follow this and additional works at: <https://digitalcommons.law.uw.edu/wjlta>



Part of the [Internet Law Commons](#)

---

### Recommended Citation

M. M. McKeown, *The Internet and the Constitution: A Selective Retrospective*, 9 WASH. J. L. TECH. & ARTS 133 (2014).

Available at: <https://digitalcommons.law.uw.edu/wjlta/vol9/iss3/2>

This Article is brought to you for free and open access by the Law Reviews and Journals at UW Law Digital Commons. It has been accepted for inclusion in Washington Journal of Law, Technology & Arts by an authorized editor of UW Law Digital Commons. For more information, please contact [lawref@uw.edu](mailto:lawref@uw.edu).

THE INTERNET AND THE CONSTITUTION:  
A SELECTIVE RETROSPECTIVE<sup>\*</sup>

*The Honorable M. Margaret McKeown*<sup>\*\*</sup>

© M. Margaret McKeown

Cite as: 9 WASH J.L. TECH. & ARTS 133 (2014)  
<http://digital.law.washington.edu/dspace-law/handle/1773.1/1327>

ABSTRACT

*Over the last two decades, the Internet and its associated innovations have rapidly altered the way people around the world communicate, distribute and access information, and live their daily lives. Courts have grappled with the legal implications of these changes, often struggling with the contours and characterization of the technology as well as the application of constitutional provisions and principles. Judge M. Margaret McKeown of the United States Court of Appeals for the Ninth Circuit has had a close-up view of many of these Internet-era innovations and the ways the courts have addressed them. In this Article, adapted from her October 2013 Roger L. Shidler Lecture at the University of Washington School of Law, Judge McKeown offers her retrospective thoughts on the ways courts have handled constitutional issues in Internet cases. She also discusses some of the challenges currently facing courts and legislators alike as the U.S. legal system incorporates and accommodates Internet-based technologies and the societal, commercial, governmental, and relational changes they spawn.*

---

<sup>\*</sup> This Article is adapted from the Roger L. Shidler Lecture given at the University of Washington School of Law on Oct. 22, 2013.

<sup>\*\*</sup> Judge McKeown sits on the United States Court of Appeals for the Ninth Circuit. She thanks Marissa Doran (Yale 2013) and Ray Tolentino (Georgetown 2012) for their research assistance.

## INTRODUCTION

*Newsweek*, circa 1995, predicted that no one would ever “buy books and newspapers straight over the Internet” or “tote that laptop to the beach.”<sup>1</sup> By 2012, Americans were spending billions shopping online during the holiday season, and *Newsweek* had left the print business entirely.<sup>2</sup>

So much for the reliability of predictions.

In 1997, the year before I joined the bench, on the eve of the initial public offering for Amazon.com, I walked into a federal courtroom in New York. Barnes and Noble, hoping to upend Amazon, claimed there was no bookstore, no books, no nothing. Virtually nothing. The argument reminded me of Gertrude Stein who said, “there is no there there.”<sup>3</sup> Barnes and Noble was challenging Amazon’s claim of being the “Earth’s Biggest Bookstore.” It was a time when judges did not have computers, were not familiar with the Internet, and e-commerce was just a buzzword. But everyone thought they knew what a bookstore was. We beat back that skepticism. Now, fifteen years later, I look back and query: Has the Internet been a game changer for the bench? And more specifically, has the Internet changed how we think about the Constitution?

Today the Internet is ubiquitous. We often forget that it was not commercialized until the mid-1990s, and that its intersection with the law is a relatively recent development—it has been less than 20 years.

In the early days of Internet law, there was the famous debate of whether the Internet was different. One judge argued that you don’t need special rules and laws for the Internet any more than

---

<sup>1</sup> Clifford Stoll, *The Internet? Bah!: Hype Alert: Why Cyberspace Isn’t, and Never Will Be, Nirvana*. NEWSWEEK (Feb. 26, 1995).

<sup>2</sup> *Black Friday Billions*, COMSCORE (Dec. 1, 2013), [http://www.comscore.com/Insights/Press\\_Releases/2013/12/Black\\_Friday\\_Billions\\_12\\_Billion\\_in\\_Desktop\\_ECommerce\\_Spending\\_Marks\\_First\\_BillionDollar\\_Online\\_Shopping\\_Day\\_of\\_the\\_2013\\_Holiday\\_Season](http://www.comscore.com/Insights/Press_Releases/2013/12/Black_Friday_Billions_12_Billion_in_Desktop_ECommerce_Spending_Marks_First_BillionDollar_Online_Shopping_Day_of_the_2013_Holiday_Season); Robert Daniel and Keach Hagey, *Turning a Page: Newsweek Ends Print Run*, THE WALL ST. J. (Dec. 26, 2012), <http://online.wsj.com/news/articles/SB10001424127887324660404578201432812202750>.

<sup>3</sup> GERTRUDE STEIN, EVERYBODY’S AUTOBIOGRAPHY 298 (1937).

you do for horses.<sup>4</sup> This approach was adapted, of course, from Karl Llewellyn's view when he was drafting the first UCC principles.<sup>5</sup>

Being from Wyoming, I know about horses. Over the course of time, courts did create the law of the horse,<sup>6</sup> just as they have now created the law of the Internet or cyberspace. So while the "law of the horse" debate is interesting, particularly since we are here in the West, I view it as no longer worthwhile. In this Article, I will illustrate just how significant the impact of the Internet has been. Though building on foundational principles, there is a new frontier. The Internet is the modern-day Gold Rush in more ways than money.

Since the 1990s we have all become I-lawyers. It began with patent lawyers, known years ago as invention lawyers. Then, intellectual property, dubbed IP, came out of the woods. No longer was it a nerdy subject, but an interesting and lucrative one. Everyone became IP lawyers and then Internet lawyers, and, as judges, we have now become I-judges, with our I-pads on the bench.

---

<sup>4</sup> See Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. Chi. L. Forum 207, 214 (1996) (quoting University of Chicago Dean Gerhard Casper as saying that the University's law school did not offer a course in "the law of the horse").

<sup>5</sup> See generally Karl N. Llewellyn, *Across Sales on Horseback*, 52 HARV. L. REV. 725, 737-40 (1939). See also, e.g., George Henry Hewitt Oliphant & Clement Elphinstone Lloyd, *THE LAW OF HORSES: INCLUDING THE LAW OF INNKEEPERS, VETERINARY SURGEONS, ETC.* 174 (1882); *O'Brien v. Miller*, 60 Conn. 214 (1891) (action for personal injury caused by being struck by a team of runaway horses at a railroad crossing); *Goodsell v. Dunning*, 34 Conn. 251, 256 (1867) (action of trespass for taking the plaintiff's horse pursuant to a statute permitting landowners to impound horses that have strayed onto their land); *Parker v. State*, 1 Ala. App. 244 (Ct. App. 1911) (criminal appeal involving defendant charged with "unlawfully engag[ing] in a horse race on a public road against the peace and dignity," *id.* at 245).

<sup>6</sup> See, e.g., Easterbrook, *supra* note 4, at 214 (arguing "that the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on 'The Law of the Horse' is doomed to be shallow and to miss unifying principles.")

With iPad or Surface or other tablet in hand, let me take you on a journey of how the judiciary has responded to the constitutional challenges of the Internet era. Instead of focusing on intellectual property and the Internet—a worthwhile topic where there are thousands of cases—I deliberately focus on the Constitution as the fulcrum because it offers a stark juxtaposition of the application of our cherished foundational principles to new technology.

In talking with lawyers and scholars, the first reaction is the story of a system overwhelmed: by the rapid pace of technological changes; by whole areas of doctrine, like the First Amendment, that are an uncomfortable fit with the Internet; by legal regimes, like jurisdiction, that haven't yet adapted to technologies that don't play by old rules or respect physical boundaries. And of course, there is the old joke about how we judges are too old to possibly understand the "Interwebs." All of those things are true (though I hope not about me!). Jurisdiction is cloudy, and certain areas of doctrine have, at the very least, some catching up to do.

But in the middle of that narrative—the "the Internet is changing all the rules and the system can't keep up" approach—there's a story that is getting lost: one about institutional stability in the face of change. That's the story I want to tell.

#### TECHNOLOGY MATTERS

How then, with technology that moves in gigabytes, zettabytes, and milliseconds, do the courts—which move cautiously—deal with the Internet? It is important to understand how courts view the Internet—is it something special or is it "old wine, new bottle"? To begin, it is instructive to take a look how the courts historically have written about Internet cases:

The first published appellate opinion to mention the "internet" came in 1991, in a Second Circuit case involving criminal prosecution for spreading a worm and crashing government and university computers. The court wrote that the defendant had "released into INTERNET, a national computer network, a computer program known as a 'worm' that spread and multiplied

eventually causing computers to . . . ‘crash . . . .’<sup>7</sup> Not even THE INTERNET, just “INTERNET.”

Three years later, there had still been only a few cases.<sup>8</sup> But by 2012, the landscape had changed: the word Internet appeared in some 20,000 state and federal cases, and the race was on. The Supreme Court first got in on the act in 1996 in a case involving cable television—*Denver Area Educational Telecommunications Consortium v. FCC*.<sup>9</sup> Although the case was about cable TV, not the Internet, in a concurrence Justice Souter presciently noted: “[A]s broadcast, cable, and the cybertechnology of the Internet and the World Wide Web approach the day of using a common receiver, we can hardly assume that standards for judging the regulation of one of them will not have immense, but now unknown and unknowable, effects on the others.”<sup>10</sup> So began the Supreme Court’s first reference to the Internet.

The following year, the Supreme Court directly faced its first Internet challenge, interpreting a statute on Internet decency.

At this stage, in 1997, courts were still grappling with definitions and the shape of the box. In *Reno v. ACLU*,<sup>11</sup> the Supreme Court described “THE” Internet—the word at least received an article—as “an international network of interconnected computers that enables millions of people to communicate with one another in ‘cyberspace’ and to access vast amounts of information from around the world.”<sup>12</sup> That description became the ubiquitous tag line and is parroted again and again in lower court cases.

Beginning with Justice Souter’s references in the cable TV case, it soon became clear that the Court recognized the Internet as different and that the details of technology mattered.

---

<sup>7</sup> *United States v. Morris*, 928 F.2d 504, 505 (2d Cir. 1991).

