HOW LAW MADE SILICON VALLEY

Anupam Chander[*]

ABSTRACT

Explanations for the success of Silicon Valley focus on the confluence of capital and education. In this Article, I put forward a new explanation, one that better elucidates the rise of Silicon Valley as a global trader. Just as nineteenth-century American judges altered the common law in order to subsidize industrial development, American judges and legislators altered the law at the turn of the Millennium to promote the development of Internet enterprise. Europe and Asia, by contrast, imposed strict intermediary liability regimes, inflexible intellectual property rules, and strong privacy constraints, impeding local Internet entrepreneurs. This study challenges the conventional wisdom that holds that strong intellectual property rights undergird innovation. While American law favored both commerce and speech enabled by this new medium, European and Asian jurisdictions attended more to the risks to intellectual property rights holders and, to a lesser extent, ordinary individuals. Innovations that might be celebrated in the United States could lead to imprisonment in Japan. I show how American companies leveraged their liberal home base to become global leaders in cyberspace. I argue that nations seeking to incubate their own Silicon Valley must focus on freeing speech, and so must the United States, if it hopes not to break this new industry.

---

[*] Professor of Law, University of California, Davis, and Director, California International Law Center; J.D., Yale Law School; A.B., Harvard College. For insightful comments, I thank Jack Balkin, Ash Bhagwat, Mario Biagioli, James Boyle, Eoin Carolan, Jens Dammann, Deven Desai, Stephen Diamond, Bill Dodge, Eric Goldman, Sung Gi Hwang, Suchul Kim, Tom Joo, Carlton Larson, Mark Lemley, Fred von Lohmann, Deirdre Mulligan, Pierluigi Perri, Markku Räsänen, Haochen Sun, Madhavi Sunder, Louis Trager, Mark Wu, and Kyu Ho Youm. Similarly, I thank participants in colloquia at the Yale Information Society Project; the Berkeley Globalization and Information Technology Center; the New York Law School Global Law and Policy Roundtable, Stanford Law School Law, Science and Technology Program; the UC Davis Center for Science and Innovation Studies, the Northern California International Law Scholars Conference; and Zhejiang University Guanghua Law School. I am grateful to Sarah Anker, Uyên Lê, Dimple Patel, Chia-Fen Jennifer Yu, and Louis Wai for excellent research assistance. I am grateful as well to Google, for Google Research Awards supporting this and related research.

INTRODUCTION[1]

Nearly every company set up in a garage in Silicon Valley hopes to take over the world. There is reason for such optimism. Again and again, Silicon Valley firms have become the world's leading providers of Internet services. How did Silicon Valley become the world's leading supplier of Internet services?

Popular explanations for Silicon Valley's recent success revolve around two features. First, Silicon Valley bestrides the great academic centers of Stanford University and the University of California, Berkeley, and sits near the artistic and intellectual hub of San Francisco. Second, the center of venture capital in the United States also happens to be in Menlo Park, California, allowing both industries to profit from each other in a symbiotic relationship. But education and money coincide in other parts of the United States as well. Why did those parts not prosper in the manner of Silicon Valley? More fundamentally, did not the Internet make geography irrelevant? Scholars answer that Silicon Valley's advantage lies in the economies of agglomeration.[2] Ronald Gilson argued that California's advantage was its labor law, which he believes encourages "knowledge spillovers" and agglomeration economies by facilitating employee mobility.[3] While these standard accounts do much to explain the dynamism of Silicon Valley relative to other parts of the United States, they do not explain the relative absence of such Internet

---

[1] This Article was inspired by the research and writing of a subsection, also called "How Law Made Silicon Valley," in a recent book by the author. *See* ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD IN COMMERCE 55–58 (2013). Some portions of this Article's introduction were previously published in that book. *See id*.

[2] ANNALEE SAXENIAN, REGIONAL ADVANTAGE: CULTURE AND COMPETITION IN SILICON VALLEY AND ROUTE 128, at 6, 8 (1994) ("Dense networks of social relations play an important role in integrating the firms in Silicon Valley's fragmented industrial structure."). In more recent work, Saxenian describes how diasporas help power innovation across the world. ANNALEE SAXENIAN, THE NEW ARGONAUTS: REGIONAL ADVANTAGE IN A GLOBAL ECONOMY (2006).

[3] Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. REV. 575, 578 (1999) ("Postemployment covenants not to compete have the potential to restrict seriously the movement of employees between existing firms and to start-ups and, hence, to restrict seriously employee-transmitted knowledge spillovers."); *see also* James Pooley & Mark Lemley, *California Restrictive Employee Covenants After* Edwards, 23 CAL. LAB. & EMP. L. REV., Jan. 2009, at 3, 29 ("California's long-standing ban on employee covenants not to compete is a centerpiece of state innovation policy, and it is perhaps the most important reason why California has enjoyed its leading position in the technology industries over the past twenty-five years."); Daniel B. Rodriguez & David Schleicher, *The Location Market*, 19 GEO. MASON L. REV. 637, 640–47 (2012) (describing "agglomeration economies").

innovation hubs outside the United States, or the success of Silicon Valley enterprises across the world.[4]

Law played a far more significant role in Silicon Valley's rise and its global success than has been previously understood. It enabled the rise of Silicon Valley while simultaneously disabling the rise of competitors across the world. In this Article, I will argue that Silicon Valley's success in the Internet era has been due to key substantive reforms to American copyright and tort law that dramatically reduced the risks faced by Silicon Valley's new breed of global traders.[5] Specifically, legal innovations in the 1990s that reduced liability concerns for Internet intermediaries, coupled with low privacy protections, created a legal ecosystem that proved fertile for the new enterprises of what came to be known as Web 2.0. I will argue that this solicitude was not accidental—but rather a kind of cobbled industrial policy favoring Internet entrepreneurs. In a companion paper, Uyên Lê and I show that these aspects of copyright and tort law were not driven by commercial considerations alone, but were undergirded in large part by a constitutional commitment to free speech.[6] As we argue there, a First Amendment-infused legal culture that prizes speech offered an ideal environment in which to build the speech platforms that make up Web 2.0.

I will compare the legal regimes not between Silicon Valley and Boston's Route 128, but between the United States and key technological competitors across the globe. The indulgence of American law for Internet enterprise appears in sharper relief when contrasted with the legal regimes faced by web entrepreneurs elsewhere. In Europe, concerns about copyright violations and strict privacy protections hobbled Internet startups. Asian web enterprises faced not only copyright and privacy constraints, but also strict intermediary liability rules. I will contrast the leading cyberlaw statutes and cases in the United States, with their explicit embrace of commerce and speech, with those

---

[4] Tim Devaney & Tom Stein, *Can Ireland Offer Startups Something Silicon Valley Can't?*, READWRITE (Dec. 24, 2012), http://readwrite.com/2012/12/24/can-ireland-offer-startups-something-silicon-valley-cant (Even though "just about every country with a high-speed network and a national budget has hatched a 'startup ecosystem[,]' . . . [n]one has succeeded. The Dropboxes and Instagrams of the world still flock to the original Silicon Valley.").

[5] My focus here is on Silicon Valley in its current non-silicon-based-life form, not its previous incarnations. For an account of the rise of early industry in the region, see CHRISTOPHE LÉCUYER, MAKING SILICON VALLEY: INNOVATION AND THE GROWTH OF HIGH TECH, 1930–1970 (2006).

[6] Anupam Chander & Uyên Lê, *The Free Speech Foundations of Cyberlaw* (UC Davis Legal Studies Research Paper Series, Research Paper No. 351, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320124.

from Europe and Asia, which are more attendant to the risks of this new medium for existing interests. I will show that Google and Yahoo were so worried that Japanese copyright law would make search engines illegal that they placed their search servers offshore.[7] A Japanese computer science professor advised his students to publish their software outside Japan.[8] British Prime Minister David Cameron suggested that Google's search engine might have been illegal under English copyright law.[9]

This Article upends the conventional wisdom, which sees strong intellectual property protections as the key to innovation—what the World Intellectual Property Organization calls a "power tool" for growth.[10] Understanding the reasons for Silicon Valley's global success is of more than historical interest. Governments across the world, from Chile to Kenya to Russia, seek to incubate the next Silicon Valley.[11] My review suggests that overly rigid intellectual property laws can prove a major hurdle to Internet innovations, which rely fundamentally on empowering individuals to share with each other. This study helps make clear what is at stake in debates over new laws such as the Stop Online Piracy Act (SOPA) and its relatives, highlighting the effect of these laws on Silicon Valley's capacity for

---

[7] *See infra* notes 202–04 and accompanying text.

[8] *See infra* notes 205–06 and accompanying text.

[9] *See infra* notes 123–25 and accompanying text.

[10] *See, e.g.*, KAMIL IDRIS, INTELLECTUAL PROPERTY: A POWER TOOL FOR ECONOMIC GROWTH 1 (2d ed. 2003), *available at* http://www.wipo.int/export/sites/www/freepublications/en/intproperty/888/wipo_pub_888_1.pdf.

[11] Ryan Underwood, *The Silicon Valley of South America?*, INC., Apr. 2011, at 96; Katrina Manson, *Kenya Breaks Ground on Africa's Silicon Savannah*, FIN. TIMES (Jan. 23, 2013, 6:26 PM), http://blogs.ft.com/beyond-brics/2013/01/23/kenya-breaks-ground-on-africas-silicon-savannah/; Simon Shuster, *Russia Plans a Silicon Valley*, TIME, Apr. 19, 2010, http://content.time.com/time/magazine/article/0,9171,1978772,00.html; *see also* John Boudreau, *China Strives to Create Its Own Silicon Valley*, SAN JOSE MERCURY NEWS, June 7, 2012, at A1; Alexandra A. Seno, *Is Silicon Asia Sprouting?*, NEWSWEEK, Dec. 16, 2002, at E10 ("Would-be Silicon Valleys are springing up throughout the region, from the $1.7 billion Cyberport in Hong Kong to the $5 million Greater Phuket Digital Paradise in Thailand, several mini-valleys in Vietnam, Indonesia's Bandung High-Technology Valley and, of course, the $20 billion Malaysian mother of all these clones, the Multimedia Super Corridor."); *Cameron Reveals Silicon Valley Vision for East London*, BBC (Nov. 3, 2010, 8:37 PM), http://www.bbc.co.uk/news/uk-england-london-11689437.

innovation.[12] I show that government has the power to enable, or disable, a new industry. The power to make in this case implies the power to break.[13]

Innovation scholars worry about the "valley of death," the stage between start-up idea and successful commercialization, in which most start-up enterprises founder.[14] Cyber scholars fond of citing Joseph Schumpeter's "creative destruction" need to attend to his focus as well on the finance needed by innovators.[15] Imagine the boardroom in a Silicon Valley venture capital firm, circa 2005. A start-up less than a year old has already attracted millions of users. Now that start-up, which is bleeding money, needs an infusion of cash to survive and scale up. The start-up lets people share text, photos, and videos, and includes the ability to readily share text, pictures, and videos posted by one's friends. If that start-up can be accused of abetting copyright infringement on a massive scale, or must police its content like a traditional publishing house lest it face damages claims or an injunction, your hundred-million-dollar investment might simply vanish to plaintiffs' lawyers in damages and fees.[16]

---

[12] Moves that might further hamstring Internet enterprises are under consideration elsewhere as well. For example, a draft communiqué from the Organization for Economic Cooperation and Development proposes to take away some of the liability protections that intermediaries have for copyright infringement. Rick Mitchell, *OECD Says Net Policy Should Protect IP Rights, but Limit Provider Liability*, 16 ELECTRONIC COM. & L. REP. 1168 (2011).

[13] Indeed, legal scholars concerned about SOPA warned Congress not to "break the Internet." Mark Lemley et al., *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (2011), http://www.stanfordlawreview.org/sites/default/files/online/articles/64-SLRO-34_0.pdf. Many have raised similar alarms about the Anti-Counterfeiting Trade Agreement, the Trans-Pacific Partnership Agreement, and patent law. *See, e.g.*, JAMES BESSEN & MICHAEL J. MEURER, PATENT FAILURE: HOW JUDGES, BUREAUCRATS, AND LAWYERS PUT INNOVATORS AT RISK (2008); DAN L. BURK & MARK A. LEMLEY, THE PATENT CRISIS AND HOW THE COURTS CAN SOLVE IT (2009); Peter K. Yu, *Six Secret (and Now Open) Fears of ACTA*, 64 SMU L. REV. 975, 1044–46 (2011) (describing the "ACTA Boomerang" harming domestic industry); Jessica E. Vascellaro, *The Valley: Firms Fear Patent War*, WALL ST. J., Nov. 10, 2011, at A16A; Margot Kaminski, *Plurilateral Trade Agreements Lack Protections for Users, Intermediaries*, INTELL. PROP. WATCH (Oct. 27, 2011, 11:47 PM), http://www.ip-watch.org/weblog/2011/10/27/plurilateral-trade-agreements-lack-protections-for-users-intermediaries/. Considering the late opposition that ended SOPA, Google's Larry Page suggests, "10 or 20 years from now, we'll look back and say we were a millimeter away from regulating [the Internet] out of existence." Steven Levy, *Google's Larry Page on Why Moon Shots Matter*, WIRED (Jan. 17, 2013, 6:30 AM), http://www.wired.com/business/2013/01/ff-qa-larry-page/all/.