<sup>8</sup> *See, e.g., MTV Networks, a Div. of Viacom Intern., Inc. v. Curry*, 867 F.Supp. 202 (S.D.N.Y. 1994) (trademark suit against former employee alleging that employee used employer’s marks in his Internet site).

<sup>9</sup> 518 U.S. 727 (1996).

<sup>10</sup> *Denver Area Educ. Telecomms. Consortium v. FCC*, 518 U.S. 727, 776–77 (1996) (Souter, J., concurring).

<sup>11</sup> *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 117 S. Ct. 2329, 138 L.Ed.2d 874 (1997) (Stevens, J.).

<sup>12</sup> *Id.* at 849.

The nuances of technology have been significant in the evolution of Internet law. More accurately, it should be called the evolution of law and facts. Because it is a comfortable form of analysis, courts often query through analogies. Is the Internet really just the Victorian telegraph or is it like broadcast media, or is it something different altogether? The file sharing cases—*Betamax*, *Napster*, and *Grokster*<sup>13</sup>—are good examples. For instance, when Sony came along with its Betamax device to record television programs, the entertainment industry claimed the sky was falling and the movie industry would be wiped out. As we now know, this new revenue source would help to keep the industry afloat. What impressed the Court was the testimony of Fred Rogers of *Mr. Rogers' Neighborhood*.<sup>14</sup> He said that home taping for noncommercial use was a public service; his program reached 3 million families a day. The Court also detailed the mechanical and other capabilities of the machine.<sup>15</sup> So a homespun argument plus an explanation of the technology carried the day. Courts are concerned not just with the case at hand but with the ripple effect of that case on technology not yet understood or created.

The importance of such details was front and center when the Court sent a follow-on appeal in *Reno v. ACLU* back to the trial court: “The factual record does not reflect current technological reality—a serious flaw in any case involving the Internet. The technology of the Internet evolves at a rapid pace.”<sup>16</sup> Justice Scalia also underscored this point in *Kyllo v. United States*, a 2001 case involving thermal imaging: “It would be foolish to contend that the degree of privacy secured by the Fourth Amendment has been entirely unaffected by the advance of technology.”<sup>17</sup>

---

<sup>13</sup> *MGM Studios, Inc. v. Grokster*, 545 U.S. 913, 125 S. Ct. 2764, 162 L. Ed. 2d 781 (2005); *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 104 S. Ct. 774, 78 L. Ed. 2d 574 (1984); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

<sup>14</sup> *Sony Corp.*, 464 U.S. at 445 (citing testimony of Fred Rogers that he had no objection to home taping for noncommercial use, and holding that there is no contributory copyright infringement where a product may be used for “substantial” or “commercially significant noninfringing uses”).

<sup>15</sup> *Id.*

<sup>16</sup> *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656, 671 (2004).

<sup>17</sup> 533 U.S. 27, 34, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001).

Fast forward from the beginning of the millennium to 2010, the Supreme Court's current take on technology might be divined from the case of *City of Ontario v. Quon*.<sup>18</sup> There the Court was called on to determine whether a California police department violated the constitutional rights of an employee when it inspected personal text messages sent and received by a city-owned pager. The case required familiarity with the technology behind pagers.

At oral argument, the Justices posed the following questions. Can you guess who asked what?

1. "[W]hat is the difference between a pager and e-mail?" [Chief Justice Roberts]<sup>19</sup>
2. "What happens if [an officer] is on the pager and sending a message [when other officers are] trying to reach him . . . ? Does he . . . get a busy signal?" [Chief Justice Roberts]<sup>20</sup>
3. "[And if that happens, does he] ha[ve] a voicemail saying that your call is very important to us; we'll get back to you?" [Justice Kennedy]<sup>21</sup>
3. "Could [the Plaintiff] print these . . . spicy conversations out and circulate them among his buddies?" [Justice Scalia]<sup>22</sup>

The point is that technology matters in these Internet cases. Despite the emphasis on juries, most often it is a judge, not a jury, who shapes the case, whether for constitutional interpretation, preliminary injunctions, discovery matters, or appeals.

---

<sup>18</sup> 560 U.S. 746, 130 S. Ct. 2619, 177 L. Ed. 2d 216 (2010).

<sup>19</sup> Transcript of Oral Argument, *City of Ontario v. Quon*, 560 U.S. 746 (2010), [http://www.supremecourt.gov/oral\\_arguments/argument\\_transcripts/08-1332.pdf](http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf), at 29.

<sup>20</sup> *Id.* at 44.

<sup>21</sup> *Id.*

<sup>22</sup> *Id.* at 49.



## THE CHANGING JUDICIARY

Not only are the law and technology changing, but the judiciary is changing. Let's take a look at who is doing the judging and how that has evolved over the years. We know that the age range on the Supreme Court today is from 53 to 81. I asked the Federal Judicial Center for profiles of the lower courts, and this is what I discovered in a 20 year snapshot from 1990-2010<sup>23</sup>:

The age range of all sitting judges has increased; this includes senior judges. The range was from 36 to 94 years old in 1990, and the range was from 40 to 102 years old in 2010. Judges may not age well, but we last a long time. More significantly, the median age of active judges has declined: from 58 years old in 1990 to 50 years old in 2010.

Over these years, the number of active judges with B.S. degrees has decreased. But most amazingly, the number of active federal judges with PhDs has tripled, from two to six judges. The point is that few judges have a science or math background—perhaps that's why they went to law school instead of MIT—but federal judges are getting younger, and over time you will see a new generation that grew up on computers. Although we won't see the true generation of Internet babies become federal judges until a few years down the road, judges are quick learners and are adapting to changing technology.

Before you despair about the Supreme Court and lower court federal judges, who have actually done an excellent job absorbing the nuances of the Internet, remember that politicians have been infamous for their pronouncements about the Internet. When Al Gore claimed to have created the Internet,<sup>24</sup> Dan Quayle shot back:

---

<sup>23</sup> Statistics provided to author by the Federal Judicial Center in October 2013.

<sup>24</sup> Interview with Vice President Al Gore, CNN Late Edition, Mar. 9, 1999, available at <http://www.youtube.com/watch?v=BnFJ8cHA1co> (“During my service in the United States Congress, I took the initiative in creating the Internet. I took the initiative in moving forward a whole range of initiatives that have proven to be important to our country’s economic growth and environmental protection, improvements in our educational system.”).

“If Al Gore invented the Internet, I invented spell check.”<sup>25</sup> Or you might consider what a member of the Senate had to say during a debate over amendments to the Telecom Act: “The Internet is not something that you just dump something on. It's not a big truck. It's a series of tubes. And if you don't understand, those tubes can be filled, and if they are filled, when you put your message in, it gets in line and it's going to be delayed by anyone that puts into that tube enormous amounts of material[.]”<sup>26</sup>

### THE CONSTITUTION IN THE INTERNET AGE

Let me now turn to three areas where the courts have charted constitutional frontiers: due process, free speech, and the Fourth Amendment.

#### *Jurisdiction and Due Process*

I begin with what is admittedly the “mess and confusion” arena. To my mind, the most significant change wrought by the Internet has been with respect to personal jurisdiction. The constitutional principle of due process underlies our jurisprudence in this area. But it is an area where the Supreme Court has yet to weigh in, despite confusion and conflicts among the lower courts. Personal jurisdiction once seemed so easy—the concepts of minimum contacts, purposeful availment, and due process make sense in a physical world.

If a cow—or a horse—wandered across the open range on the Colorado–Wyoming border and caused an accident, jurisdiction

---

<sup>25</sup> John Schwartz, *Gore Deserves Internet Credit, Some Say*, WASHINGTON POST Mar. 21, 1999, at A4, available at <http://www.washingtonpost.com/wp-srv/politics/campaigns/wh2000/stories/gore032199.htm>. In fact, my childhood neighbor in Wyoming, Bruce Wampler, claims to have developed “the first spelling checker for the PC,” running on a Radio Shack TRS-80. Bruce E. Wampler, *About*, BRUCE WAMPLER'S BLOG, <http://www.brucewampler.wordpress.com/about>.

<sup>26</sup> Michael Socolow, *Ted Stevens Wins: The Internet's Tubes Will Be Unclogged*, SLATE (Jan. 15, 2014), [http://www.slate.com/blogs/future\\_tense/2014/01/15/net\\_neutrality\\_struck\\_down\\_in\\_a\\_victory\\_for\\_the\\_late\\_sen\\_ted\\_stevens.html](http://www.slate.com/blogs/future_tense/2014/01/15/net_neutrality_struck_down_in_a_victory_for_the_late_sen_ted_stevens.html).

was easy. The same was true if the cow wandered into Canada—no question. Jurisdiction was metes and bounds—based on place, territory, and almost always physical borders.

Then came the computer, the web, and the cloud. Courts were flummoxed on how to approach the topic and so began the era of “interactive” and “passive” websites.

Adopting a sliding scale of commercial activity and interactivity as a benchmark for purposeful availment, a district court in Pennsylvania established a foundational framework for analysis.<sup>27</sup> Under the *Zippo* sliding scale test, “the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet.”<sup>28</sup> At one end of this continuum are defendants who do business over the Internet and have repeated contacts with the forum state such that personal jurisdiction is proper.<sup>29</sup> At the other end are defendants whose minimal presence on the Internet, such as those who simply post information on a website, does not suffice to establish jurisdiction.<sup>30</sup> And in the middle of these poles are “interactive Web sites where a user can exchange information with the host computer,” where personal jurisdiction is determined by looking to the level of interactivity and commercial nature of the exchange of information that occurs on the site.<sup>31</sup>

As is often the case, first may not be right, but it is first, and the *Zippo* test took off like a bolt of lightning.<sup>32</sup> The test, however,

---

<sup>27</sup> *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124 (W.D. Penn. 1997).

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *See, e.g.*, *Johnson v. Arden*, 614 F.3d 785, 796 (8th Cir. 2010) (finding *Zippo* test “instructive” in determining “sufficiency of internet contacts under a specific jurisdiction analysis”); *Gator.com Corp v. L.L. Bean, Inc.*, 341 F.3d 1072, 1080 (9th Cir. 2003) (applying *Zippo*); *ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, 293 F.3d 707, 713–14 (4th Cir. 2002) (“adopting and adapting” the *Zippo* test); *Revell v. Lidov*, 317 F.3d 467, 470 (5th Cir. 2002) (drawing on *Zippo* as guidance “in determining whether the operation of an internet site can support the minimum contacts necessary for the exercise of personal jurisdiction”).

was not universally accepted<sup>33</sup> and has eroded over time, with more sophisticated analysis of the Web and the nature of websites and e-commerce changing drastically.

By 2008, the United States Court of Appeals for the Ninth Circuit responded to *Zippo*, poking a huge hole in its logic. In *Boschetto v. Hansing*,<sup>34</sup> a California plaintiff purchased a car from a Wisconsin seller via eBay.<sup>35</sup> The Ninth Circuit held that personal jurisdiction did not exist in California, despite the “interactive” nature of the sale, noting that “traditional jurisdictional analyses are not upended simply because a case involves technological developments that make it easier for parties to reach across state lines.”<sup>36</sup>

But, being the Hollywood circuit, what applies to cars may not apply to celebrities. In *Mavrix Photo, Inc. v. Brand Technologies, Inc.*,<sup>37</sup> a Florida photo company discovered its photos of pop singer Fergie and her actor husband Josh Duhamel were being hosted by “celebrity-gossip.net,” an Ohio company.<sup>38</sup> Naturally, the company sued in the Central District of California.<sup>39</sup> The interactive nature of the website—it included features like user polls and comment fields—did not confer general jurisdiction, such that a non-resident defendant intended to “sit down and make itself at home.”<sup>40</sup> However, the court found specific jurisdiction because (1) “celebrity-gossip.net” received a “substantial number of hits . . . from California residents”; (2) third parties advertised to Californians, and (3) the website focused on a California industry—the entertainment world.<sup>41</sup> Taken together, these data

---

<sup>33</sup> *E.g.*, *Hy Cite Corp. v. Badbusinessbureau.com, L.L.C.*, 297 F. Supp. 2d 1154, 1161 (W.D. Wis. 2004) (declining to adopt *Zippo* test “as substitute for minimum contacts” but acknowledging that “website’s level of interactivity may be one component” of jurisdictional analysis).

<sup>34</sup> 539 F.3d 1011 (9th Cir. 2008).

<sup>35</sup> *Id.* at 1014–15.

<sup>36</sup> *Id.* at 1019.

<sup>37</sup> 647 F.3d 1218 (9th Cir. 2011).

<sup>38</sup> *Id.* at 1221–23.

<sup>39</sup> *Id.* at 1223.

<sup>40</sup> *Id.* at 1227 (internal quotation marks omitted).

<sup>41</sup> *Id.* at 1230.

points indicated that a single targeted transaction may not net jurisdiction, but a matrix of transactions might.

So where does that leave us with Internet jurisdiction? Almost nowhere. In some respects, we are approaching universal personal jurisdiction depending on how the court characterizes a certain website and its effect. In my view, there is no coherent theme in jurisdiction cases, and the risk is that we may be heading toward nationwide jurisdiction. It becomes a gestalt exercise of lining up factors on both sides of the argument and assessing fairness. So let me leave you with a few practical observations:

- Predicting Internet jurisdiction is a neither an art nor a science—*International Shoe*<sup>42</sup> and *Burger King*<sup>43</sup> are easy to recite but difficult to apply. This is an area ripe for challenge.
- *Zippo*'s bright line test is anything but; it has caused chaos and confusion
- The Supreme Court has not yet considered an Internet jurisdiction case. There was hope that its decisions in *Goodyear Dunlop Tires Operations, S.A. v. Brown*,<sup>44</sup> and *J. McIntyre Machinery, Ltd. v. Nicastro*,<sup>45</sup> might shed some light, even though they were not Internet cases.<sup>46</sup> The closest insight came from Justice Breyer's comment in his concurrence that *McIntyre*, albeit an international case, wasn't the case to rework personal jurisdiction "without a better understanding of the relevant contemporary commercial circumstances."<sup>47</sup>

---

<sup>42</sup> *Int'l Shoe Co. v. State of Wash., Office of Unemployment Comp. & Placement*, 326 U.S. 311, 66 S. Ct. 154, 90 L. Ed. 95 (1945).

<sup>43</sup> *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 470, 105 S. Ct. 2174, 85 L. Ed. 2d 528 (1985).

<sup>44</sup> 131 S. Ct. 2846 (2011).

<sup>45</sup> 131 S. Ct. 2780 (2011).

<sup>46</sup> In *Goodyear*, the Court held that a court may exercise general jurisdiction over a foreign corporation "to hear any and all claims against [it]" when the corporation's affiliations with the State in which the case is brought "are so continuous and systematic as to render [the corporation] essentially at home in the forum State." 131 S. Ct. at 2851 (internal quotation marks omitted). In

- Legislation in other countries makes jurisdiction an even dicier proposition. For example, Malaysia's Computer Crimes Act extends outside the geographical borders of Malaysia and applies "if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time."<sup>48</sup>

Now let me complicate the jurisdiction equation even further. For the last ten years, I have taught a class in Paris called "International Internet and Intellectual Property." I need no textbook. The course writes itself every year with vast changes in technology and the law. Globalization was always a good catch phrase. But to my mind, the Internet has made it a reality. In the past, doing business overseas took affirmative action—setting up an office, getting boots on the ground, advertising to a foreign market, etc. With the Internet, which knows no national borders, globalization is automatic, not induced or planned.<sup>49</sup> A poignant

---

*McIntyre*, decided the same term as *Goodyear*, the Court addressed the contours of specific, rather than general, jurisdiction, and held that a New Jersey State court lacked the power to entertain a suit against a British company whose marketing and sales efforts failed to show that the company availed itself of the New Jersey market. 131 S. Ct. at 2790 (plurality opinion). Building on its precedent in *Goodyear* and *McIntyre*, the Supreme Court revisited the scope of personal jurisdiction in *Daimler AG v. Bauman*, 134 S. Ct. 746 (2014). In *Daimler*, the Court held that a foreign company with a subsidiary in California was not subject to the general jurisdiction of California courts because the company's "slim contacts with the State hardly render it at home there." *Id.* at 760. Although *Daimler*, like *Goodyear* and *McIntyre* before it, was not an Internet case, it explores the outer limits of personal jurisdiction in cases implicating global matters.

<sup>47</sup> *McIntyre*, 131 S. Ct. at 2794 (Breyer, J., concurring).

<sup>48</sup> Computer Crimes Act of 1997, Act 563, § 9(2) (2006) (Malay.), available at <http://www.agc.gov.my/Akta/Vol.%2012/Act%20563.pdf>. Germany has a similar law that holds Internet Service Providers ("ISPs") liable for violations of German content laws if those ISPs had knowledge of the illegal content and failed to remove or disable access to that content. German Telemedia Act Sec. 10, available at <http://www.cgerli.org>. See also Betsy Rosenblatt, *Principles of Jurisdiction*, available at [cyber.law.harvard.edu/property99/domain/Betsy.html](http://cyber.law.harvard.edu/property99/domain/Betsy.html).

<sup>49</sup> Zack Kertcher & Ainat Margalit, *Challenges to Authority, Burdens of Legitimation: The Printing Press and the Internet*, 8 YALE J. L. & TECH. 1 (2005) ("The Internet is unique in its capability to instantaneously transmit

reminder of globalization comes from the *Kirtsaeng* case, decided by the Supreme Court in 2013.<sup>50</sup> While the case involved copyright—specifically the first sale doctrine for print books manufactured outside the United States—a consortium of e-commerce groups, eBay, and Google argued in an amicus brief that unless the first sale doctrine is applied to works created internationally, it “will stifle e-Commerce,” including international secondary markets.<sup>51</sup> That argument would have little practical traction but for the geometric expansion of Internet use.

As Figure 1 on the following page illustrates, usage of the Internet has risen dramatically in the past two decades. The geometric rise of international use of the Internet has spawned a growing judicial docket.

One emblematic case is *La Ligue v. Yahoo!*, which spanned courts in France and the United States. That case placed the globalization of the Internet in stark relief and raised difficult questions regarding Internet jurisdiction. For example, what happens when the “free speech zone” in the United States “leaks” into France? Or, put another way, when do French rulings impact the First Amendment rights of a U.S. company’s conduct on the Internet?

---

information across the globe. Information thus sent disregards the national territorial borders by which a modern state is identified.”). And even more recently, the Supreme Court decided *Walden v. Fiore*, Slip Op. No. 12-574 (Feb. 25, 2014), a jurisdiction case involving activity in two different states. At argument, several Justices suggested that this was a traditional, old-fashioned case, not one that implicated modern technology. In contrast, according to Justice Alito, “When you’re talking about the internet, you’re in a different world.” Oral Argument Tr. at 45, *available at* [http://www.supremecourt.gov/oral\\_arguments/argument\\_transcripts/12-574\\_9o6b.pdf](http://www.supremecourt.gov/oral_arguments/argument_transcripts/12-574_9o6b.pdf). Ultimately, in its opinion, the Court noted that “this case does not present the very different questions whether and how a defendant’s virtual ‘presence’ and conduct translate into ‘contacts’ with a particular State. . . . We leave questions about virtual contacts for another day.” *Walden*, Slip Op. 12- 574, at 13 n.9.

<sup>50</sup> *Kirtsaeng v. John Wiley & Sons, Inc.*, 133 S. Ct. 1351 (2013).

<sup>51</sup> Brief of Amici Curiae eBay Inc., Google, Inc., et al. in support of Petitioner, 2012 WL 2861166, at \*22–23 (2012).