[14] Vicki Loise & Ashley J. Stevens, *The Bayh-Dole Act Turns 30*, 45 LES NOUVELLES 185, 192 & n.35 (2010) (noting that the phrase was "popularized by Congressman Vernon Ehlers, himself a Ph.D. physicist when the term was used in a Report to Congress by the Science Committee, of which he was Vice-Chair in 1998").

[15] Schumpeter, who served as Finance Minister of Austria in 1919, described the banker as "the ephor of the exchange economy." JOSEPH A. SCHUMPETER, THE THEORY OF ECONOMIC DEVELOPMENT 74 (Redvers Opie trans., 1934).

[16] This hypothetical finds real-world inspiration in a recent story. Matt Lynley, *Pinterest: We're Not Going to Be Sued into Oblivion, and Here's Why*, BUSINESS INSIDER (Mar. 9, 2012, 3:01 PM), http://www.businessinsider.com/pinterest-were-not-going-to-be-sued-into-oblivion-and-heres-why-2012-3; Hayley

An injunction might stop the site from continuing without extensive human monitoring that could not be justified by potential revenues. Because of the insulation brought by U.S. law reforms in the 1990s, American start-ups did not fear a mortal legal blow. The legal privileges granted to Internet enterprises in the United States helped start-ups bridge the valley of death.

Let me anticipate criticism. First, legal realists might object that I have spoken about law on the books. What about law in action? I demonstrate through actual cases the practical importance of the liberal American law and the strict European and Asian laws. Second, some might seek to trivialize my thesis: law always matters to the success of an enterprise because it could have made that enterprise illegal, but did not. That is not my claim; rather, my claim is that U.S. authorities (but not those in other technologically advanced states) acted with deliberation to encourage new Internet enterprises by both reducing the legal risks they faced and largely refraining from regulating the new risks they introduced. Third, some will insist that if law was relevant, it was only because it got out of the way. After all, the last person hired at a Silicon Valley start-up is the lawyer. The story of Silicon Valley is not only a story of brilliant programmers in their garages, but also a legal environment specifically shaped to accommodate their creations.

My claim may resonate with students of American legal history. Morton Horwitz famously argued that nineteenth-century American courts modified liability rules to favor the coming of industrialization.[17] I suggest an even more widespread effort, with the Executive, Congress, and the Courts, each in their own way promoting Internet enterprise. Horwitz decried the nineteenth-century's laws' implicit subsidy to industrialists, which he saw as being borne on the backs of society's least fortunate.[18] The limitations on Internet intermediary liability and the lack of omnibus privacy protections beyond those that are promised contractually by websites mean that there is a price to be paid for the amazing innovation of the past two decades. Even while we celebrate innovation, we must recognize its costs.

Tsukayama, *Pinterest Addresses Copyright Concerns*, WASH. POST (Mar. 15, 2012), http://articles.washingtonpost.com/2012-03-15/business/35447213_1_ben-silbermann-pinterest-content; *see also infra* note 292 and accompanying text.

[17] MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW 1780–1860 (1977). This thesis has its critics. *See* Gary T. Schwartz, *Tort Law and the Economy in Nineteenth-Century America: A Reinterpretation*, 90 YALE L.J. 1717, 1720 (1981); Grant Gilmore, *From Tort to Contract: Industrialization and the Law*, 86 YALE L.J. 788, 794 (1977) (book review); Eben Moglen, *The Transformation of Morton Horwitz*, 93 COLUM. L. REV. 1042, 1042 n.2 (1993) (book review) (collecting criticism).

[18] *See infra* notes 274–75 and accompanying text.

I do not allege the discovery of the DNA for economic development in the Information Age. The cyberlaw I describe here must be understood against the broader legal, cultural, and economic background in particular societies. What works in one jurisdiction might not work elsewhere because of differences in the role of law, the role of norms, enforcement, and other features.[19] At the same time, a comparative exercise is highly instructive, offering experience with different methods of achieving a desired result.[20] It also helps us recognize the impact of differing legal cultures (including what James Whitman has called "the two Western cultures of privacy"[21]) on such values as speech and enterprise.

This Article proceeds as follows. Part I reveals how American legislators and courts altered the law to accommodate new Internet enterprises. Part II shows that European and Asian nations offered relatively stricter intermediary liability regimes and privacy protections, making illegal the new business model embraced by their American counterparts.[22] Part III calls for due attention to the hidden price of innovation in order to avoid the "wow" to "yuck" curve—the move from dazzlement to disgust that scholars have identified for other new technologies.[23]

---

[19] Law and development scholar Kevin Davis observes two significant reasons why universal claims are likely to fail:

> First, the law may not be necessary to induce the outcome in question because the presence of certain other factors is sufficient; in other words, there may be *substitutes* for the law. A second possibility is that the law is not sufficient to generate the outcome in question; in other words, there may be *complements* for the law, in the absence of which it has no impact.

Kevin E. Davis, *Legal Universalism: Persistent Objections*, 60 U. TORONTO L.J. 537, 540 (2010).

[20] Ralf Michaels, *The Functional Method of Comparative Law*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW 339, 351 (Mathias Reimann & Reinhard Zimmermann eds., 2006) ("If law fulfils functions and meets societal needs, then the lawyer's job is to develop laws that perform these tasks ('social engineering'), and comparative law can help compare the ability of different solutions to solve similar problems, and spur similar degrees of progress.").

[21] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004). Whitman distinguishes cultures focused on dignity and liberty, drawing upon Robert Post's conceptualization of privacy. *Id.* at 1167; *see also* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001).

[22] In another paper, yet a work in progress, I will show how Silicon Valley firms leveraged their liberal home jurisdiction to conquer the world.

[23] *The Societal Implications of Nanotechnology: Hearing Before the H. Comm. on Sci.*, 108th Cong. 49, 51–52 (2003) [hereinafter *Hearings*] (statement of Vicki L. Colvin, Executive Director, Center for Biological and Environmental Nanotechnology) (observing a "wow" to "yuck" trajectory in genetically modified organisms, and seeking to avoid it for nanotechnology).

I. MAKING AMERICA SAFE FOR SILICON VALLEY

I review here key legal developments that enabled the rise of Web 2.0. Each of the individual stories I tell in this Part may seem familiar.[24] Yet, by weaving these stories together, one begins to see a stunning pattern in the larger narrative. The pattern appears even sharper when contrasted with my survey of Europe and Asia in Part II.

In the last decade of the Millennium, the infant industry spawned by the invention of the World Wide Web posed pressing challenges. How could we protect children from being awash in pornography?[25] Would early Internet pioneers such as AOL and Yahoo fail in the face of claims that they abetted defamation and other wrongs?[26] Would Hollywood disappear in the face of easy and perfect digital copying through services such as Napster? Could we protect children from communicating with dangerous adults?[27] Would companies be at the mercy of individuals who were quicker to register corporate trademarks as domain names?[28] Would contracts entered into online,

---

[24] *See, e.g.*, Brief of Amici Curiae Center for Democracy & Technology and Electronic Frontier Foundation Supporting Appellees and Urging Affirmance at 4, Doe v. SexSearch.com, 551 F.3d 412 (6th Cir. 2008) (No. 07-4182) ("With this broad immunity against all civil claims, Section 230 has successfully promoted free speech and innovations on the Internet."); Cecilia Ziniti, Note, *The Optimal Liability System for Online Service Providers: How* Zeran v. America Online *Got It Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583 (2008). One *Wired* news piece even observes the connection between the CDA and the DMCA:

> Paired with the 1996 Communications Decency Act, which provides similar immunity against noncopyright claims like defamation, the DMCA made it possible for everyone from Digg to WordPress to provide forums for users without constant fear of being sued out of existence.
>
> "These two protections for intermediaries have been absolutely crucial for giving us the internet today," says Fred von Lohmann, an internet attorney with the Electronic Frontier Foundation . . . . "You could not run a blog without these. You couldn't run MySpace, AOL without these two things."

David Kravets, *10 Years Later, Misunderstood DMCA Is the Law That Saved the Web*, WIRED (Oct. 27, 2008, 3:01 PM), http://www.wired.com/threatlevel/2008/10/ten-years-later/.

[25] James Coates & Graeme Zielinski, *Internet: Bigger Audiences, Wider Access, Less Control*, CHI. TRIB., July 4, 1997, at 1.

[26] *See AOL Again Involved in Complex Speech Issue*, COMM. DAILY, Sept. 30, 1997, *available at* 1997 WLNR 3620335 ("Governor [Jim Geringer] also said that if AOL didn't change its policy, 'parents in Wyoming who are using AOL should discuss whether they can support a company that allows the promotion of torture, rape and murder.'").

[27] Robert Coles, *Safety Lessons for the Internet*, N.Y. TIMES, Oct. 11, 1997, at A11 ("The Internet can bring into a home not only passive entertainment, like television images, but also the interactive presence of other voices, ready to engage in conversation.").

[28] *See* Joshua Quittner, *Billions Registered*, WIRED, Oct. 1994, at 50 (discussing the speculative practice of domain name purchases in the early 1990s).

lacking an ink signature, prove unenforceable?[29] Would e-commerce be saddled with multiple tax obligations from the thousands of taxing jurisdictions across the country?[30]

The Clinton Administration published a white paper outlining its vision for "Global Electronic Commerce."[31] Announcing the report, President Clinton presciently observed, "Governments can have a profound effect on the growth of electronic commerce. By their actions, they can facilitate electronic trade or inhibit it."[32] The report concluded that "[e]xisting laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age."[33] Most importantly, it declared the Administration's commitment to self-regulation: the first principle announced that "[t]he private sector should lead," and the second principle that "[g]overnments should avoid undue restrictions on electronic commerce."[34] That preference for self-regulation over governmental intrusions would mark congressional activity during this period. This meant even carving out Internet enterprises from the reach of existing law. The Administration's simple mandate: "Let a thousand Web sites bloom."[35]

Congress responded to the rise of the Internet with a flurry of laws. These are the laws of this fruitful period, in chronological order: the Communications Decency Act of 1996 (CDA),[36] the Internet Tax Freedom Act,[37] the Children's Online Privacy Protection Act of 1998 (COPPA),[38] the Digital Millennium Copyright Act (DMCA),[39] the Anticybersquatting Consumer Protection Act

---

[29] Geanne Rosenberg, *Legal Uncertainty Clouds Status of Contracts on Internet*, N.Y. TIMES, July 7, 1997, at D3 ("[B]usiness managers, corporate lawyers and legal scholars [are] uncertain about the enforceability of electronic agreements. The uncertainty has had a chilling effect, even at computer-astute places . . . . Lawmakers are scrambling to fill the gap between technology and the law.").

[30] S. REP. NO. 105-276, at 4 (1998) (citing 6,600 potential taxing jurisdictions within the United States).

[31] WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), *available at* http://clinton4.nara.gov/WH/New/Commerce/read.html. A draft of the white paper was published in 1996.

[32] Message to Internet Users on Electronic Commerce, 2 PUB. PAPERS 901, 902 (July 1, 1997).

[33] CLINTON & GORE, *supra* note 31.

[34] *Id*.

[35] John M. Broder, *Let It Be: Ira Magaziner Argues for Minimal Internet Regulation*, N.Y. TIMES, June 30, 1997, at D1.

[36] Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133–43 (codified as amended in scattered sections of 18 and 47 U.S.C.).

[37] Internet Tax Freedom Act, Pub. L. No. 105-277, tit. XI, 112 Stat. 2681, 2681-719 to -726 (1998).

[38] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, tit. XIII, 112 Stat. 2681, 2681-728 to -735 (codified at 15 U.S.C. §§6501–6506 (2012)).

[39] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 5, 17, 28, and 35 U.S.C.).

(ACPA),[40] and the Electronic Signatures in Global and National Commerce Act (E-Sign).[41]

Taken together, these statutes helped undergird a legal framework that proved conducive to the development of Internet-based services. While the titles of these statutes often professed consumer-oriented goals—a remarkable list including decency, tax freedom, privacy, and consumer protection—commercial concerns were never far from the table, as we will see. I review below the CDA and the DMCA, statutes that proved especially significant for Silicon Valley enterprises over the course of the following decade.[42] I also consider the crucial judicial interpretations that bent the law to foster web innovation.