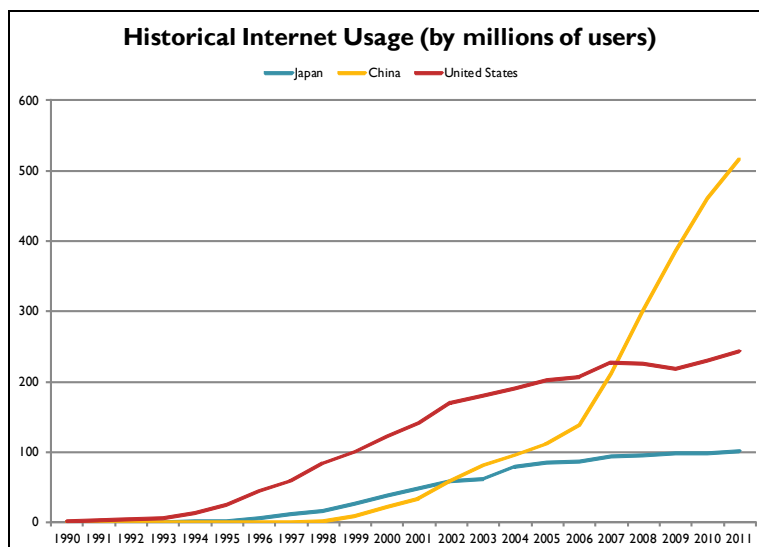


Figure 1: Historical Internet Usage (M. Margaret McKeown)<sup>52</sup>

The *Yahoo!* case started in France but ended up in a U.S. court, setting up a quintessential meeting of jurisdictional and First Amendment issues in the Internet age. La Ligue complained that Yahoo! was allowing its online auction service to be used for the sale of memorabilia from the Nazi period, contrary to the French Criminal Code. This was true.

The defense rested on the fact that these auctions were conducted under the jurisdiction of the United States. Yahoo! also claimed that there were no technical means to prevent French residents from participating in these auctions, at least without significant financial impact and compromising the essence of the Internet. Yahoo! noted that its servers were located on U.S. territory, that its services were primarily aimed at U.S. residents; that the First Amendment to the United States Constitution guarantees freedom of speech and expression, and that any attempt

---

<sup>52</sup> Figure 1 represents statistical data adapted from INTERNET WORLD STATS, [www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm), and Katherine Zickuhr, *Who's not online and why*, PEW RESEARCH INTERNET PROJECT, 4, [http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP\\_Offline%20adults\\_092513\\_PDF.pdf](http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_Offline%20adults_092513_PDF.pdf).



to enforce a judgment in the United States would therefore fail for unconstitutionality.

Yahoo! lost in the Paris court.<sup>53</sup> In fact, the judge recognized the significance of the technology and the complexity of the competing arguments and called in big-name experts, like Vincent Cerf, often referred to as the “Father of the Internet,” who established that Yahoo! had filter tools and other means to minimize exposure for French residents. Not perfect but doable. In tracking down the judge from Le Tribunal de Grande Instance de Paris, Judge Jean Jacques Gomez, who at the time was equivalent to a state trial court judge, I learned he had no prior experience in intellectual property or Internet law. He was unmoved by the claim that the Paris court was not competent to settle the dispute and that there were no technological solutions. He later rose to a position on the Cour de Cassation, the French Supreme Court, and is now retired from the court and serves as a consultant on—you guessed it—Internet law.

Saddled with a French judgment, Yahoo! sought a declaratory judgment in federal district court in California, claiming that the French order was unenforceable in the United States because it violated Yahoo!’s free speech rights under the First Amendment. The district court agreed.<sup>54</sup> In the end, these colliding values were never resolved as the Ninth Circuit disposed of the case in a sharply divided decision based on jurisdiction and ripeness.<sup>55</sup> It takes a Ouija board to divine the jurisdictional analysis in this opinion, highlighting that globalization is stretching the boundaries of jurisdiction to their constitutional breaking point.

Although this example involved Nazi emblems, it just as easily could have been another of a growing number of suits about representations of Muslims, pornography, or other clashes of competing values in the global arena. Domestically, these are First Amendment issues. Internationally, they are political, cultural, and,

---

<sup>53</sup> *La Ligue Contre Le Racisme et L’Antisemitisme v. Yahoo! Inc.*, The County Court of Paris, No. RG: 00/05308 (2000).

<sup>54</sup> *Yahoo, Inc. v. La Ligue Contre Le Racisme et L’Antisemitisme*, 169 F.Supp.2d 1181 (N.D. Cal. 2001).

<sup>55</sup> *Yahoo, Inc. v. La Ligue Contre Le Racisme et L’Antisemitisme*, 433 F.3d 1199 (9th Cir. 2007) (en banc).

at times, legal issues.

Because of the well-known constraints on extraterritorial application of the Constitution, I turn now to the First Amendment at home to consider how the Internet free speech cases have played out in the past two decades.

### *The First Amendment and Free Speech*

The First Amendment provides that “Congress shall make no law . . . abridging the freedom of speech, or of the press. . . .”<sup>56</sup> In First Amendment law, the classic dilemma has been to figure out how to characterize the Internet. Is it like a park? A sidewalk? Is it like a billboard, a telephone, or a cable network? Or is it one grand “public forum” that should be subject to little if any government regulation? This effort to analogize the digital world to the physical world is a theme repeated in many Internet cases.

Since the early days of the Internet, courts have struggled with the challenge of developing a constitutional vocabulary for this new medium. Courts draw on analogies and categories embedded in our First Amendment lexicon to varying degrees, and there is no uniform approach to free speech in the Internet context. Often courts undertake the task of developing free speech jurisprudence in the Internet context with a heavy dose of caution, unwilling to issue broad rulings that may be undermined or outdated by the pace of technology.

The jurisprudence is characterized by incrementalism, in contrast to Internet development which is almost cataclysmic. It is no wonder that the breadth of communicative possibilities introduced by the Internet has been described as “diverse as human thought.”<sup>57</sup>

Interestingly, that diversity of subject matter is not reflected in the cases before our high court. Significantly, the Supreme Court’s landmark Internet free speech cases in the past two decades have centered on regulations seeking to protect children from exploitation and from viewing obscene and indecent material.

---

<sup>56</sup> U.S. CONST. amend. I.

<sup>57</sup> *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 870 (1997) (internal quotation marks omitted).

Over this period—1996–2012—the Supreme Court issued just under 1,400 opinions. Of those, only seventeen mention the Internet substantively,<sup>58</sup> and only seven were actually about the Internet.<sup>59</sup> For a technology that has been so pervasive in our lives, this tiny handful of cases is remarkable. Curiously, the Court has addressed such oddities as whether a floating houseboat counts as a "vessel" for purposes of maritime law<sup>60</sup> but not Internet jurisdiction, and has addressed only limited Internet cases in other constitutional areas.

As noted earlier, the foundational case is *Reno v. ACLU*.<sup>61</sup> Although the Court recognized the well-established "interest in protecting children from harmful materials," the Court struck down provisions of the Communications Decency Act ("CDA"), a statute that sought to protect minors from such harmful material on the Internet.<sup>62</sup> The Court found unjustified the CDA's unnecessarily

---

<sup>58</sup> *United States v. Alvarez*, 132 S. Ct. 2537, 183 L. Ed. 2d 574 (2012); *Brown v. Entm't Merchants Ass'n*, 131 S. Ct. 2729, 180 L. Ed. 2d 708 (2011); *Hollingsworth v. Perry*, 558 U.S. 183, 130 S. Ct. 705, 175 L. Ed. 2d 657 (2010); *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 130 S. Ct. 876, 175 L. Ed. 2d 753 (2010); *John Doe No. 1 v. Reed*, 561 U.S. 186, 130 S. Ct. 2811, 177 L. Ed. 2d 493 (2010); *Fed. Commc'n Comm'n v. Fox Television Stations, Inc.*, 556 U.S. 502, 129 S. Ct. 1800, 173 L. Ed. 2d 738 (2009); *Crawford v. Marion Cnty. Election Bd.*, 553 U.S. 181, 128 S. Ct. 1610, 170 L. Ed. 2d 574 (2008); *Fed. Election Comm'n v. Wisconsin Right To Life, Inc.*, 551 U.S. 449, 127 S. Ct. 2652, 168 L. Ed. 2d 329 (2007); *Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 125 S. Ct. 2688, 162 L. Ed. 2d 820 (2005); *Ashcroft v. Am. Civil Liberties Union*, 542 U.S. 656, 124 S. Ct. 2783, 159 L. Ed. 2d 690 (2004) (*Ashcroft II*); *United States v. Am. Library Ass'n, Inc.*, 539 U.S. 194, 123 S. Ct. 2297, 156 L. Ed. 2d 221 (2003); *Smith v. Doe*, 538 U.S. 84, 123 S. Ct. 1140, 155 L. Ed. 2d 164 (2003); *Ashcroft v. Am. Civil Liberties Union*, 535 U.S. 564, 122 S. Ct. 1700, 152 L. Ed. 2d 771 (2002) (*Ashcroft I*); *Bartnicki v. Vopper*, 532 U.S. 514, 121 S. Ct. 1753, 149 L. Ed. 2d 787 (2001); *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997); *Denver Area Educ. Telecommunications Consortium, Inc. v. Fed. Commc'n Comm'n*, 518 U.S. 727, 116 S. Ct. 2374, 135 L. Ed. 2d 888 (1996).

<sup>59</sup> *Reed*, 130 S. Ct. 2811; *Williams*, 553 U.S. 285; *Brand X*, 545 U.S. 967; *Ashcroft II*, 542 U.S. 656; *Am. Library Ass'n*, 539 U.S. 194; *Ashcroft I*, 535 U.S. 564; *Reno*, 521 U.S. 844.

<sup>60</sup> *Lozman v. City of Riviera Beach*, 133 S. Ct. 735 (2013).

<sup>61</sup> 521 U.S. 844 (1997).

<sup>62</sup> *Id.* at 875.

broad suppression of speech addressed to adults. In the Court's view, the Internet presented a unique medium for the exchange of ideas and opinions, a medium entitled to the full range of First Amendment protections, despite the government's asserted interest in shielding children from obscene and indecent materials.

The Court concluded that the same free-speech principles that protect books, movies, and speeches apply to the Internet as well, and that the CDA's provisions prohibiting transmission of indecent communications to minors (the "indecency provisions") were unconstitutional restrictions on free speech.<sup>63</sup> But in reaching that conclusion, the Court took care to distinguish the Internet from other communicative media such as broadcast media. A broadcast medium, the Court observed, was more "invasive" in nature, had scarce available frequencies at its inception, and had a long history of government regulation.<sup>64</sup>

Not so for the Internet, which could hardly be considered a scarce expressive commodity, was not invasive like radio or television, and, given its novelty, had no long history of government supervision or regulation. "Each medium of expression," the Court reminded, "may present its own problems."<sup>65</sup> Dotted with quaint references like "computer coffee shops," instead of Internet cafes, the less-than-15-year-old case almost seems like ancient history.<sup>66</sup>

In her partial concurrence, Justice O'Connor, although agreeing that certain portions of the CDA were impermissibly restrictive of free speech, presented a somewhat different take on the Internet: as a space that could be "zoned" through the use of certain types of gateway technology.<sup>67</sup> While Justice O'Connor noted that such technology was not yet prevalent or available to all Internet speakers in 1997, she contemplated that "it is possible to construct barriers in cyberspace and use them to screen for

---

<sup>63</sup> *Id.*

<sup>64</sup> *Id.* at 868–69.

<sup>65</sup> *Id.* at 869 (internal quotation marks omitted).

<sup>66</sup> *Id.* at 850.

<sup>67</sup> *Id.* at 886 (O'Connor, J., concurring in part and dissenting in part).

identity, making cyberspace more like the physical world, and consequently, more amenable to zoning laws.”<sup>68</sup>

Congress was unwilling to accept the defeat handed to it in *Reno*,<sup>69</sup> so it passed a successor statute, the Child Online Protection Act (“COPA”). COPA imposed a fine and imprisonment for any commercial posting that was harmful to minors.<sup>70</sup> After the Third Circuit affirmed in *ACLU v. Ashcroft* the district court’s preliminary injunction of the statute on the ground that the reference to “contemporary community standards” in relation to harm to minors was overbroad,<sup>71</sup> the Supreme Court vacated the injunction and sent the case back to the appellate court for another round.<sup>72</sup> The debate in the divided Court was whether the community standards criterion could be applied because of the unique characteristics of the Internet. Drawing on precedent, the Court in effect said an Internet publisher was no different than a traditional publisher—if a publisher wants to be judged only by the standards of a particular community, then it should take the simple step of utilizing a medium that enables it to target only to that community.<sup>73</sup> Not so easy with the Internet.

With that pronouncement, the case went back to the Third Circuit, which once again affirmed the district court’s injunction of COPA.<sup>74</sup> The third time must be a charm as the death knell to the statute came after the third trip to the Supreme Court. Drawing on an earlier *Playboy* case involving a content-based restriction designed to protect minors, the Court held that the government

---

<sup>68</sup> *Id.* at 890.

<sup>69</sup> Congress subsequently amended the CDA to strike the indecency provisions found unconstitutional in *Reno*, keeping intact the obscenity provisions that went unchallenged in that case. 521 U.S. at 882–83. While *Reno* was making its way through the federal courts, the CDA’s obscenity provisions also faced a First Amendment challenge in the Southern District of New York. *See Nitke v. Gonzales*, 413 F. Supp. 2d 262, 263 (S.D.N.Y. 2005). In 2005, a three-judge panel rejected the constitutional challenge, *id.* at 273, and the Supreme Court summarily affirmed without an opinion, 547 U.S. 1015 (2006).

<sup>70</sup> Pub. L. No. 105-277, 112 Stat. 2681 (1998) (codified at 47 U.S.C. § 231).

<sup>71</sup> *Am. Civil Liberties Union v. Reno*, 217 F.3d 162, 179–81 (3d Cir. 2000).

<sup>72</sup> *Ashcroft v. Am. Civil Liberties Union*, 535 U.S. 564, 585–86 (2002).

<sup>73</sup> *Id.* at 582–84.

<sup>74</sup> *Am. Civil Liberties Union v. Ashcroft*, 322 F.3d 240 (3d Cir. 2003).

should bear its full constitutional burden of proof on less restrictive alternatives, such as filtering.<sup>75</sup> In affirming the district court's preliminary injunction, the Court held that the COPA likely violated the First Amendment because the measures adopted by Congress were not the least restrictive means available to advance the government's interest of preventing minors from accessing harmful internet materials.<sup>76</sup> Just as significant was the observation that by the time the case reached the Supreme Court, the record was out of date—the ever changing nature of the Internet had outstripped the pace of the litigation.

The denouement came when, on remand, the district court once again held the statute unconstitutional—it was both overinclusive (covering nonpornographic commercial speech) and underinclusive (not covering sexually explicit material originating outside the United States). As the Supreme Court warned earlier, the statute wasn't narrowly tailored because Internet filters, which were widely available, were a less restrictive means to protect children. The Court let the judgment stand. After a saga lasting around 13 years and several trips to the Supreme Court, portions of the CDA and COPA were dead.

Apart from the trilogy of CDA/COPA-related Internet cases, the other landmark First Amendment case came in 2003, when the Supreme Court once again took up the subject of children and the Internet in *United States v. American Library Association*,<sup>77</sup> which involved a statute called the Children's Internet Protection Act ("CIPA"). Under CIPA, public libraries could receive federal assistance to obtain Internet access, but only if they installed filters to block obscene images or child pornography and prevent minors from accessing harmful materials. A plurality of the Court held that these conditions did not violate the First Amendment and concluded that the traditional and designated public forum analyses did not apply to Internet access in public libraries.<sup>78</sup> Instead, the plurality recognized the government's broad discretion to make content-based judgments in deciding what private speech to make

---

<sup>75</sup> *Ashcroft v. Am. Civil Liberties Union*, 542 U.S. 656, 668–70 (2004).

<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

<sup>78</sup> *Id.* at 205–06 (plurality).

available to the public. Despite the disagreements among the Justices in *American Library Association*, they all recognized that the government had at least a legitimate interest in protecting minors from obscene and pornographic material.<sup>79</sup> Unlike in *Reno*, however, First Amendment free speech rights yielded to the government's interest in protecting children.

The common theme among these cases—*Reno*, *Ashcroft*, and *American Library Association*—is a focus on children as the recipients of Internet information. In other words, these cases conceive of youngsters as actors/consumers/users of the Internet. But the Court has also addressed Internet free speech cases in which children are the objects or targets of the Internet, particularly in the child pornography context. In those cases, Congressional efforts to protect children, particularly on the Internet, have fared more successfully.

For example, in the 2008 case of *United States v. Williams*,<sup>80</sup> the Supreme Court upheld the constitutionality of a statute that criminalizes the pandering or solicitation of child pornography in certain circumstances. That statute is known as the PROTECT Act: Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today.<sup>81</sup> The statute does not specifically address the Internet, but it covers conduct occurring on the Web. Williams, who had circulated pictures of minor children engaging in sexually explicit conduct, pleaded guilty to possession and pandering of child porn and then challenged the constitutionality of the Act. In upholding the statute, Justice Scalia summarized the long history of Congress's struggle to balance efforts to protect children on the Internet with First Amendment constraints:

Child pornography harms and debases the most defenseless of our citizens. Both the State and Federal Governments have sought to suppress it for many years, only to find it proliferating through the new medium of the Internet. This Court held unconstitutional Congress's previous attempt to

---

<sup>79</sup> *Id.*

<sup>80</sup> 553 U.S. 285 (2008).

<sup>81</sup> Publ. L. No. 108-21, 117 Stat. 650 (2003).

meet this new threat, and Congress responded with a carefully crafted attempt to eliminate the First Amendment problems we identified. As far as the provision at issue in this case is concerned, that effort was successful.<sup>82</sup>

Why was the congressional effort successful? Because the statute did not criminalize a substantial amount of protected expressive activity for adults.

Looking back on these landmark Internet free speech cases, two interesting trends emerge. First, as Justice Scalia recognized, there is a dialogue between Congress and the Court negotiating the appropriate balance between the interest in protecting children, and the equally important interest of protecting our constitutional free speech values.<sup>83</sup> Second, despite the rapidly evolving nature of the Internet, and despite the ubiquity of the Internet in various areas of law, from IP and e-commerce to net neutrality, the Court has not jumped in whole hog, instead focusing on similar kinds of cases (i.e., those involving children and the regulation of obscenity and vice) and modifying and revising its jurisprudence as its understanding of technology deepens over time.

While the Supreme Court's focus has been on speech restrictions on adults intended to protect children, the Internet has also spawned another line of speech cases in the lower courts, involving speech restrictions on children intended to protect both the children and the school environment. The notion that administrators may regulate speech at school is enshrined in the landmark case of *Tinker v. Des Moines Independent Community School District*, where the Supreme Court held long ago that schools may prohibit speech that might reasonably lead school authorities "to forecast substantial disruption of or material interference with school activities" or that collides "with the rights of other students to be secure and to be let alone."<sup>84</sup> That case was decided when life was easy and before schoolchildren joined the

---

<sup>82</sup> *Williams*, 553 U.S. at 307.

<sup>83</sup> *Id.*

<sup>84</sup> 393 U.S. 503, 508, 514 (1969).



nearly 1 billion people on Facebook,<sup>85</sup> 500 million on Twitter,<sup>86</sup> 270 million on WeChat,<sup>87</sup> and countless others on Tumblr and Instagram. Whatever the courts might say, technology doesn't differentiate between student speech on a cell phone or computer at school and speech emanating from a cell phone or computer off campus.

In the wake of school shootings, cyberbullying, and threats of disruption at school, school administrators began disciplining students for their speech—both on and off campus. One California school district even hired a private company, Geo Listening, to monitor students' public posts and communications in an effort to prevent harm.<sup>88</sup> But what can a school do when a post turns up random illegal activity, like drug use? Due in large part to the development of Internet and social media, we see a proliferation of cases on the extent of a school's authority to regulate off-campus speech. The activities at issue in these cases range from the mundane (disqualification of a student from running for class secretary because of a misleading blog post about cancellation of an upcoming event),<sup>89</sup> to the humorous (satire of a principal),<sup>90</sup> to the hurtful (mocking of a fellow student),<sup>91</sup> to the life-threatening (planning a violent attack on the school).<sup>92</sup>

---

<sup>85</sup> *Number of active users at Facebook over the years*, YAHOO! NEWS (May 1, 2013), <http://news.yahoo.com/number-active-users-facebook-over-230449748.html>. See also Geoffrey A. Fowler, *Facebook: One Billion and Counting*, WALL STREET JOURNAL (Oct. 4, 2012), <http://online.wsj.com/news/articles/SB10000872396390443635404578036164027386112>.

<sup>86</sup> Richard Holt, *Twitter in numbers*, THE TELEGRAPH (Mar. 21, 2013), <http://www.telegraph.co.uk/technology/twitter/9945505/Twitter-in-numbers.html>.

<sup>87</sup> *Nice little earner*, THE ECONOMIST (Jan. 18, 2014), <http://www.economist.com/news/china/21594312-can-wechat-become-world-beating-app-nice-little-earner>.