We see that each of the branches of government played an integral part in this endeavor. In the face of calls for legal protections, the Clinton Administration promoted self-regulation by the Internet industry. Congress wrote a set of statutes that dealt with some of the principal concerns of both the content industry and the public, without placing too much in the way of burdensome constraints on Silicon Valley enterprise. The Courts, for their part, sought to protect speech and promote innovation by reading immunity statutes broadly and striking down statutes that might chill speech. At the same time, each of the branches checked the others when they proved less than friendly to Internet innovation. Congress embraced the DMCA's Title II, even where the Clinton Administration was initially inclined to favor copyright holders; the

---

[40] Anticybersquatting Consumer Protection Act, Pub. L. No. 106-113, 113 Stat. 1501, 1501A-545 to -552 (1999) (codified as amended in scattered sections of 15, 16, and 28 U.S.C.).

[41] Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified at 15 U.S.C. §§ 7001–7031). Another statute, the Child Online Protection Act, a successor to the Communications Decency Act, never took effect, having been enjoined in *ACLU v. Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999), and permanently enjoined in *ACLU v. Gonzales*, 478 F. Supp. 2d 775 (E.D. Pa. 2007), *aff'd sub nom.* ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008).

[42] The other statutes proved useful, each in its own way. The Internet Tax Freedom Act helped inform the widespread (if erroneous) view that Internet commerce was a tax-free zone. Rather than a tax holiday for transactions conducted via the Internet, the statute simply banned special taxes that discriminated against the Internet or taxes on obtaining Internet service to one's home or business. By banning taxes on Internet access, the statute made Internet access itself cheaper. The perception that Internet-mediated transactions were tax-free likely contributed to the willingness of many individuals to buy goods from unseen and often unfamiliar online merchants, helping companies like eBay and Amazon. The Anticybersquatting Consumer Protection Act helped alleviate the concerns of trademark holders during the rapid development of cyberspace. E-Sign helped assure the acceptance of painless electronic contracting, imposing no formal requirements on contracts executed via the Internet. E-Sign overrode efforts such as those in Utah to require a particular technology for clearly enforceable contracts—an approach that might have created a cumbersome obstacle to widespread adoption of Internet contracting. Jane K. Winn & Robert A. Witte, *E-Sign of the Times*, E-COMMERCE L. REP., July 2000, at 2, 8.

Courts declared unconstitutional the anti-pornography restrictions imposed by Congress; and Congress offered safe harbors for intermediary liability even where courts were sometimes inclined to impose broader liability. Thus, this was a cobbled industrial policy, halting and inconsistent, yet ultimately adding up to a powerful set of pro-Internet laws.

A. Intermediary Liability

The first of this series of statutes, the Communications Decency Act, proved central to the rise of the new breed of Silicon Valley enterprise. This hardly seemed likely for a statute directed against indecent speech. The CDA made it a crime to display obscene or indecent material to persons who were less than eighteen years of age, unless the site had taken appropriate measures such as an age-verified credit card to restrict access to adults.[43] Hidden within the statute was a small fateful section, § 230,[44] that would save many corporations—most of them not even dreamed of when the Act was passed—from potentially ruinous legal challenges.

What risks did such firms face? By offering platforms for users across the world, Internet enterprises faced the hazard that some users would use these platforms in ways that violated the law, bringing with it the possibility of liability for aiding and abetting that illegal activity. Consider a sampling of the array of claims that might lie against these platforms for the behavior of their users. Yahoo might be liable if someone uses Yahoo Finance to circulate a false rumor about a public company. Match.com could face liability if a conniving user posted defamatory information about another individual. Craigslist might be liable under fair housing statutes if a landlord put up a listing stating that he preferred to rent to people of a particular race. Amazon and Yelp might be liable for defamatory comments written by a few of their legions of reviewers.

The risks were made apparent in 1995 in the case of *Stratton Oakmont, Inc. v. Prodigy Services Co*.[45] There, an investment firm, allegedly defamed on an Internet bulletin board, sued that board's owner, Prodigy. The New York trial court held that Prodigy could be liable as a publisher because it had advertised

---

[43] Communications Decency Act of 1996, Pub. L. No. 104-104, sec 502, § 223(a), (e)(5), 110 Stat. 56, 133–34 (1996) (codified as amended at 47 U.S.C. § 223 (2006)).

[44] *Id*. at sec 509, § 230, 110 Stat. at 137 (codified as amended at 47 U.S.C. § 230).

[45] 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Communications Decency Act of 1996, Pub. L. No. 104-104, sec. 509, § 230, 110 Stat. 56, 137, *as recognized in* Shiamili v. Real Estate Grp. of N.Y., Inc., 952 N.E.2d. 1011 (N.Y. 2011).

its editorial control over the site.[46] Even in this decision, marking a high point of liability concerns, the court was mindful of the impact on new Internet enterprises, which might follow the decision's logic and simply disavow any editorial control and thereby avoid any liability. The court argued that "the market will . . . compensate a network for its increased control and the resulting increased exposure."[47] There is economic logic to this, but it may be that the costs of monitoring are so high as to create a service that is too expensive to attract sufficient buyers. While it might be relatively cheap to monitor for pornography or indecent words, it is far more difficult to evaluate factual claims made in the thousands of posts on a particular site. More importantly, the court's vision of the metered website is quite different than the cyberspace that actually flourished after *Stratton Oakmont* was undone by statute the following year.

Despite the trial court's assurances of market compensation to come, the industry was understandably alarmed at the ruling. It turned to Congress to fashion a remedy. In a short section embedded within the Communications Decency Act, Congress undid *Stratton Oakmont*. Under the subsection heading "Protection for 'Good Samaritan' blocking and screening of offensive material" (no Good Samaritan behavior was actually required for the main § 230 immunity to attach), Congress declared that online service providers could never be treated as publishers for material they did not develop.[48] As interpreted by courts, the section largely immunized online service providers from secondary liability for most torts committed through their service.[49] The section offered online publishers an immunity that their offline compatriots never enjoyed. One student commentator compares the treatment of *Soldier of Fortune* magazine, held liable in 1992 for millions of dollars in damages for permitting an advertisement that led, tragically, to an actual murder-for-hire, to an online newspaper that would avoid similar liability because of § 230.[50]

---

[46] *Id*. at *5. The plaintiffs initially claimed an astonishing $200 million in damages. Peter H. Lewis, *After Apology from Prodigy, Firm Drops Suit*, N.Y. TIMES, Oct. 25, 1995, at D1 (noting that the firm ultimately agreed to drop its $200 million libel lawsuit against Prodigy in return for Prodigy saying sorry).

[47] *Stratton Oakmont*, 1995 WL 323710, at *5.

[48] 47 U.S.C. § 230(c)(1) (2006).

[49] One need only consider an alternative suggestion by Missouri Congresswoman Danner to sense the array of paths not taken: "Mr. Chairman, ... [t]elephone companies must inform us as to whom our long distance calls are made. *I believe that if computer online services were to include itemized billing, it would be a practical solution which would inform parents as to what materials their children are accessing on the Internet*." 141 CONG. REC. 22,046 (1995) (emphasis added) (statement of Rep. Pat Danner).

[50] Ryan French, Comment, *Picking up the Pieces: Finding Unity After the Communications Decency Act Section 230 Jurisprudential Clash*, 72 LA. L. REV. 443, 443–44 (2012).

Congress justified this differential treatment on the ground that "[t]he Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[51] Furthermore, Congress sought "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[52] Congress thus sought to simultaneously promote the speech potential of a largely self-regulated Internet, while fostering the rise of Internet enterprises.[53] Indeed, though largely unheralded at the time, the section proved a lifeline to Web 2.0 enterprises.

For their part, courts read the mandate in § 230 broadly, defining "interactive computer service" broadly, and as covering a large array of claims, both state and federal (but excluding intellectual property claims, as per the statute's directions). Most importantly, they not only eliminated a website's liability as a publisher, but also as a distributor. Where publishers typically faced strict liability, distributors such as a library or bookstore would be liable if they had knowledge of the wrongdoing and still refused to act.[54] In *Zeran v. America Online, Inc.*, the Fourth Circuit held that § 230 must be read to eliminate distributor liability, as well as publisher liability, for web services.[55] The court reasoned that a contrary holding would chill speech because it would create a natural incentive for service providers to take down information that some user found offensive for fear of liability for letting it remain: "Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not."[56] Other circuits followed *Zeran*'s broad reading, eliminating distributor liability as an incident of the defense against publisher liability.[57]

---

[51] 47 U.S.C § 230(a)(3).

[52] *Id.* § 230(b)(2).

[53] *See id.* § 230(a).

[54] *See* RESTATEMENT (SECOND) OF TORTS § 578 (1977); W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 113, at 799, 803–04, 810–12 (5th ed. 1984); Raymond Shih Ray Ku, *Irreconcilable Differences? Congressional Treatment of Internet Service Providers as Speakers*, 3 VAND. J. ENT. L. & PRAC. 70, 73–74 (2001).

[55] 129 F.3d 327, 332–33 (4th Cir. 1997).

[56] *Id.* at 333.

[57] Ben Ezra, Weinstein, & Co., v. Am. Online Inc., 206 F.3d 980, 986 (10th Cir. 2000); Doe v. Am. Online, Inc., 783 So. 2d 1010, 1013 (Fla. 2001).

Again and again, § 230 proved invaluable to shield web enterprises from lawsuits, as demonstrated by a plethora of cases.[58] Perhaps every major

[58] *See, e.g.*, Shrader v. Beann, 503 F. App'x 650 (10th Cir. 2012) (relying on § 230 to immunize the operators of an online messaging board against defamatory contents posted by third-party users), *cert. denied*, 134 S. Ct. 102 (2013); Getachew v. Google, Inc., 491 F. App'x 923 (10th Cir. 2012) (relying on § 230 to immunize Google against negative information about Plaintiff found with Google's search engine); Simmons v. Danhauer & Assocs., 477 F. App'x 53 (4th Cir. 2012) (relying on § 230 to immunize an online auction service against error committed by a user); Black v. Google, Inc., 457 F. App'x 622 (9th Cir. 2011) (relying on § 230 to immunize Google against defamatory comments posted by a user); Johnson v. Arden, 614 F.3d 785 (8th Cir. 2010) (relying on § 230 to immunize an Internet service provider against allegedly defamatory statements posted on Defendant's website); Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250 (4th Cir. 2009) (relying on § 230 to immunize a website operator against allegedly defamatory comments posted by users); Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008) (relying on § 230 to immunize MySpace from a negligence claim arising from the sexual assault on a fourteen-year-old girl who was assaulted after meeting the assailant through the service); DiMeo v. Max, 248 F. App'x 280 (3d Cir. 2007) (relying on § 230 to immunize an online bulletin board service for claims arising out of a user's allegedly defamatory postings); Parker v. Google, Inc., 242 F. App'x 833 (3d Cir. 2007) (relying on § 230 to immunize Google against claims for defamation, invasion of privacy, and negligence arising out of Google's automatic website archiving service); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007) (relying on § 230 to immunize a web hosting service, Lycos, from claims arising out of cyber-stalking and Florida securities and antidilution claims); Almeida v. Amazon.com, Inc., 456 F.3d 1316 (11th Cir. 2006) (relying on § 230 to immunize Amazon.com for the display of a photograph of a book cover that included a photograph of Plaintiff); Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003) (relying on § 230 to immunize a provider of web hosting services for the sale of illegal tapes through its services); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003) (relying on § 230 to immunize a matchmaking website for false content about Plaintiff); *Ben Ezra, Weinstein, & Co.*, 206 F.3d 980 (relying on § 230 to immunize an Internet service provider that provided stock quotation information, and finding that the Internet service provider was not responsible for wrong stock information because it was not the information content provider under the CDA); *Zeran*, 129 F.3d 327 (relying on § 230 to immunize a bulletin board service provider for its failure to remove allegedly defamatory notices); Klayman v. Zuckerberg, 910 F. Supp. 2d 314 (D.D.C. 2012) (relying on § 230 to immunize Facebook against harmful pages created by third-party users); Xcentric Ventures, L.L.C. v. Borodkin, 908 F. Supp. 2d 1040 (D. Ariz. 2012) (relying on § 230 to immunize www.ripoffreport.com against postings by users); Merritt v. Lexis Nexis, No. 12-CV-12903, 2012 WL 6725882 (E.D. Mich. Oct. 23, 2012) (relying on § 230 to immunize Lexis Nexis against false statements disseminated online), *report and recommendation adopted*, No. 12-12903, 2012 WL 6725881 (E.D. Mich. Dec. 12, 2012); AF Holdings, LLC v. Doe, No. 5:12-CV-02048-EJD, 2012 WL 4747170 (N.D. Cal. Oct. 3, 2012) (relying on § 230 to immunize a provider of Internet connection against the third-party posting of pirated videos on the Internet); Shah v. MyLife.com, Inc., No. 3:12-cv-1592-ST, 2012 WL 4863696 (D. Or. Sept. 21, 2012) (stating that § 230 would immunize interactive computer service providers against the online publication of private information provided by third parties, but dismissing for lack of jurisdiction), *report and recommendation adopted*, No. 3:12-cv-1592-ST, 2012 WL 4863271 (D. Or. Oct. 11, 2012); Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262 (W.D. Wash. 2012) (granting an online-advertising-service company's motion for preliminary injunction because § 230 likely preempts state law punishing anyone who directly or indirectly causes explicit content to be published); Hadley v. Gatehouse Media Freeport Holdings, Inc., No. 12 C 1548, 2012 WL 2866463 (N.D. Ill. July 10, 2012) (relying on § 230 to immunize a website operator against a user's allegedly defamatory comments); Seldon v. Magedson, No. 11 Civ. 6218(PAC)(MHD), 2012 WL 4475274 (S.D.N.Y. July 10, 2012) (relying on § 230 to immunize a website operator against users' defamatory posts), *report and recommendation adopted*, No. 11 Civ. 6218(PAC)(MHD), 2012 WL 4475020 (S.D.N.Y. Sept. 28, 2012); Echenique v. Google, Inc., No. 12-cv-00883-BNB, 2012 U.S. Dist. LEXIS 92729 (D. Colo. July 5, 2012)