<sup>88</sup> Somini Sengupta, *Warily, Schools Watch Students on the Internet*, N.Y. TIMES (Oct. 28, 2013), [http://www.nytimes.com/2013/10/29/technology/some-schools-extend-surveillance-of-students-beyond-campus.html?\\_r=0](http://www.nytimes.com/2013/10/29/technology/some-schools-extend-surveillance-of-students-beyond-campus.html?_r=0).

<sup>89</sup> *Doninger v. Niehoff*, 527 F.3d 41 (2d Cir. 2008)

<sup>90</sup> *Layshock v. Hermitage Sch. Dist.*, 650 F.3d 205 (3d Cir. 2013).

<sup>91</sup> *Kowalski v. Berkeley Cnty. Sch.*, 652 F.3d 565 (4th Cir. 2011)

<sup>92</sup> *Wynar v. Douglas Cnty. Sch. Dist.*, 728 F.3d 1062 (9th Cir. 2013).

Take for example a recent case from the Third Circuit, *Layshock v. Hermitage School District*.<sup>93</sup> In that case, a high school disciplined a student for creating a fake internet profile of the principal on MySpace. The student created the profile while at his grandmother's house, logged on to the school district's website to obtain a photograph of the principal, and after creating the profile gave access to various other students by adding them as friends on the MySpace website. The majority held that the student's speech did not qualify as "on-campus" speech and was therefore subject to full First Amendment protections, warning that it would "be an unseemly and dangerous precedent . . . to reach into a child's home and control his/her actions there."<sup>94</sup> The concurring opinion pointed out just how outdated it is to peg the First Amendment and school speech along physical boundaries:

[W]ireless internet access, smart phones, . . . Facebook and stream-of consciousness communications via Twitter . . . make[] any effort to trace First Amendment boundaries along the physical boundaries of a school campus a recipe for serious problems in our public schools.<sup>95</sup>

There is an even more recent example from the Ninth Circuit: *Wynar v. Douglas County School District*.<sup>96</sup> In the face of escalating, violent, and threatening messages on MySpace, many of which included threats to kill people, our court held that "when faced with an identifiable threat of school violence, schools may take disciplinary action in response to off-campus speech that meets the requirements of *Tinker*."<sup>97</sup> Some of the student's threatening statements included the following:

- "and ill probly only kill the people i hate?who hate me / then a few random to get the record"
- [referring to a classmate] "no im shooting her

---

<sup>93</sup> 650 F.3d 205.

<sup>94</sup> *Id.* at 216.

<sup>95</sup> *Id.* at 220–21 (Jordan, J., concurring).

<sup>96</sup> 728 F.3d 1062 (9th Cir. 2013).

<sup>97</sup> *Id.* at 1069.

boobs off / then paul (hell take a 50rd clip) / then i reload and take out everybody else on the list / hmm paul should be last that way i can get more people before they run away . . .”

- “ya i thought about ripping someones throat out with one. / wow these r weird thoughts... / then raping some chicks dead bodies to?”
- “that stupid kid from vtech. he didnt do shit and got a record. i bet i could get 50+ people / and not one bullet would be wasted.
- “i wish then i could kill more people”<sup>98</sup>

The court sought to strike “the appropriate balance between allowing schools to act to protect their students from credible threats of violence while recognizing freedom of expression by students.”<sup>99</sup> To strike this balance, the court was “reluctant to try and craft a one-size-fits-all approach” for the “myriad of circumstances involving off-campus speech,” many of which involve speech on the Internet.<sup>100</sup>

The limits of the First Amendment are also being tested in the new frontier of cyberbullying and criminal prosecutions. In October 2013, the state of Florida brought felony charges against two young girls, ages 12 and 14, for bullying a classmate online until she committed suicide, although the charges were ultimately dropped.<sup>101</sup>

The upshot of 15-plus years of litigation in the free speech arena has been a singular judicial focus revolving around efforts to protect children from the effects of the Internet—from child pornography and child pornographers, ostensibly inappropriate materials, cyberbullying, or other threats. In part this has occurred because of ready satisfaction of the government action

---

<sup>98</sup> *Id.* at 1065–66.

<sup>99</sup> *Id.* at 1070.

<sup>100</sup> *Id.* at 1069.

<sup>101</sup> Steve Almasy, *Charges dropped in Rebecca Sedwick bullying case*, CNN (Nov. 21, 2013)

<http://www.cnn.com/2013/11/20/us/rebecca-sedwick-bullying-death/>.

requirement—the proliferation of statutes protecting minors and speech occurring in the public school forum.

In focusing on these issues, I don't mean to discount other important areas in which the Internet implicates the First Amendment. The net neutrality/Open Internet debate and issues related to e-commerce and intellectual property involve important issues that courts have considered and continue to consider in the First Amendment context. But these issues have yet to reach the Supreme Court. In taking a retrospective look at the Constitution and the Internet, it is important to benchmark where the Supreme Court started the Internet free speech discussion: in the context of balancing the urge to protect children against the long-held value of free expression.

This remarkable focus among the courts on issues related to children reflects the judiciary's important role as a stabilizing force in a very murky and tempestuous area of law. By drawing upon and adapting old metaphors to address new scenarios, courts mediate the rapid development of technology in familiar ways. In doing so, the judiciary maintains some semblance of order in a messy context, acting slowly and deliberately in specific areas of law while willing to alter, revise, and renew First Amendment principles in the context of a shifting technological world. As Justice Souter presciently observed in 1996, “we should be shy about saying the final word today about what will be accepted as reasonable tomorrow,” particularly “when we know too little to risk the finality of precision.”<sup>102</sup> In my view, that's a good summary of the story told by the Internet free speech cases.

#### *The Fourth Amendment and Privacy*

Leaving the First Amendment, I turn to another volatile constitutional subject—privacy. The Internet has challenged nothing so profoundly as our understandings of privacy. In 1999, Scott McNeely of Sun Microsystems was quoted as claiming,

---

<sup>102</sup> Denver Area Educ. Telecomms. Consortium, Inc. v. Fed. Comm'n Comm'n, 518 U.S. 727, 777, 116 S.Ct 2374, 135 L.Ed. 2d 888 (1996) (Souter, J., concurring).

“You have zero privacy. Get over it.”<sup>103</sup> Technology is moving the bar on what we consider private information. We share more; companies collect more; search engines can aggregate more.

But the law’s mechanisms for dealing with privacy issues often come from statutes and contracts, not the Constitution. Invoking the Fourth Amendment requires state action, and many of the most challenging privacy issues involve private actors, not the state. In large part, the uproar about Google and Facebook data collection and use bypasses the Constitution because the government is not necessarily involved. That said, the government is involved in a vast array of activities that implicate citizens’ Fourth Amendment and privacy rights, from search warrants for digital data to electronic monitoring and city-sponsored street cameras.

There has been a virtual explosion of federal criminal statutes dealing with computers, child pornography, and Internet fraud—from the Computer Fraud and Abuse Act to the Communications in Decency Act to the Electronic Communications Privacy Act, the Cybersecurity Enhancement Act, the Internet Tax Freedom Act, Unlawful Internet Gambling Act, etc., and a host of other statutes introduced but not passed. Fourth Amendment issues related to the reasonableness of searches and seizures often play out in the context of these laws.

As the *Williams* case showed in the First Amendment context, child pornography cases are a treasure trove for insights about technology and how courts respond to the digital world. The number of federal child pornography offenders sentenced annually has increased from approximately 150 in 1996 to approximately 1,800 in 2011.<sup>104</sup> Lack of user sophistication has been no defense, and images erased but left on hard drives have led to hard time.

The question for the courts has been what expectations of privacy are reasonable in the face of changing technology—historically, this technology has included cameras, telephones,

---

<sup>103</sup> Stephen Mares, *Private Lives? Not ours!*, PC World (Apr. 18, 2000).

<sup>104</sup> U.S. Sentencing Comm’n, 2012 Booker Report, at 7, 111, *available at* [www.ussc.gov/Legislative\\_and\\_Public\\_Affairs/Congressional\\_Testimony\\_and\\_Reports/Booker\\_Reports/2012\\_Booker/Part\\_C11\\_Child\\_Pornography\\_Offenses.pdf](http://www.ussc.gov/Legislative_and_Public_Affairs/Congressional_Testimony_and_Reports/Booker_Reports/2012_Booker/Part_C11_Child_Pornography_Offenses.pdf) (compiling statistics for annual number of child pornography production and non-production offenses).

beepers, and surveillance airplanes. Before the Internet age, the rule was relatively stable. Many forms of surveillance escaped from constitutional regulation because they captured information that was either voluntarily shared with a third party or observable using devices in general public use. Both notions are variants of the same idea, namely that people assumed the risk that others would see the information they chose to share. Our citizens were responsible for anticipating the consequences of their information disclosures.

A bit of history is in order. We have come a long way from *Olmstead v. United States*,<sup>105</sup> where the Supreme Court held that a telephone wiretap was not a search. That case was overruled by *Katz v. United States*<sup>106</sup> in 1967, which established that the privacy concerns of electronic surveillance were not beyond the Fourth Amendment. Defining the reasonable expectations of privacy called for in *Katz* has proven more difficult.

In 1983, the Court considered the constitutionality of using an electronic surveillance device on a car, which could be tracked for short distances. The Court wrote in *United States v. Knotts* that a “person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”<sup>107</sup> Likewise, in the “flyover cases,” like *Dow Chemical*, the Court held that surveillance of private property from the air was constitutionally permissible because the cameras used to conduct that surveillance were “available to the public.”<sup>108</sup> (Those cameras, apropos, cost about \$22,000.)<sup>109</sup>

Of course, those cases were from the 1980s. By the mid-2000s, the range of technologies that were “generally available to the public” had exploded. It was becoming possible to use those technologies—surveillance cameras, global position satellites (GPS), cell tower data, Internet packet data—to aggregate hundreds, thousands, or more data points about any particular person, and in the process, to get closer and closer to a model of

---

<sup>105</sup> 277 U.S. 438 (1926).

<sup>106</sup> 389 U.S. 347 (1967).

<sup>107</sup> 460 U.S. 276, 281 (1983).

<sup>108</sup> *Dow Chemical Co. v. United States*, 476 U.S. 227, 234 (1986).

<sup>109</sup> *Id.* at 242 n.4 (Powell, J., dissenting).

total surveillance.<sup>110</sup> This world, a far cry from the *Dow Chemical* fly-by, was foreshadowed in the movie *The Bourne Ultimatum*, where the CIA tracked a target's precise movements using location data.<sup>111</sup>

The evolution of creative technology led to cases like *Kyllo*, which involved a thermal imaging device that could “see through” walls from the outside.<sup>112</sup> Pushing back against law enforcement, the Court held that there are limits on how the government can use technologies, even those in public use, because the manner of use might reveal too much. Justice Scalia wrote: “The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.”<sup>113</sup>

Technological changes put special pressure on the third party doctrine, particularly in the context of Internet surveillance. Early in the email and Web era, courts had held that using computer surveillance techniques that revealed the addresses of the websites a person had visited, or the addresses to or from which a person had sent emails, was not a search—or, to use the metaphor from paper mail, that people had no reasonable expectation of privacy in “envelope,” as opposed to “content,” data.<sup>114</sup> Federal courts soon started to see cases challenging knowing exposure, public use, and the third party doctrine and began asking whether these concepts—each of them drawing on metaphors from physical space or life before digital technology—provided sufficient protection in an age in which technology made limitless surveillance cheap and easy.<sup>115</sup>

---

<sup>110</sup> See, e.g., *In re. U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013).

<sup>111</sup> *The Bourne Ultimatum*, 2007, clip available at <http://www.anyclip.com/movies/the-bourne-ultimatum/failing-to-track-daniels/>.

<sup>112</sup> 533 U.S. 27, 34 (2001).

<sup>113</sup> *Id.*

<sup>114</sup> See, e.g., *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (holding that an internet user had no reasonable expectation of privacy in the identifying information—name, email address, telephone number, physical address—provided to an Internet Service Provider).

<sup>115</sup> See, e.g., *In re. Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 312-13 (3d Cir. 2010) (involving cell site location information); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); *Kerns v. Bader*, 663 F.3d 1173, 1197 (10th Cir. 2011), *cert. denied*, 133 S. Ct. 645 (2012) (debate between majority and

We share information with others all the time, parties were saying, but we don't expect the government to collect and sift through all of it.

It turns out that, in voicing these concerns, parties and the courts were echoing an argument that Chief Justice Rehnquist made in an article back in 1974.<sup>116</sup> "Suppose," he wrote, "that the local police in a particular jurisdiction were to decide to station a police car at the entrance to the parking lots of a well-patronized bar from 5:30 p.m. to 7:30 p.m. every day. . . . I would guess that the great majority of people . . . would say that this is not a proper police function. . . . There would be an uneasiness[.]"<sup>117</sup> By the 2000s, the kind of surveillance that seemed relatively fanciful in 1974 was cheap and easy, and challenges to surveillance started winding their way through the federal courts.<sup>118</sup>

Then, in 2012, came *United States v. Jones*. In *Jones*, the Court held that law enforcement's installation and use of a physical GPS device, which had been attached to the underside of a criminal suspect's car, was a search.<sup>119</sup> It was a search, according to Justice Scalia (and three others—the Chief Justice and Justices Kennedy and Thomas), because the act of invading the physical space of the car was a trespass to property. It is significant how the court distinguished *Knotts*, where there was "no infringement of Knotts' reasonable expectation of privacy since the information obtained—the location of the automobile carrying the container on public roads, and the location of the off-loaded container in an open field

---

dissent over scope of the third-party doctrine). *See also* *United States v. Jones*, 132 S. Ct. 945, 957, 181 L. Ed. 2d 911 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

<sup>116</sup> William H. Rehnquist, *Is An Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement: Or: Privacy, You've Come a Long Way, Baby*, 23 KANSAS L. REV. 1 (1974).

<sup>117</sup> *Id.* at 9.

<sup>118</sup> *See, e.g.,* *Hepting v. AT & T Corp.*, 539 F.3d 1157 (9th Cir. 2008) (considering action against AT&T alleging constitutional and statutory violations in connection with AT&T's alleged participation in the government's alleged warrantless surveillance programs, *see* *Hepting v. AT & T Corp.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006), and remanding to district court in light of the FISA Amendments of 2008).

<sup>119</sup> *Jones*, 132 S. Ct. 945.



near Knotts' cabin—had been voluntarily conveyed to the public.”<sup>120</sup> The *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespass test.

In truth, technology is going to eclipse the narrow holding of *Jones*. The police can already use On\*Star and cell phone GPS for tracking people, without the need for any physical contact with the car. And of course, the government can surveil people in other ways, including by monitoring Web traffic or phone or credit card records.

*Jones* was notable for much more than the trespass holding. Four Justices—Alito, joined by Ginsburg, Breyer, and Kagan—wrote a concurrence about the privacy implications of surveillance technology. Justice Alito characterized the threat in *Jones* not as an invasion of property, as Justice Scalia had, but as an invasion of privacy. “In the pre-computer age,” he wrote, “the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.”<sup>121</sup> The Justices would have asked “whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.”<sup>122</sup> Here, they said, they would have held that a reasonable person would not expect that law enforcement would “secretly monitor and catalog every movement of an individual’s car for a very long period.”<sup>123</sup> This approach harkens back to Justice Rehnquist’s argument.

Justice Sotomayor wrote another particularly illuminating concurrence:

[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the

---

<sup>120</sup> *Id.* at 951.

<sup>121</sup> *Id.* at 963 (Alito, J., concurring).

<sup>122</sup> *Id.* at 964.

<sup>123</sup> *Id.*

course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the “tradeoff” of privacy for convenience “worthwhile,” or come to accept this “diminution of privacy” as “inevitable,” . . . , and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.<sup>124</sup>

Together, the *Jones* concurrences point to the conclusion that constitutional law might need a new theory—not just trespass, not just “knowing exposure,” not just the third party doctrine, and probably not the old *Dow Chemical/Kyllo* notion that the state can use technology so long as it is in “general public use.” Rather, the concurrences signaled that constitutional law might need a theory more like intrusion: a theory that could reinvigorate the *Katz* “reasonable expectation of privacy” test. Just as the technology in *Kyllo* called into question the assumptions of *Dow Chemical*, the technology in *Jones* calls into question some of the assumptions of those earlier cases.

A year after *Jones*, the Ninth Circuit considered the case of *United States v. Cotterman*, involving a border search of a person’s laptop.<sup>125</sup> The question in *Cotterman* was, as in *Kyllo*, “what limits there are upon this power of technology to shrink the realm of guaranteed privacy.”<sup>126</sup>

Cotterman came across the border with laptop. Authorities detained him, took his laptop for several days for extensive forensic analysis, and discovered child pornography. The government took the position that no suspicion was needed for the

---

<sup>124</sup> *Id.* at 957 (Sotomayor, J., concurring).

<sup>125</sup> 709 F.3d 952 (9th Cir. 2013), *cert. denied* 134 S. Ct. 899 (2014).

<sup>126</sup> *Id.* at 956-57.

search because it originated at the border. I wrote on behalf of the en banc court, explaining that the Fourth Amendment's guarantee of people's right to be secure in their "papers" can encompass the right to be secure in records stored in electronic form. Laptops contain financial records, confidential business documents, medical records, and private emails. They are not just containers.

*Cotterman* was a case that, like *Jones*, challenged the old metaphors that courts had been using to address internet issues in the Fourth Amendment context. The opinion noted that the "amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile," but that "is no longer the case," because "[e]lectronic devices are capable of storing warehouses full of information."<sup>127</sup> The reality of personal digital storage was described as follows:

Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails. This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their "papers."<sup>128</sup>

*Cotterman* poked holes in old metaphors on another level as well: the incriminating data that border agents found in Cotterman's laptop was in the "deleted files" section. "It is as if," we said, "a search of a person's suitcase could reveal not only what the bag contained on the current trip, but everything it had ever carried."<sup>129</sup> Significantly, "[a] person's digital life ought not to be hijacked simply by crossing a border."<sup>130</sup>

The *Recorder*, a San Francisco legal newspaper, depicted the opinion in the following cartoon showing Chief Judge Kozinski, who joined the opinion, and me at the border fence.

---

<sup>127</sup> *Id.* at 964.

<sup>128</sup> *Id.*

<sup>129</sup> *Id.* at 965.

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



Figure 2: The *Cotterman* cartoon (reprinted courtesy of George Riemann)

Why do I focus on *Jones* and *Cotterman*? Because those cases demonstrate, like *Katz* and *Kyllo* before them, that the courts have been remarkably willing to revise theories and metaphors that no longer make sense in the face of changing technology. The new reality is that many, if not most, of the daily activities we once could perform in relative privacy, from shopping to driving to reading, are now activities that, by force of infrastructure, we “share” with third parties.

The punch line on digital privacy is that the courts have just begun to plumb the depths of the Fourth Amendment. Our conceptions of privacy have changed dramatically since the time of *Olmstead* in the early 1900s. *Katz* gave us the brilliant “reasonable expectation of privacy” test. The question now is how the limits of that standard will be tested by the Internet.

Which brings me to my last point: What is on the horizon? What are the emerging challenges?

## CHANGES ON THE HORIZON

*Government Surveillance*

Courts are already experiencing a wave of constitutional challenges to government surveillance programs. Many of these challenges are arising in response to the government's national security and warrantless wiretapping cases, particularly in the wake of the 2013 Edward Snowden leaks. Snowden revealed the National Security Agency's (NSA) electronic surveillance program PRISM, which, in the words of one writer, made the NSA "the virtual landlord of the digital assets of Americans and foreigners alike."<sup>131</sup> Earlier efforts to upend such programs have generally been blocked. For example, in February 2013, the Supreme Court dismissed a case challenging the constitutionality of NSA surveillance under the 2008 FISA Amendments Act, holding that plaintiffs lacked standing because they could not prove that they had been wiretapped.<sup>132</sup> But that may start to change.<sup>133</sup> In October 2013, the *New York Times* broke a story saying that the Justice Department is "setting up a potential Supreme Court test of whether [the warrantless surveillance program] is constitutional by notifying a criminal defendant, for the first time, that evidence

---

<sup>131</sup> James Risen & Eric Lichtblau, *How the U.S. Uses Technology to Mine More Data More Quickly*, N.Y. TIMES (June 8, 2013), available at [http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html?pagewanted=all&_r=0).