(relying on § 230 to immunize Google against search results that allegedly defamed Plaintiff and violated Plaintiff's privacy rights); Courtney v. Vereb, No. 12-655, 2012 WL 2405313 (E.D. La. June 25, 2012) (relying on § 230 to immunize an online-forum provider from defamatory comments posted by a user); Nieman v. Versuslaw, Inc., No. 12-3104, 2012 WL 3201935 (C.D. Ill. June 13, 2012) (relying on § 230 to immunize search engine companies against online searches that allegedly defame Plaintiff and violate Plaintiff's privacy rights), *report and recommendation adopted*, No. 12-3104, 2012 WL 3201931 (C.D. Ill. Aug. 3, 2012), *aff'd*, 512 F. App'x 635 (7th Cir. 2013); Price v. Gannett Co., No. 2:11-cv-00628, 2012 WL 1570972 (S.D. W. Va. May 1, 2012) (relying on § 230 to immunize operators of an online forum against defamatory posts by unknown users on Defendants' forum webpages); S.C. v. Dirty World, LLC, No. 11-CV-00392-DW, 2012 WL 3335284 (W.D. Mo. Mar. 12, 2012) (relying on § 230 to immunize the operator of a website against third-party user posts that allegedly defame Plaintiff and violate Plaintiff's privacy rights); Ascentive, LLC v. Op. Corp., 842 F. Supp. 2d 450 (E.D.N.Y. 2011) (denying Plaintiff's motion for preliminary injunction because § 230 will likely immunize the website, PissedConsumer.com, even though the website invited third parties to submit negative reviews); Hopkins v. Doe, No. 2:11-CV-100-RWS, 2011 WL 5921446 (N.D. Ga. Nov. 28, 2011) (relying on § 230 to immunize a website for allegedly defamatory statements posted to the website); Inman v. Technicolor USA, Inc., No. 11-666, 2011 WL 5829024 (W.D. Pa. Nov. 18, 2011) (relying on § 230 to immunize eBay for allegedly defective vacuum tubes sold through the site); Levitt v. Yelp! Inc., Nos. C-10-1321 EMC, C-10-2351 EMC, 2011 WL 5079526 (N.D. Cal. Oct. 26, 2011) (relying on § 230 to immunize Yelp for allegedly manipulating user comments); Holomaxx Techs. Corp. v. Microsoft Corp., No. 10-cv-04924 JF (HRL), 2011 WL 3740813 (N.D. Cal. Aug. 23, 2011) (relying on § 230 to immunize Microsoft for computer fraud and intentional interference with contract when Microsoft's spam blocker blocked Plaintiff's advertising e-mail); M.A. *ex rel* P.K. v. Vill. Voice Media Holdings, LLC, 809 F. Supp. 2d 1041 (E.D. Mo. 2011) (relying on § 230 to immunize the publisher of a website against a claim that the website was used by a convicted child trafficker); Asia Econ. Inst. v. Xcentric Ventures LLC, No. CV 10-01360 SVW (PJWx), 2011 WL 2469822 (C.D. Cal. May 4, 2011) (relying on § 230 to immunize a consumer complaint website from liability for allegedly defamatory statements posted to the site by users); Collins v. Purdue Univ., 703 F. Supp. 2d 862 (N.D. Ind. 2010) (relying on § 230 to immunize a newspaper website against tort claims arising out of allegedly defamatory remarks posted by third parties); Dart v. Craigslist, Inc., 665 F. Supp. 2d 961 (N.D. Ill. 2009) (relying on § 230 to immunize Craigslist against claims that it facilitated prostitution); Goddard v. Google, Inc., 640 F. Supp. 2d 1193 (N.D. Cal. 2009) (relying on § 230 to immunize Google for providing tools to advertisers when advertisers use the tools to post allegedly fraudulent content); e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605 (N.D. Ill. 2008) (relying on § 230 to immunize an Internet service provider for filtering or blocking e-mails the provider believes to be objectionable in good faith); Langdon v. Google, Inc., 474 F. Supp. 2d 622 (D. Del. 2007) (relying on § 230 to immunize Internet service providers from claims arising from their monitoring, screening, and deleting of content from their network); Prickett v. InfoUSA, Inc., 561 F. Supp. 2d 646 (E.D. Tex. 2006) (relying on § 230 to immunize an online-data-gathering company that collected information from third parties about individuals and businesses for distributing false information); Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523 (D. Md. 2006) (relying on § 230 to immunize an Internet service provider despite allegations that it knew of its customers' potentially illegal activities); Whitney Info. Network, Inc. v. Verio, Inc., No. 2:04CV462FTM29SPC, 2006 WL 66724 (M.D. Fla. Jan. 11, 2006) (relying on § 230 to immunize a web hosting service for defamation claims arising from statements on a website hosted by the service); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090 (W.D. Wash. 2004) (relying on § 230 to immunize Amazon.com for state consumer protection claims and for tortious interference with business relationships arising out of the display of content uploaded by third parties); Optinrealbig.com, LLC v. Ironport Sys., Inc., 323 F. Supp. 2d 1037 (N.D. Cal. 2004) (relying on § 230 to immunize a business that reported alleged spam e-mails against trade, libel, intentional interference with contractual relations, and unfair competition claims brought by a bulk commercial e-mail business); Novak v. Overture Servs., Inc., 309 F. Supp. 2d 446 (E.D.N.Y. 2004) (relying on § 230 to immunize Google for breach of contract and tort claims arising out of its failure to remove material); Noah v. AOL Time Warner Inc., 261 F. Supp. 2d 532 (E.D. Va. 2003) (finding

Internet enterprise has relied on the statute to defend itself over the years. The CDA insulated web enterprises from the reach of a variety of federal and state causes of action, both statutory and common law.[59] These include, for example, the Federal Fair Housing Act, Title II of the Civil Rights Act of 1964, the Washington State Consumer Protection Act, and common law actions such as invasion of privacy, negligence, and tortious interference with business relations. The CDA's § 230 was no panacea—it failed as a defense a third of the time; it still required the Internet enterprise to engage in expensive litigation; and, even when it proved a successful defense, a year had often passed in the interim.[60]

---

that Defendant, an Internet service provider, is immune under the CDA and, therefore, is not responsible for the anti-Islamic comments submitted onto its online chat rooms by users), *aff'd*, No. 03-1770, 2004 WL 602711 (4th Cir. Mar. 24, 2004); PatentWizard, Inc. v. Kinko's, Inc., 163 F. Supp. 2d 1069 (D.S.D. 2001) (relying on § 230 to immunize a provider of Internet service in a case arising out of a patron's use of Defendant's service in an alleged defamation); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (relying on § 230 to immunize AOL against defamation claims arising out of statements by a gossip columnist, even though AOL had contracted with the gossip columnist to provide content); Stoner v. eBay Inc., No. 305666, 2000 WL 1705637 (Cal. Super. Ct. 2000) (relying on § 230 to immunize eBay from claims related to the sale of bootleg and other infringing sound records posted by users); Giordano v. Romeo, 76 So. 3d 1100 (Fla. Dist. Ct. App. 2011) (relying on § 230 to immunize a website operator for alleged defamation by third parties); Delle v. Worcester Telegram & Gazette Corp., No. 11-0810, 2011 Mass. Super. LEXIS 295 (Mass. Super. Ct. 2011) (relying on § 230 to immunize an online news website for comments posted by users); Shiamili v. Real Estate Grp. of N.Y., Inc., 952 N.E.2d 1011 (N.Y. 2011) (relying on § 230 to immunize a website operator for allegedly defamatory statements even though Defendants reposted these statements and added headings to the comments); UMG Recordings, Inc. v. Escape Media Grp., Inc., 948 N.Y.S.2d 881 (Sup. Ct. 2012) (relying on § 230 to immunize an operator of a website against copyright infringement on the operator's website), *rev'd on other grounds*, 964 N.Y.S.2d 106 (App. Div. 2013); Hill v. StubHub, Inc., 727 S.E.2d 550 (N.C. Ct. App. 2012) (relying on § 230 to immunize an online marketplace against the sale of tickets on the marketplace in violation of state law regulating ticket pricing), *review denied*, 736 S.E.2d 757 (N.C. 2013). *But see* CYBERsitter, LLC v. Google Inc., 905 F. Supp. 2d 1080 (C.D. Cal. 2012) (denying Google's motion to dismiss because § 230 immunity is dependent on whether Google materially contributed to the damaging information on its website and it was too early to make such a determination); Amerigas Propane, L.P. v. Op. Corp., No. 12-713, 2012 WL 2327788 (E.D. Pa. June 19, 2012) (denying a website operator's motion to dismiss under § 230 because Plaintiff alleged that the website operator was the creator of some of the posts that infringed Plaintiff's trademark); Chang v. Wozo LLC, No. 11-10245-DJC, 2012 WL 1067643 (D. Mass. Mar. 28, 2012) (denying Internet advertising companies' motions to dismiss under § 230 because Plaintiff alleged that the Internet advertising companies, at least in part, created the fraudulent Internet advertisements); Lansing v. Sw. Airlines Co., 980 N.E.2d 630 (Ill. App. Ct. 2012) (holding that § 230 does not grant immunity against a claim of negligent supervision when an employee uses Southwest's computer and Internet to send harassing and threatening e-mails because whether Defendant is treated as a publisher or not is irrelevant to Plaintiff's pled claim).

[59] Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. ON TELECOMM. & HIGH TECH. L. 101, 102–05 (2007).

[60] David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 493 (2010).

Two foundational cases demonstrate the practical value of the CDA to web enterprises. In *Doe v. MySpace, Inc.*, the social networking site faced a claim for liability arising from a heinous act—an assault on a minor by a nineteen-year-old man whom she met through MySpace.[61] The family sued MySpace for negligence in not verifying her age on the ground that verification would have revealed that she was thirteen when she registered, not eighteen as she claimed.[62] The Fifth Circuit Court of Appeals ruled that § 230 protected MySpace from the suit.[63] The CDA also protected an Internet dating service from a lawsuit arising from a malicious posting of a false profile on a dating site.[64] Someone using a computer in Berlin posted a profile using photos of the actress Christianne Carafano suggesting that she was interested in meeting men, and made her home address and phone number available.[65] In *Carafano v. Metrosplash.com, Inc.*, the Ninth Circuit Court of Appeals relied on § 230 to deny Carafano's lawsuit against the owner of the dating site for invasion of privacy, misappropriation of the right of publicity, defamation, and negligence.[66] The court ruled that "despite the serious and utterly deplorable consequences that occurred in this case, we conclude that Congress intended that service providers such as Matchmaker be afforded immunity from suit."[67] The court recognized that as a result of the law, "Internet publishers are treated differently from corresponding publishers in print, television and radio."[68]

With CDA § 230, both commercial and speech considerations coincided. As the Fourth Circuit noted in *Zeran*, a notice and takedown system would inevitably lead to firms generally choosing to take down controversial statements, rather than face any specter of liability.[69] As Neal Katyal writes: "Because an ISP [Internet Service Provider] derives little utility from providing access to a risky subscriber, a legal regime that places liability on an

---

61 528 F.3d 413, 416 (5th Cir. 2008).

62 *Id.* at 420–21.

63 *Id.* at 422.

64 Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1121, 1125 (9th Cir. 2003).

65 *Id.* at 1121.

66 *Id.* at 1122, 1125.

67 *Id.* at 1125.

68 *Id.* at 1122.

69 Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997); Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 28 (2006).

ISP for the acts of its subscribers will quickly lead the ISP to purge risky ones from its system."[70]

Even while § 230 offered a lifeline to Internet enterprises, the remainder of the CDA complicated their work tremendously. Core provisions of the CDA sought to make it difficult for children to access material judged indecent by a community. But in *Reno v. ACLU*, the Supreme Court stepped in to strike down those provisions as a violation of the freedom of speech.[71] The CDA's anti-indecency provisions posed a particular challenge to sites that welcomed user content. Unless these sites verified the ages of their users, typically through credit cards, they faced the very real possibility that someone would post indecent material on their pages. The statute covered all "communications," not just images, and thus required a website administrator to actually read through the postings of users to adjudicate decency.[72] In a very real sense then, *Reno v. ACLU* made possible Web 2.0.

The interaction between Congress and the Court expressed through the CDA § 230/*Reno v. ACLU* pairing consisted in a legislature that immunized Internet enterprises from the actions of others, and a court that declared that Internet enterprises could not be made to act as censors for the state, at least under certain terms. Neither Congress nor the Courts were consistently single-minded in their promotion of Internet enterprise, yet their interaction resulted in precisely this. Congress overruled any court that might have sought to hold intermediaries liable for user-generated content (other than for intellectual property-based claims, an area we turn to next). Meanwhile the Courts overturned congressional efforts to require Internet enterprises to censor speech widely. The end result was a legal framework conducive to promoting speech on the Internet through online speech intermediaries.

B. Copyright

Any technology that allows individuals to share information can lend itself to copyright infringement. A company like Yahoo that allows individuals to post whatever they want online faces a high risk that its service will be used for

---

[70] Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1007–08 (2001). Law and economics scholars have argued that the problem was that users were unwilling to pay ISPs for the full social benefit because of positive externalities from their use, and this resulted in a market failure. *See, e.g.*, Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 225–26 (2006).

[71] 521 U.S. 844 (1997).

[72] 47 U.S.C. § 231 (2006).

extensive copyright infringement. The company might be liable for direct infringement every time it delivers a copy of the copyrighted work (direct infringement being a strict liability offense), for contributory infringement if it has knowledge and makes a material contribution to the infringement, and for vicarious infringement if it controls and earns a direct financial benefit from the infringement. Given that statutory damages for direct infringement alone range from $200 to $150,000 for each work,[73] and that millions of works are copied online, the specter of liability would be enough to stop most Internet companies dead in their tracks. This is not a hypothetical concern. Consider the graveyard of dot-com enterprises, felled not by flawed monetization plans, but by copyright law: MP3.com, ICraveTV.com, Aimster, Grokster, and, most famously, Napster.[74]

While § 230 of the CDA protected websites against a wide variety of claims arising out of the actions of their users, it explicitly excluded intellectual property claims from its ambit.[75] This meant that any site that collected material provided by users might still be held liable for claims arising out of copyright or trademark. Internet enterprises remembered well the 1993 case of *Playboy Enterprises, Inc. v. Frena*, in which a court held the operator of an online bulletin board strictly liable for copyright infringement by users of that board.[76] The declaration by a federal court that "[i]t does not matter that Defendant Frena may have been unaware of the copyright infringement"[77] must have rattled many in Silicon Valley.[78]

---

[73] 17 U.S.C. § 504(c)(1)–(2) (2012) (providing statutory damages per work of $750 to $30,000, but permitting damages per work to be reduced to $200 in cases where the defendant was not aware, and had no reason to believe, that infringement was occurring, or increased to $150,000 in cases of willful infringement). For a cogent critique, see Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. 439 (2009).

[74] *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000); Twentieth Century Fox Film Corp. v. iCraveTV, Nos. Civ. A. 00-120, Civ. A. 00-121, 2000 WL 255989 (W.D. Pa. Feb. 8, 2000).

[75] 47 U.S.C. § 230(e)(2).

[76] 839 F.Supp. 1552, 1559 (M.D. Fla. 1993).

[77] *Id.*

[78] Another federal district court refused to uphold a direct copyright infringement claim, though that court was more willing to entertain a claim of secondary infringement. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1372 (N.D. Cal. 1995) ("[I]t does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet. . . . The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred.").

The Internet industry set out to reform the law, but the content industries resisted, as did the White House initially. In 1995, a White House task force led by Patent Commissioner Bruce Lehman concluded that it was "premature" to reduce legal risks for Internet intermediaries, preferring to treat them as publishers for copyright purposes.[79] Traditional publishers, of course, are strictly liable for copyright infringement in their publications, and thus this approach would have subjected Google and Facebook to strict liability for their users' actions.[80] Given the volume of material they carry, it is hard to imagine how we might have Google or Facebook today if they were to have the publisher liability of *The New York Times* or Time Warner. CompuServe's general counsel Stephen Heaton testified before Congress that strict liability for online service providers shifted enforcement responsibility from copyright owners to the online enterprises.[81] Requiring such enterprises to monitor the "trillions of bits of data" that crossed their computer networks would "bring[] their businesses to a halt, almost immediately," he averred.[82] The recording industry denied the need for special protections for online service providers, making plain the industry's aversion to such special rules for online companies:

> Internet Access Providers . . . . argue that copyright liability will stifle the growth of the Internet, chill investment in companies that provide Internet access, and unfairly harm their companies when they have no control over or knowledge of what users may be doing on their network.
>
> Frankly, we don't see it.[83]

---

[79] INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 122 (1995) ("The Working Group believes it is—at best—premature to reduce the liability of any type of service provider in the [on-line] environment. On-line service providers currently provide a number of services. With respect to the allowance of uploading of material by their subscribers, they are, in essence, acting as an electronic publisher."); Mike Scott, Note, *Safe Harbors Under the Digital Millennium Copyright Act*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 99, 113–15 (2005).

[80] *See, e.g.*, *Playboy*, 839 F. Supp. at 1559 (applying traditional copyright publisher liability to online bulletin board service).

[81] *NII Copyright Protection Act of 1995 (Part 2): Hearing on H.R. 2441 Before the Subcomm. on Courts & Intellectual Prop. of the H. Comm. on the Judiciary*, 104th Cong. 235 (1996) (statement of Stephen M. Heaton, General Counsel and Secretary, CompuServe, Inc.).

[82] *Id.*

[83] *The Copyright Infringement Liability of Online and Internet Service Providers: Hearing on S. 1146 Before the S. Comm. on the Judiciary*, 105th Cong. 15 (1997) (statement of Cary H. Sherman, Senior Executive Vice President and General Counsel, Recording Industry Association of America).

Public interest groups, including library associations and consumer groups, argued against expanded rights of the copyright industry online.[84] Consumer electronics firms, too, worried about expanded copyright liabilities, but the copyright industries responded that this was merely an effort by Japanese manufacturers to profit from American material.[85]

By late 1998, the copyright and information industries came to a mutual understanding,[86] reflected in a complicated set of safe harbors under which Internet companies could seek shelter from copyright liability. With the Digital Millennium Copyright Act, Congress sought to address the impact of the digital environment on copyrighted works by (a) barring devices that circumvented copyright protection schemes (Title I, the "WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998");[87] and (b) offering companies that followed certain policies respectful of copyright immunity from claims for copyright infringement (Title II, the "Online Copyright Infringement Liability Limitation Act" or OCILLA).[88] While the DMCA was best known for its first Title, which made it illegal to circumvent copyright protection schemes like those found in DVD movies, the second Title of the statute provided safe harbors for Internet enterprises from copyright liability.[89]

OCILLA provided four safe harbors for commercial enterprises: the first for the companies that bring the Internet to one's home, the second for the companies that make temporary copies of data being routed on the Internet, the third for companies that host on the Internet material provided by others, and the fourth for Internet search engines.[90] The last two safe harbors in particular proved crucial to Silicon Valley enterprises.[91] As Edward Lee writes, "virtually

---

[84] JESSICA LITMAN, DIGITAL COPYRIGHT 125–27 (2001).

[85] *Id*. at 126.

[86] Cassandra Imfeld & Victoria Smith Ekstrand, *The Music Industry and the Legislative Development of the Digital Millennium Copyright Act's Online Service Provider Provision*, 10 COMM. L. & POL'Y 291, 306–11 (2005) (describing music industry's "change of heart" in favor of Title II after obtaining significant changes in draft legislation).

[87] Pub. L. No. 105-304, §§ 101–105, 112 Stat. 2861–77 (1998) (codified as amended in scattered sections of 5, 17, 28, and 35 U.S.C.).

[88] *Id*. §§ 201–203, 112 Stat. at 2877–86.

[89] As copyright scholar Edward Lee notes, "Title I expanded copyright liability, while Title II contracted it." Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 233 (2009).

[90] *See* 17 U.S.C. § 512(a)–(d) (2012).

[91] *See, e.g*., UMG Recordings, Inc. v. Shelter Capital Partners, 718 F.3d 1006 (9th Cir. 2013) (relying on 17 U.S.C. § 512(c)'s safe harbor to immunize a website operator against copyright infringement claims); Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007) (relying on 17 U.S.C. § 512(c)'s safe harbor provision to immunize Defendant, a provider of webhosting and Internet connectivity, from Plaintiff's claims

all commercial websites in the U.S. that deal with third-party content attempt to follow and fall within the safe harbors. Indeed, it would be foolish, if not a breach of corporate fiduciary duty, for any such company not to do so."[92]

OCILLA achieved a modus vivendi between northern and southern California—where Silicon Valley would banish repeat offenders and take down material if requested by the copyright owner, often based in Hollywood.[93] By performing these duties diligently, Silicon Valley enterprises generally managed to avoid liability for the widespread copyright infringement that still occurred through their systems. While some have legitimately criticized OCILLA for leading firms to take down material too quickly for fear of jeopardizing their safe harbor,[94] OCILLA marked a significant

against Defendant for providing services for websites that infringed Plaintiff's copyrights); Viacom Int'l Inc. v. YouTube, Inc., No. 07 Civ. 2103(LLS), 2013 WL 1689071 (S.D.N.Y. Apr. 18, 2013) (relying on 17 U.S.C. § 512(c) to immunize YouTube from liability for copyrighted materials on the website that were uploaded by third-party users, despite the fact that YouTube may have known that infringement was ubiquitous throughout the website); Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724 (S.D.N.Y. 2012) (relying on 17 U.S.C. § 512(c) to immunize Photobucket from Plaintiff's claims that Photobucket users have copied, displayed, and modified Plaintiff's copyrighted material); Brown v. Way, No. 10-cv-13016, 2011 WL 3555618 (E.D. Mich. Aug. 5, 2011) (finding that 17 U.S.C. § 512 immunizes Defendant's online message boards from liability for its users' postings of allegedly copyrighted content); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132 (N.D. Cal. 2008) (relying on 17 U.S.C. § 512(c) to immunize Veoh from liability for copyrighted videos posted on its site by third parties, even though Veoh's website may have facilitated users in accessing copyrighted materials); Parker v. Google, Inc., 422 F. Supp. 2d 492 (E.D. Pa. 2006) (relying on 17 U.S.C. § 512(b) to immunize Google from copyright claims against Google's automatic website caching and indexing activities); Hendrickson v. eBay Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (relying on 17 U.S.C. § 512 to immunize eBay from liability for the third-party sale of pirated materials on eBay's website). *But see* Ellison v. Robertson, 357 F.3d 1072 (9th Cir. 2004) (denying AOL's summary judgment motion because AOL may not satisfy the safe harbor requirements in 17 U.S.C. § 512(i) because it failed to have a working e-mail address for infringement notifications); Columbia Pictures Indus. v. Fung, No. CV 06-5578 SVW(JCx), 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009) (denying defendants safe harbor protection because they were aware of their users' ongoing infringing activities), *aff'd in part as modified*, 710 F.3d 1020 (9th Cir. 2013); Capitol Records, Inc. v. MP3tunes, LLC, No. 07 Civ. 9931(WHP), 2009 WL 3364036 (S.D.N.Y. Oct. 16, 2009) (denying an online music storage website's motion to dismiss against Plaintiff's copyright infringement claims because the website did not meet the safe harbor threshold requirements stipulated in 17 U.S.C. § 512(i)); Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124 (S.D.N.Y. 2009) (denying an online bulletin board safe harbor protection because it knowingly failed to take action to prevent infringing material).

92 Lee, *supra* note 89, at 234.

93 Jerome H. Reichman et al., *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981, 983 (2007) ("When enacting the Digital Millennium Copyright Act (DMCA) of 1998 as the U.S. implementation of the WCT, Congress achieved a reasonable balance of competing interests in its creation of safe harbors from copyright liability for internet service providers (ISPs) and other intermediaries for the infringing acts of others." (footnote omitted)).