<sup>132</sup> *Clapper, Director of National Intelligence, et al. v. Amnesty International USA et al.*, No. 11-1025, Slip Op. at 1 (Feb. 26, 2013).

<sup>133</sup> In fact, following this lecture, there has been a tsunami of suits related to the NSA's surveillance program. Compare *Klayman v. Obama*, 2013 WL 6598728 (D.D.C. 2013) (issuing a preliminary injunction requiring the government to cease collection of telephone metadata and concluding that the plaintiffs had demonstrated a substantial likelihood of succeeding on the merits of their Fourth Amendment claims, *id.* at 5) with *Am. Civil Liberties Union v. Clapper*, 2013 WL 6819708 (S.D.N.Y. 2013) (holding, in a case about the NSA's bulk collection of telephone metadata, that the "collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search," *id.* at \*22).

against him derived from eavesdropping.”<sup>134</sup> It seems that, after Snowden, the lid is now off. Companies like Dropbox, Google, and LinkedIn have filed briefs in the FISA court requesting permission to publish the number of requests the U.S. Government has made for their data—information they are not currently permitted to release. Senator Ed Markey is making inquiries about the number of times cellphone companies have been asked to share data with the government, and what data they have shared.<sup>135</sup> Two email services that were asked to provide data to the government “voluntarily” shut down in August rather than provide user data to the government.<sup>136</sup>

News reports on data collection are illuminating. For example, the *New York Times* headlined that \$7 million in federal money granted to the city of Oakland, California to thwart terrorist attacks has gone to a “police initiative that will collect and analyze reams of surveillance data from around town—from gunshot-detection sensors in the barrios of East Oakland to license plate readers mounted on police cars patrolling the city’s upscale hills.”<sup>137</sup> Chicago has a network of more than 2,200 cameras, and an operations center costing \$43 million from which to watch the feeds they produce.<sup>138</sup> The City of Houston is now using drones for surveillance.<sup>139</sup> The police have made more than 8 million requests

---

<sup>134</sup> Charlie Savage, *Doors May Open for Challenge to Secret Wiretaps*, N.Y. TIMES (Oct. 16, 2013), <http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html>.

<sup>135</sup> Somini Sengupta, *Senator Asks Cellphone Carriers: What Exactly Do You Share with Government?*, N.Y. TIMES: BITS (Sept. 12, 2013, 1:57 PM), [http://bits.blogs.nytimes.com/2013/09/12/senator-asks-cellphone-carriers-what-exactly-do-you-share-with-government/?\\_r=0](http://bits.blogs.nytimes.com/2013/09/12/senator-asks-cellphone-carriers-what-exactly-do-you-share-with-government/?_r=0).

<sup>136</sup> Somini Sengupta, *2 E-Mail Services Shut Down to Protect Customer Data*, N.Y. TIMES: BITS (Aug. 8, 2013, 11:15 PM), <http://bits.blogs.nytimes.com/2013/08/08/two-providers-of-encrypted-e-mail-shut-down>.

<sup>137</sup> Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance*, N.Y. TIMES, Oct. 14, 2013, <http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html?pagewanted=all>.

<sup>138</sup> Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, in THE FUTURE OF THE CONSTITUTION, Brookings Governance Studies Series (Dec. 8, 2010) (citing Fran Spielman, *Feds Give City \$48 Million in Anti-terrorism Funds*, CHICAGO SUN-TIMES, Dec. 4, 2004, at 10).

<sup>139</sup> *Id.* (citing Katie Baker, *Houston Police Use Drone Planes*,

to phone companies to help track individual cellphones using GPS technology.<sup>140</sup> And the list goes on.

### *Legislative Fixes*

Most efforts to respond to the Internet, and especially its impact on privacy, have come from legislatures. In the past 15 years, Congress has passed numerous statutes related to conduct on the Internet, from the Children's Online Privacy Protection Act of 1998 to the Keeping the Internet Devoid of Sexual Predators Act of 2008. Many more legislative efforts have come from state legislatures. For example, in the same 15-year time period, California has enacted dozens of statutes related to the privacy implications of the Internet, dealing with subjects ranging from public DNA databases to social media profiles of students to voter ID information.

Beyond these legislative fixes, state and federal administrative regulations provide yet another, perhaps nimbler, tool to address new challenges posed by the Internet. This phenomenon is playing out in the net neutrality/Open Internet debate, where much of the litigation focuses largely on the validity of the Federal Communication Commission's administrative regulations.<sup>141</sup>

### *The Court of Public Opinion*

The law has traditionally lagged behind technology. Lawsuits take time and money but the Internet offers something the law does

---

TRUTHNEWS, <http://www.truthnews.us/?p=973>).

<sup>140</sup> *Id.* (citing Justin Elliott, *How Easy Is It for the Police to Get GPS Data from Your Phone?*, TPM MUCKRAKER (Dec. 9, 2009), [http://tpmmuckraker.talkingpointsmemo.com/2009/12/cell\\_phone\\_surveillance\\_unpacking\\_the\\_legal\\_issues.php](http://tpmmuckraker.talkingpointsmemo.com/2009/12/cell_phone_surveillance_unpacking_the_legal_issues.php)).

<sup>141</sup> Following this lecture, the D.C. Circuit struck down the FCC's net neutrality rules, known as the Open Internet Order, on the ground that because "the Commission has chosen to classify broadband providers in a manner that exempts them from treatment as common carriers, the Communications Act expressly prohibits the Commission from nonetheless regulating them as such." *Verizon v. FCC*, — F.3d —, 2014 WL 113946, at \*1 (D.C. Cir. 2014).

not—a cheap worldwide platform for communication, often anonymously. Public opinion may drive private and government conduct in ways that courts and legislatures cannot. A classic example is the consumer review, often anonymous or ghostwritten, on Yelp and other websites. Just this year, after a trial court ordered a customer to rewrite a negative review posted on both Yelp and Angie’s List about her home contractor, the Virginia Supreme Court reversed the order.<sup>142</sup> The court noted that the contractor had no right to have the review excised, though he could pursue a defamation action.

One of the best things about the Internet has been the unregulated proliferation of LOL—laugh out loud—humor. But not everyone is laughing.

As another example of how the Internet can backfire from a public relations standpoint, consider the case of Danish/Dutch artist Nadia Plesner. Plesner, as part of her “Simple Living” campaign, decided to dress-up an emaciated Darfur victim with a Louis Vuitton-inspired bag and a Paris Hilton–style accessory dog. All of the profits went to charity. However, Louis Vuitton was not amused by the artist’s creative expression, and filed a lawsuit against her.<sup>143</sup> After a French court ruled against Plesner, she agreed to remove the offending references to Louis Vuitton.<sup>144</sup>

Yet despite Plesner’s promise, she later exhibited a painting called “Darfurnica”—a modern day adaptation of Picasso’s *Guernica*—which included the illustration of the Simple Living boy carrying what appeared to be a Louis Vuitton bag. This exhibition prompted an *ex parte* order against Plesner from a Dutch court.<sup>145</sup>

Plesner received broad public support. An anonymous group launched “Operation Skankbag,” an effort to damage Louis

---

<sup>142</sup> *Perez v. Dietz Development, LLC*, 2012 WL 6761997 (S. Ct. Va. 2012).

<sup>143</sup> District Court of the Hague, May 4, 2011, 389526/KG ZA 11-294 (Plesner / Louis Vuitton Malletier SA) (Neth.), available at <http://www.mediareport.nl/wp-content/uploads/2011/05/english-translation-plesner-vs-louis-vuitton-judgement-4-may-2011.pdf> (unofficial translation).

<sup>144</sup> *Id.*

<sup>145</sup> *Id.*



Vuitton by “buying replica Louis Vuitton handbags, and giving them away to homeless people.”<sup>146</sup> The Dutch court later quashed the ex parte order with retroactive effect, characterizing Plesner’s use of the Simple Living image as a “lawful statement” of her artistic opinion.<sup>147</sup> In an ironic twist, the Dutch court ordered Louis Vuitton to pay Plesner’s legal costs.<sup>148</sup>

These are just a few examples of what happens when the Internet intersects with the court of public opinion as well as the court of law.

### CONCLUSION

The Constitution and the Internet share something fundamental in their foundations. The framers of the Constitution created a blueprint for a system of decentralized governance, organized around a set of unifying principles, a system that could evolve over time as the nation debated what it should become. In much the same way, ICANN, the Internet Corporation for Assigned Names and Numbers, revolutionized the world of telecommunications by creating a blueprint for a decentralized network united by common organizing principles and the uniform system we call “code.”<sup>149</sup> These innovations—this early foundation—enabled decentralized groups of engineers to work together to correct system errors, through groups like the Internet Engineering Task Force, and to meet new challenges.

The complexity of these challenges and the pace of change in the technological realm have been staggering, and many have wondered how a centuries-old and tradition-bound legal system could possibly keep up. In my view, the answer is that the mechanisms that give the Internet its vitality and its capacity to pursue ordered evolution are the very same kinds of building blocks that give the courts the ability to respond to that change.

The courts have been willing to question the ways we

---

<sup>146</sup> See Image: Operation Skankbag, <http://i.imgur.com/OpJaw.png> (last visited Mar. 28, 2014).

<sup>147</sup> Plesner, 389526/KG ZA 11-294.

<sup>148</sup> *Id.*

<sup>149</sup> ICANN coordinates the Internet’s system of unique identifiers.

understand new technology, by asking, for instance, whether the Internet is “physical space,” whether computers are “containers,” whether emails are “papers,” and whether citizens have reasonable expectations of privacy in aggregate “envelope” data. That evolution—responsive both to established principles and new realities—speaks to the endurance and competence of the courts.

This leads me to believe that, however far we are from a bulletproof unified theory of the Constitution and the Internet, there is, in the midst of the rapid change, an institution that works. Slowly, yes; cautiously, yes. But the sky isn’t falling, and that’s in part because the institution of the judiciary—the great meeting-place of scholars, lawyers, parties, jurors, and judges—is doing what it has done in the face of other waves of change: respect tradition, but listen, deliberate, and adapt. The challenges posed by the intersection of the Internet and the Constitution are not easy ones. But they are challenges and tensions for a free society to sort out over time.