94 Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171, 176 (2010) (arguing that "the copyright notice-and-takedown regime operates in the shadow of the law, silencing speech indirectly through private intermediaries

accomplishment for Silicon Valley in creating rules that allowed Web 2.0 enterprises to flourish without either excessive copyright management costs or high liability risks.[95]

In recent years, especially in the battle against SOPA, it has become apparent that the content industry is dissatisfied with the détente struck in 1998. The extent of the content industry's distaste for Silicon Valley is evident in—of all things—Rupert Murdoch's tweets. In January 2012, Murdoch used Twitter to accuse Google of being a "[p]iracy leader."[96]

Courts, too, played a central role in the flourishing of Silicon Valley enterprise in the face of claims of copyright holders. Major advances in information technology had put pressure on copyright holders before, and courts had been called upon to adjudicate disputes between the two industries. In the 1980s, courts had largely sheltered the electronics industry against copyright infringement claims. When Sony introduced a video-cassette recorder, Hollywood studios sued because the device could copy television shows. The Supreme Court in 1984 in *Sony Corp. of America v. Universal City Studios, Inc.* protected the new technology, arguing that the device had "substantial noninfringing uses."[97] As Pamela Samuelson writes, had it not been for the relief from liability offered by the *Sony* decision, "tape recorders, photocopiers, CD burners, CD ripping software, iPods, and MP3 players, and a host of other technologies that facilitate private or personal use copying might have never become widely available."[98] The decision did not insulate every new technology. Peter Menell and David Nimmer observe that, in the years since the *Sony* decision, "the developers and distributors of Napster, Aimster, Grokster, Morpheus, and KaZaA—peer-to-peer systems that have

where the government could not do so directly"); Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 622 (2006).

[95] *But see* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 522–24 (1999) (arguing that the DMCA was broader than necessary in relation to WIPO, and that the Act's anti-circumvention provisions "do not match up well with the needs of the digital economy").

[96] Murdoch said, "Piracy leader is Google who streams movies free, sells [advertisements] around them." David Carr, *A Glimpse of Murdoch Unbound*, N.Y. TIMES, Jan. 30, 2012, at B1 (internal quotation mark omitted).

[97] 464 U.S. 417, 442 (1984).

[98] Pamela Samuelson, *The Generativity of* Sony v. Universal: *The Intellectual Property Legacy of Justice Stevens*, 74 FORDHAM L. REV. 1831, 1850 (2006); *see also* Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1356 (2004) (arguing that the *Sony* rationale offered "significant protection for innovation in technologies that are related to the use of copyrighted material").

noninfringing uses—have all been held liable for contributory infringement, *Sony* notwithstanding."[99]

Yet, the Supreme Court's own intervention in the digital copyright, in the case of *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*,[100] yielded a result that was largely friendly to Silicon Valley innovation. The movie studios and others had invited the Court to erode the *Sony* rule by requiring that it be the principal actual use of a device or service, not its potential use, that should determine its legality.[101] In arguing their cause before the Court, the copyright industries understood that they must not be seen as standing in the way of innovation. The songwriter plaintiffs devoted one of the three parts of their main brief to the proposition that "[h]olding Grokster and Streamcast liable will encourage, not restrain, legitimate commerce."[102] The motion picture studios and recording companies argued that a holding in favor of the file-sharing services would threaten "artistic innovation" as well as "obstruct[] innovators seeking to use digital technology for lawful distribution of copyrighted works."[103] For their part, the file-sharing services pressed the potential chill on innovation with even greater zeal. The word "innovation" appears no less than forty-five times in their brief. The file-sharing services argued:

> Modifying the *Sony* rule as petitioners suggest would . . . . deter investment in innovation by subjecting innovators to standards that are unpredictable in application and expensive to litigate, and put large sectors of the digital-technology economy in the hands of entertainment-industry incumbents with a vested interest in preserving their existing business arrangements, to the detriment of both creators and consumers.[104]

Justice David Souter, writing for the Court, observed that the rule in Sony "leaves breathing room for innovation and a vigorous commerce."[105]

The Supreme Court's decision marked the death knell for two Internet services, Grokster and Streamcast, which could be found liable for "inducing"

---

[99] Peter S. Menell & David Nimmer, *Legal Realism in Action: Indirect Copyright Liability's Continuing Tort Framework and* Sony*'s De Facto Demise*, 55 UCLA L. REV. 143, 145 (2007).

[100] 545 U.S. 913 (2005).

[101] *See* Reply Brief for Motion Picture Studio & Recording Co. Petitioners at 1–6, *Grokster*, 545 U.S. 913 (No. 04-480).

[102] Brief for Songwriter & Music Publisher Petitioners at 17, *Grokster*, 545 U.S. 913 (No. 04-480).

[103] Reply Brief for Motion Picture Studio & Recording Co. Petitioners, *supra* note 101, at 11–12.

[104] Brief for Respondents at 14, *Grokster*, 545 U.S. 913 (No. 04-480).

[105] *Grokster*, 545 U.S. at 933.

copyright infringement.[106] Yet, the *Grokster* decision itself largely continued to extend the Court's welcome mat for innovation, even where the service (like any digital information service) might be used widely for copyright infringement.[107] It only outlawed services that explicitly condoned or "induced" such infringement. While an Internet provider could not "tout the copyright-infringing uses" of its tools, Jonathan Zittrain notes that "the tools themselves seem to have remained largely, if not entirely, protected by *Sony*."[108]

The American concept of "fair use" also proved conducive to various innovations in the digital realm. Fair use allowed a court to provide exceptions to copyright after considering multiple factors. Take the example of image search, introduced by Google in 2001. Google's computers now supplied images that matched search terms. This required Google to show smaller, "thumbnail" versions of those images. When Google was challenged, the Ninth Circuit ruled that these thumbnail versions of the images constituted fair use.[109]

C. Privacy

U.S. privacy law offers limited constraints for American Internet entrepreneurs. The vaunted common law privacy torts are each quite narrow in scope and mostly unavailing to web users concerned about protecting personal information.[110] The torts are not well-suited to the typical privacy concern with

---

[106] *Id.* at 941.

[107] Anupam Chander & Madhavi Sunder, *Apple Rips While Grokster Burns: How MGM v. Grokster Benefits Information Technology Companies*, FINDLAW (June 29, 2005), http://writ.lp.findlaw.com/commentary/20050629_sunder.html ("This week's Supreme Court decision in *MGM v. Grokster* . . . substantially reduces the risks faced by information technology companies as they innovate. Steve Jobs must be breathing a sigh of relief."). *But see* Lawrence Lessig, *A Rotten Ruling*, WIRED (Sept. 13, 2005), http://www.wired.com/wired/archive/13.09/posts.html?pg=7 (arguing that *Grokster* created uncertainty and would impose substantial litigation costs on companies); *see also* Rob Hof, *Larry Lessig: Grokster Decision Will Chill Innovation*, BUSINESS WEEK (June 28, 2005), http://www.businessweek.com/the_thread/techbeat/archives/2005/06/larry_lessig_gr.html.

[108] Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 291 (2006).

[109] Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1168 (9th Cir. 2007).

[110] James Whitman concludes that "after a century of legal history, [the right-to-privacy tort] amounts to little in American practice today." Whitman, *supra* note 21, at 1204; *see also* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. ON TELECOMM. & HIGH TECH. L. 357 (2011) (arguing that tort privacy is poorly suited to the digital age); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1634 (1999) ("Unfortunately, various limitations that the common law has established on [the privacy torts] eliminate their usefulness in responding to violations of privacy in cyberspace. As a result of these restrictions, most data processing on the Internet is excluded from the scope of the four branches of the privacy tort." (footnote omitted)). Consider each of Prosser's famous torts in turn. The tort of intrusion upon seclusion requires that the tortfeasor intentionally invade the solitude of another in his or her private affairs, such as through secret

respect to social media, doing little to bar the use of personal information for marketing or the onward sharing of personal information in unexpected ways.[111] Statutory protections remain quite narrow.[112]

With the dawn of the World Wide Web, the Clinton Administration convened a task force to think through privacy rules for these new communications services. The task force's 1995 white paper began by observing that "many people may be reluctant to use the NII [National Information Infrastructure] if they are afraid that the personal information transmitted over it can be used in ways that are unexpected or inappropriate."[113] But instead of a new omnibus privacy statute, the task force

videotaping. STUART M. SPEISER ET AL., 9 THE AMERICAN LAW OF TORTS § 30.9 (2012). Courts have been reluctant to extend the tort to cases involving Google photos of the outside of one's home, or the disclosure of information for advertising purposes. *See, e.g.*, Boring v. Google Inc., 362 F. App'x 273, 279–80 (3d Cir. 2010) (rejecting seclusion claim involving Internet posting of photos of private a residence taken from outside, where the residents were not visible inside home); Deering v. CenturyTel, Inc., No. CV-10-63-BLG-RFC, 2011 WL 1842859, at *2 (D. Mont. May 16, 2011) ("[T]here is no reasonable expectation of privacy when a plaintiff has been notified that his Internet activity may be forwarded to a third party to target him with advertisements."). The tort of publication of embarrassing private facts requires that the facts be held private, be embarrassing in nature, and be published; it has been successful relatively rarely. 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5:68 (2d ed. 2011). There may be a narrow set of claims available for sharing on social networks—but typically against the individual users who forward private material, rather than the network itself (again as a result of 47 U.S.C. § 230). *See* Anupam Chander, *Youthful Indiscretion in an Internet Age*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 124, 127, 130 (Saul Levmore & Martha C. Nussbaum eds., 2010). The false light tort requires a person whom intentionally or recklessly publicizes false information about another person. 2 RODNEY A. SMOLLA, LAW OF DEFAMATION § 10:8 (2d ed. 2011). Invasion of the right of publicity requires the exploitation of a person's name or likeness, usually for commercial gain; it might be implicated when Facebook seeks to use one's photo to promote a product (though consent may be based on the site's terms of use). *See, e.g.*, CAL. CIV. CODE § 3344 (West 2013); MCCARTHY, *supra*, at § 3:2; Amy Morganstern, *In the Spotlight: Social Network Advertising and the Right of Publicity*, 12 INTELL. PROP. L. BULL. 181, 183–85 (2008); Daniel Nemet-Nejat, *Hey, That's My Persona!: Exploring the Right of Publicity for Blogs and Online Social Networks*, 33 COLUM. J.L. & ARTS 113 (2009).

[111] William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105, 1135–36 ("The most significant problem with these limits on disclosure derives from their circumscribed scope. . . . Against this general background, social marketing appears unlikely to violate most U.S. privacy laws.").

[112] Jane K. Winn, *Electronic Commerce Law: 2001 Developments*, 57 BUS. LAW. 541, 573 (2001) ("American privacy law . . . [has] a surprisingly narrow scope when applied to the business use of personal information."); Ian C. Ballon, *Using Trademarks to Drive Traffic to Websites and Other E-Commerce Law Issues*, 590 PLI/Pat 111 (2000) ("U.S. Data privacy law . . . afford[s] substantial protection in very narrow areas."); Daniel J. Solove, *The Origins and Growth of Information Privacy Law*, 828 PLI/Pat 23 (2005); Schwartz, *supra* note 110, at 1616 (describing the "[l]ack of [p]rivacy in [c]yberspace" under U.S. law).

[113] U.S. DEP'T OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995), *available at* http://www.ntia.doc.gov/legacy/ntiahome/privwhitepaper.html. The white paper was posted at gopher://www.ntia.doc.gov/00/policy/privwhitepaper.txt using the now-obsolete Gopher protocol, revealing how fluid and inchoate Internet practices and standards were at the time.

proposed a voluntary framework whereby companies would notify users of how they intended to collect and use information, and seek the consent of the users for such collection and use.[114] That model, of course, became the operative one, allowing websites to set the terms for user privacy, subject only to public acceptance of those terms rather than regulatory constraints.

Congress did in fact act to protect children's privacy through the Children's Online Privacy Protection Act of 1998 (COPPA). COPPA established significant protections for younger children online, including requiring parental consent before websites could collect information from children under thirteen and requiring adequate security measures for information that was collected.[115] This might have posed a challenge to web providers, which would have had to either segregate how they handled children's information or refuse children access. Yet, the statute proved easy to avoid by e-commerce providers, who simply officially banned those under thirteen from their sites. Millions of American children responded by fabricating a false birth year to enable them to access sites such as Facebook[116]—an expedient available to youth with a modicum of mathematical ability.[117] As long as the sites did not have actual knowledge that the child was under thirteen, they had no statutory obligation to treat his or her information with care.[118]

During the last decade, the absence of strong privacy regulations proved particularly important because of the business model used by many consumer-oriented websites. Web 2.0 providers earn money through advertising or through selling additional services. If the online provider can tailor advertisements precisely to the interests of the user, then the advertising will be

---

[114] *Id*. ("If such private sector action is not forthcoming, however, that framework can and should form the basis for government-mandated privacy regulations or standards.").

[115] 15 U.S.C. § 6502(b)(1)(A)(ii) (2012) (requiring website operators "to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children"); *id*. § 6502(b)(1)(D) (providing for the promulgation of regulations that "require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children").

[116] *Consumer Reports* estimates that nearly 7.5 million children under the age of thirteen use Facebook by lying about their age. *Online Exposure*, CONSUMER REP., June 2011, at 29, 30.

[117] Tony Bradley, *Kids Under 13 Are Already Allowed on Facebook*, PCWORLD (May 21, 2011, 6:48 AM), http://www.pcworld.com/article/228348/kids_under_13_are_already_allowed_on_facebook.html; Matt Richtel & Miguel Helft, *Where Age Is What You Say It Is*, N.Y. TIMES, Mar. 12, 2011, at B1.

[118] Under the actual knowledge standard, "operators of general audience Web sites are not required to investigate the ages of their users." Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804, 59,806 (Sept. 27, 2011) (to be codified at 16 CFR pt. 312).

more lucrative.[119] In other words, the more the online provider knows about you, the more it can earn. Rules protecting user privacy can, accordingly, interfere with a company's ability to gather information about you, or to develop a better profile of you by collating information with other online providers. Thus, the absence of a broad array of effective privacy-enhancing restraints leaves online services largely free to exploit user information for maximum profit. As long as the services do not promise more privacy than they actually deliver, online companies in the United States have a free hand with information.

The absence of privacy constraints proved especially conducive to Internet innovation. The success of Silicon Valley enterprises has often been a result not just of a single initial inspiration, but of successive rounds of serial innovation within a single firm.[120] Much of this innovation results from rapid experimentation—roll-out of new products, beta-testing, and appraisal. Many Web 2.0 businesses rely upon a trial-and-error model for innovation. Beta offerings are presented to be retracted, modified, enhanced, or finalized depending on the market reception. The plasticity of the software allows quick responses to market conditions. Because the businesses are innovating new relationships between users and information, the risk to privacy in this process of experimentation is especially high. A liberal privacy regime thus proves conducive to this kind of trial-and-error method for innovation, allowing companies to base their offerings not on legal constraints but on market reaction.

---

[119] Robert D. Hof, *You Are the Ad*, TECH. REV., May/June 2011, at 64, 66 ("[O]ne reason advertisers love Facebook is that ads can be precisely targeted to specific audiences on the basis of their stated interests, location, 'likes,' and much more."); Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES MAG., Feb. 19, 2012, at 30 ("Almost every major retailer, from grocery chains to investment banks to the U.S. Postal Service, has a 'predictive analytics' department devoted to understanding not just consumers' shopping habits but also their personal habits, so as to more efficiently market to them."); Saul Hansell, *Microsoft Plans to Sell Search Ads of Its Own*, N.Y. TIMES, Sept. 26, 2005, at C1; Michael Zimmer, *The Externalities of Search 2.0: The Emerging Privacy Threats When the Drive for the Perfect Search Engine Meets Web 2.0*, 13 FIRST MONDAY (2008), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/2136/1944 ("[S]earch engines can charge higher advertising rates when ads are accurately placed before the eyes of users with relevant needs and interests . . . .").

[120] Google, which occupies the campus of Silicon Graphics, a company that once was a flagship Silicon Valley enterprise, erected an enormous dinosaur statue on that campus to serve as a reminder of the need to innovate constantly. Dean Takahashi, *Google: Where Food Is Free, IQs Are High*, SAN JOSE MERCURY NEWS, July 19, 2007; *see also The Internet: How Long Will Google's Magic Last?*, ECONOMIST, Dec. 4, 2010, at 81 (quoting Google's head of product management Jonathan Rosenberg as stating, "[Y]ou only win if you innovate faster than the players in the rest of the system." (internal quotation mark omitted)).

The end result is as follows: while Facebook's and Google's innovations have often drawn public outcries,[121] they seldom draw successful lawsuits or government enforcement actions.[122]

***

By the end of the twentieth century, laws conducive to the business model of Web 2.0 were in place. Companies would offer platforms on which users could provide content, which would in turn attract other users. Companies would then monetize these large numbers of users by exploiting personal information about them for marketing. And the law would abide this.

I have shown that, just as nineteenth-century American judges altered the common law in order to subsidize industrial development, judges and

---

[121] *See, e.g.*, Economist Intelligence Unit, *"Act Now, Apologize Later": Will Users "Friend" Facebook's Latest Intrusion on Privacy?*, EXEC. BRIEFING, June 18, 2010, at 7 (consumer advocates complained that Facebook's new "Open Graph" architecture which connects third-party websites to the Facebook Platform so that users can "like" or recommend content, invades user privacy); Miguel Helft, *Google Photos Stir a Debate Over Privacy*, N.Y. TIMES, June 1, 2007, at C1 (consumer advocates complained that Google's new feature on Google Maps, which shows pictures of street-level views of addresses, invades user privacy); Jon Swartz, *Privacy Advocates Don't 'Like' Facebook's Ad Plans*, USA TODAY, Jan. 31, 2011, at B1 (consumer advocates complained that Facebook's new feature called "Sponsored Stories," which allows advertisers to pay for users to be able to "like" their brand or check in at a store and have that action appear on the user's friends' pages, invades user privacy); Jamin Warren & Vauhini Vara, *New Facebook Features Have Members in an Uproar*, WALL ST. J., Sept. 7, 2006, at B1 (consumer advocates complained that Facebook's new feature called "News Feed," which keeps track of users' actions and then notifies all of their friends of those developments, invades user privacy); Jenna Wortham, *Facebook Flagged on Privacy Issue*, N.Y. TIMES, Aug. 23, 2010, at B4 (consumer advocates complained that Facebook's new feature called "Facebook Places," which allows users to share their location and find their friends' locations, invades user privacy); Michael Arrington, *Google Desktop 3.0: Privacy Is Dead(er)*, TECHCRUNCH (Feb. 8, 2006), http://techcrunch.com/2006/02/08/google-desktop-new-version-tonight/ (consumer advocates complained that Google's new search feature, which allows users to search the contents of one computer from another, invades user privacy); Thomas Claburn, *Privacy Groups Decry Google's Plans for DoubleClick*, INFO. WEEK (Apr. 20, 2007, 3:57 PM), http://www.informationweek.com/news/199200331 (consumer advocates complained that Google's new feature called "Web History," which allows Google to create a complete picture of its users' online activity by combining data about Google searches, webpage visits, images, videos, and news stories, invades user privacy); *Facebook Facial Recognition Raises Eyebrows in Germany, EU*, DEUTSCHE WELLE (June 9, 2011), http://dw.de/p/11Xg8 (consumer advocates complained that Facebook's new feature using facial recognition technology to identify persons in newly added photos, invades user privacy); *Facebook Opens Users Shopping Habits*, UPI (Nov. 24, 2007, 6:46 PM), http://www.upi.com/Business_News/2007/11/24/Facebook-opens-users-shopping-habits/UPI-61161195948019/ (consumer advocates complained that Facebook's new feature, which makes users' online shopping habits public, invades user privacy).

[122] There are exceptions, one arising from Google's introduction of Buzz, and the other from Facebook's introduction of Beacon. *In re* Google Buzz User Privacy Litig., No. 5:10-CV-00672-JW, 2010 WL 6336647 (N.D. Cal. Sept. 3, 2010); Lane v. Facebook, Inc., No. C 08-3845 RS, 2010 WL 2076916 (N.D. Cal. May 24, 2010); *In re* Facebook, Inc., No. 092-3184, 2011 WL 6092532 (F.T.C. Nov. 29, 2011); *In re* Google Inc., No. 102-3136, 2011 WL 5089551 (F.T.C. Oct. 13, 2011).

legislators at the turn of the Millennium altered the law to subsidize the development of Internet companies. Did technologically advanced nations in Europe and Asia do the same?

II. CONSTRAINTS IN EUROPE AND ASIA

Could Google have been founded in London? According to Google's Larry Page and Sergey Brin, as related by Prime Minister David Cameron, the answer is no.[123] This is not due to the lack of brilliant engineers in the United Kingdom, or sufficient capital in the City of London. Prime Minister Cameron explains that the Google founders told his government that Google's service "depends on taking a snapshot of all the content on the internet at any one time and they feel our copyright system is not as friendly to this sort of innovation as it is in the United States."[124] Unlike the law in the United Kingdom, where Google's search engine activities might cross the line of copyright infringement without any promising legal lifeline, U.S. law seems more flexible. Prime Minister Cameron explained, with apparent envy: "Over there, they have what are called 'fair-use' provisions, which some people believe gives companies breathing space to create new products and services."[125]

But did not Europe offer inducements through the law to web enterprises similar to those in the United States? And what of Japan and South Korea, Asian nations that were at the forefront of creating information societies?[126] I

---

[123] *UK Copyright Laws to Be Reviewed, Announces Cameron*, BBC, http://www.bbc.co.uk/news/uk-politics-11695416?utm_source=twitterfeed&utm_medium=twitter (last updated Nov. 4, 2010, 1:37 PM). Cameron accordingly launched a review of British intellectual property law, resulting in the important study known as the Hargreaves Report. IAN HARGREAVES, DIGITAL OPPORTUNITY: A REVIEW OF INTELLECTUAL PROPERTY AND GROWTH (2011), *available at* http://www.ipo.gov.uk/ipreview-finalreport.pdf. There is controversy as to veracity of this "killer quote." Andrew Orlowski, *Cameron's 'Google Review' Sparked by Killer Quote That Never Was*, REGISTER (Mar. 21, 2012), http://www.theregister.co.uk/2012/03/21/cameron_google_source/.

[124] *UK Copyright Laws to Be Reviewed, Announces Cameron*, *supra* note 123.

[125] *Id*. (internal quotation mark omitted). This is not idle speculation offered in retrospect. Google's Larry Page reports that even in the relatively liberal United States, "at the time, people were arguing that making a copy of a file in a computer's memory was a violation of copyright. We put the whole web on our servers, so if that were true, bye-bye search engines." Levy, *supra* note 13.

[126] *See* Brian Deutsch, Editorial, *See the Digital Future: Korea Today*, PITTSBURGH POST-GAZETTE, Mar. 28, 2010, at B7 (detailing South Korea's information-based society); Mark McDonald, *For South Korea, Internet at Blazing Speeds Is Still Not Fast Enough*, N.Y. TIMES, Feb. 22, 2011, at B3 (noting that South Korea plans to upgrade its already fast Internet services to provide one gigabit per second Internet speeds to every home in the country); Jon Brodkin, *Two-Thirds of U.S. Internet Users Lack Fast Broadband*, NETWORK WORLD (Jan. 24, 2011, 3:29 PM), http://www.networkworld.com/news/2011/012411-us-internet-users-broadband.html (noting that in the United States only 34% of users have Internet connections greater than 5 Mbps, while in Korea and Japan over 60% of Internet connections are greater than 5 Mbps); *Internet*

will show that indeed these nations took steps to adjust their laws to the new cyber-environment, but without the same depth of preference for web enterprises. Where the United States sought to insulate Internet intermediaries from liability for the misdeeds of their users, Europe, Japan, and South Korea created special responsibilities for Internet services. Indeed, what might be celebrated in the United States could be illegal in Europe, Japan, and South Korea. Facebook finds the distinction between U.S. law of intermediary liability and the law elsewhere to be material to its investors. Facebook states that the risk that it will face claims "is enhanced in certain jurisdictions outside the United States where our protection from liability for third-party actions may be unclear and where we may be less protected under local laws than we are in the United States."[127]

Comparative law scholars may observe that many jurisdictions lack the statutory or punitive damages available under U.S. law, making more legally demanding obligations abroad less harsh in reality in comparison to the plaintiff-friendly United States. But when it comes to Internet intermediaries, a simple injunction alone could require a restructuring of the system that made the platform economically unfeasible. Only the most foolhardy financiers would invest in an early stage enterprise that had a business that a tribunal might declare illegal at any moment. The programmer might even be sent to jail.

In the sections below, I examine the laws of the European Union, South Korea, and Japan, demonstrating that when it comes to intermediary liability, copyright liability, and privacy, the laws of these regions are far less conducive to Internet enterprise than the United States.

A. Intermediary Liability

1. European Union

The European Union's intermediary liability law proved less welcoming to Internet entrepreneurs than U.S. law. Europe takes a unified approach to the

Economy: Wireless Broadband Subscriptions Top Half a Billion, Says OECD, OECD (June 26, 2011), http://www.oecd.org/newsroom/interneteconomywirelessbroadbandsubscriptionstophalfabillionsaysoecd.htm (noting that Korea's broadband penetration doubles the OECD average); *Japan Internet Users Spend Most Time on Blogs Worldwide*, COMSCORE (Aug. 24, 2011), http://www.comscore.com/Press_Events/Press_Releases/2011/8/Japan_Internet_Users_Spend_Most_Time_on_Blogs_Worldwide (noting that Japanese Internet users spend the most time on Internet blogs).

[127] Facebook, Inc., Registration Statement (Form S-1) 23 (Feb. 1, 2012).

issue of intermediary liability, setting the same standard for holding intermediaries liable regardless of the nature of the underlying offense. There is logic to this approach, even if it is unlike the American approach, which, as we have seen in Part I.A above, offers different rules for intermediary liability for copyright, trademark, and other offenses.[128] The European Union's Electronic Commerce Directive sets out what are essentially safe harbors from liability for specified intermediary activities, such as acting as a "mere conduit," "caching," or "hosting" (but not search services). Some countries go further to include safe harbors for search engines and hyperlink providers.[129] Yet, from the perspective of Internet intermediaries, the safe harbors remain inferior to their American counterparts, providing less protection for copyright, trademark, defamation, and other claims. I explain here some of the deficiencies of the European law vis-à-vis U.S. law for Internet intermediaries.[130] I reserve discussion of intermediary liability for copyright infringement for the following section.

First, the European approach stops far short of the near blanket exclusion from liability offered by the Communications Decency Act for non–intellectual property related wrongs.[131] Second, the Electronic Commerce Directive largely adopts the DMCA's notice-and-takedown approach, but leaves open the possibility of additional proactive responsibilities on the part of the online intermediary. Even while disavowing any duty to "monitor,"[132] the European law expressly contemplates the imposition by member states of "duties of

---

[128] The Europeans describe their approach as a "horizontal" one, encompassing secondary liability for all illicit behavior. Miquel Peguera, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 COLUM. J.L. & ARTS 481, 482 (2009).

[129] THIBAULT VERBIEST ET AL., MARKT/2006/09/E, STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES, *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

[130] I do not mean to suggest that European law is invariably hostile to Internet intermediaries. For example, an Italian court recently rejected an attempt to hold Google liable for the automatically generated suggestions of additional search terms that happened to add offensive words after a person's name. Giulio Coraggio, *Google NOT Liable for Suggest Search Results*, GAMINGTECHLAW (Jan. 4, 2013), http://www.gamingtechlaw.com/2013/04/google-not-liable-for-suggest-search.html.

[131] *See* Eric Pfanner, *YouTube Can't Be Liable on Copyright, Spain Rules*, N.Y. TIMES, Sept. 24, 2010, at B7 (quoting a London lawyer as saying, "'The issue of when a host was liable has been getting a bit vague, and some hosts in Europe have been getting a little bit nervous'"); Bradley L Joslove & Vanessa De Spiegeleer-Delort, *Web 2.0: Aggregator Website Held Liable as Publisher*, INT'L L. OFFICE (June 26, 2008), http://www.internationallawoffice.com/newsletters/detail.aspx?g=4b014ec1-b334-4204-9fbd-00e05bf6db95#11 ("[T]he scope of liability of Web 2.0 websites is an unsettled point of law.").

[132] Directive 2000/31, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1, 13 [hereinafter Electronic Commerce Directive].

care" on intermediaries to detect and prevent certain activities.[133] Third, the European directive lacks a statutory notice-and-takedown regime, creating greater uncertainty among European providers as to whether they have sufficient knowledge to withdraw liability if they do not delete material.[134] Finally, the European approach permitted injunctions against online service providers more liberally than the American approach, which was more attentive to the problem of prior restraint.[135] The Electronic Commerce Directive contemplates "orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it."[136]

The difference between the American and European approaches to intermediary liability in trademark is evident when we contrast two authoritative decisions involving the same defendant (eBay) and similar facts on either side of the Atlantic (storied trademark holders claiming infringement). Before the European Court of Justice, L'Oréal sought to hold eBay liable for trademark infringement occurring on eBay's site.[137] EBay relied on Article 14(1) of the Electronic Commerce Directive to argue that it was "not liable for the information stored at the request of a recipient of the service."[138] The court held that this immunity would not be available where the operator had undertaken "an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale."[139] The Court of Justice sent the case back to the national court for consideration of whether eBay "was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously."[140] Reporting on the decision, the law firm of Latham & Watkins advised its clients that sites like eBay will "have to engage in a higher degree of self policing in the future, especially with respect to the offer for sale of well

---

133 *Id*. at 6.

134 Peguera, *supra* note 128, at 490.

135 *Id*. at 486.

136 Electronic Commerce Directive, *supra* note 132, at 6.

137 Case C-324/09, L'Oréal SA v. eBay Int'l AG, 2011 E.C.R. I-06011, para. 34 (July 12, 2011), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=107261&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1040212.

138 Electronic Commerce Directive, *supra* note 132, at 13.

139 *L'Oréal*, 2011 E.C.R. I-06011, para. 116.

140 *Id*. para. 124.

known or famous brands."[141] They further observed that eBay might have to modify its system with respect to Europe to allow for easier identification of a seller: "It would be ironic, but predictable that it could become as difficult to open an account to sell goods on an auction site without proper identity checks as it is to open a bank account or instruct a lawyer in the EU."[142] By contrast, in *Tiffany (NJ) Inc. v. eBay Inc.*, the Second Circuit Court of Appeals largely sided with eBay against the trademark holder.[143] The U.S. court upheld summary judgment in favor of eBay on the issue of contributory liability for trademark infringement.[144] It remanded the case on the issue of whether eBay had itself misled users in its advertising campaign invoking the Tiffany's name.[145] Commentators rightly hailed the case as a victory for Internet intermediaries.[146]

2. South Korea

Where U.S. law seeks to reduce the liability of Internet intermediaries for statements posted on their sites, South Korean law seeks to make intermediaries responsible for activities on their sites. In the wake of demonstrations against American beef exports to Korea organized online, the South Korean legislature imposed additional obligations on Internet intermediaries to police online behavior, on the theory that the public was manipulated by allegedly false claims about the threat of mad cow disease.[147] It also imposed additional obligations on users themselves—the Framework Act on Telecommunications singles out those using electronic means to spread information: "A person spreading a false rumor maliciously intending to damage the public interest by using an electronic machine can be sentenced to imprisonment for under five years or given a fine under fifty million won."[148]

---

[141] Latham & Watkins, Client Alert No. 1226, *L'Oréal v. eBay*: The Court of Justice of the European Union Tightens Liability of Online Marketplace Operators 4 (2011), http://www.lw.com/thoughtLeadership/cjeu-tightens-online-marketplace-operators-liability. One case note is headlined, "*L'Oréal v. eBay*: A Warning to Online Marketplace Operators." Joel Smith & Joanna Silver, 6 J. INTELL. PROP. L. & PRAC. 765 (2011).

[142] Latham & Watkins, *supra* note 141, at 4.

[143] 600 F.3d 93, 109 (2d Cir. 2010).

[144] *Id.*

[145] *Id.* at 114.

[146] *Federal Appellate Courts Poised to Deliver Key Cyberlaw Rulings in 2012*, 17 ELECTRONIC COM. & L. REP. 67 (2012) (characterizing decision as "a favorable ruling for online intermediaries").

[147] John M. Leitner, *To Post or Not to Post: Korean Criminal Sanctions for Online Expression*, 25 TEMP. INT'L & COMP. L.J. 43, 54–55 (2011).

[148] *Id.* at 59 (quoting Jeongitongsingibonbeop [Framework Act on Telecommunications], Act No. 4393, Aug. 10, 1991, art. 47(1), *amended by* Act No. 10393, Jul. 23, 2010 (S. Kor.), *translated at*

Furthermore, like many countries, South Korea has a more liberal substantive standard for defamation (thereby favoring plaintiffs) and permits injunctive relief for defamation.[149]

In 2009, the Korean Supreme Court issued a decision holding web portal sites Naver, Daum, SK Communications, and Yahoo Korea liable for the defamation of a person named "Kim" occurring on their sites.[150] The court upheld judgments of 10 million won, 7 million won, 8 million won, and 5 million won, respectively, against these services, stating that a web service "must delete slanderous posts or block searches of the offending posts, even if not requested to do so by the victim."[151] While these were relatively small judgments amounting to just thousands of U.S. dollars (approximately $5,700 at the highest[152]), this might well have caused sites to fear the accumulation of such fines. The court held that

> the obligation of the portal site to remove the [defamatory material] arose when (a) the content was apparently illegal in the sense of defamation, and (b) the portal site had actual knowledge of the illegality of the infringing activity or, awareness of facts or circumstances from which infringing activity was apparent even without the [victim's] notice . . . to the portal site.[153]

Critics worried that the decision would chill speech, causing websites to delete user posts to preclude liability.[154] The decision seems to confirm Kyu Ho Youm's observation that, at least when reputation or honor is at risk, "South Korea does not protect freedom of expression as a transcendent value."[155]

---

http://elaw.klri.re.kr) (internal quotation marks omitted); *see also id*. at 58 ("Cyber defamation is therefore punished with stronger penalties than defamation expressed through other channels . . . .").

149 Kyu Ho Youm, *Freedom of Expression and the Law: Rights and Responsibilities in South Korea*, 38 STAN. J. INT'L L. 123, 145 (2002) ("The South Korean judiciary has continually rejected any defamation defense premised upon the U.S. model of 'actual malice,' and injunctive relief continues to exist as a prior restraint against publication.").

150 *Courts Open Up South Korean Web Sites to Liability Charges*, HANKYOREH (Apr. 17, 2009, 12:47 PM), http://english.hani.co.kr/arti/english_edition/e_national/350253.html.

151 *Id*.; *accord* Supreme Court [S. Ct.], 2008Da53812, Apr. 16, 2009 (S. Kor.).

152 For historical exchange rates at the date of the 2009 decision, see http://www.x-rates.com/historical/?from=EUR&amount=1.00&date=2009-04-16.

153 Memorandum from Sung Gi Hwang, Professor, Hanyang Univ., to author (Mar. 7, 2012) (on file with author).

154 *Id*.

155 Kyu Ho Youm, *Defamation Law and the Internet in South Korea*, 9 MEDIA & ARTS L. REV. 141, 141 (2004) (citing article 21 of the Constitution of Korea, which provides that "Neither speech nor the press shall violate the honor or rights of other persons . . .").

In February 2012, the Korean Constitutional Court upheld the power of the Korea Communications Standards Commission under the Act on the Promotion of Information and Communications Network Utilization and Information Protection (the Network Act) to order the takedown of "unhealthy information" on the Internet.[156] Importantly, however, the Network Act did not impose "penalties against non-compliance."[157]

3. Japan

Japan may not be a litigious society, but Internet providers seem to have faced their share of claims. In Japan, running a bulletin board service in 1997 might render you liable for the defamation occurring on that service. That year, a Tokyo trial court held Internet service provider Nifty Service liable for failing to delete defamatory messages.[158] A heated exchange on a forum titled "Contemporary Ideas" had resulted in defamatory posts, which the forum's manager left up, "apparently believing that continuing the discussion and trying to engage the parties in a more issue-oriented dialogue would address the problem."[159] It was not until 2001 that the Tokyo High Court would reverse the decision.[160]

That same year, the Diet passed the Law Concerning the Limits of Liability for Damages of Specified Telecommunications Service Providers, under which a telecommunications service provider would not be liable for the actions of its users unless it knew, or where there was "reasonable ground to find that said relevant service provider could know[,] the violation of the rights of others was caused by the information distribution via said specified telecommunications."[161] Like the European approach, the law applies to all

---

156 Constitutional Court [Const. Ct.], 2011Hun-Ka13, Feb. 23, 2012, (24-1(A) KCCR, 25) (S. Kor.).

157 *Id*.

158 Hisanari Harry Tanaka, *Post-Napster: Peer-to-Peer File Sharing Systems: Current and Future Issues on Secondary Liability Under Copyright Laws in the United States and Japan*, 22 LOY. L.A. ENT. L. REV. 37, 67 (2001).

159 Salil K. Mehra, *Post a Message and Go to Jail: Criminalizing Internet Libel in Japan and the United States*, 78 U. COLO. L. REV. 767, 801 (2007).

160 *Id*. at 801–02.

161 Tokutei denkitsuushin ekimu teikyousha no songaibaishou sekinin no seigen oyobi hasshinsha jouhou no kaiji ni kansu ru houritsu [Law Concerning the Limits of Liability for Damages of Specified Telecommunications Service Providers and the Right to Request Disclosure of Identification Information of the Senders], Law No. 137 of 2001, art. 3, *translated at* http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/Compensation-Law.pdf (Japan); *see also* Itsuko Yamaguchi, *Beyond De Facto Freedom: Digital Transformation of Free Speech Theory in Japan*, 38 STAN. J. INT'L L. 109, 114 (2002) (characterizing standard as "considerable reason" to know of wrongdoing).

intermediary activity, whether involving copyright, trademark, or tort claims.[162] By imposing not only an actual knowledge-and-takedown approach, but also a more vague "reasonable ground" that the provider "could know," the 2001 limitation law was a pale shadow of the American § 230 from the perspective of Internet enterprises.

In 2002, the popular bulletin board service 2Channel was held liable using the approach of the 2001 law (but not its text because the complained of acts occurred before the law became effective). The court found that the site's "management had been unreasonable in its refusal to remove the offensive posts when requested."[163] The posts arose on a thread entitled "Corrupt Animal Hospital."[164] 2Channel was fined 4 million yen (approximately $40,000) in damages.[165] Salil Mehra suggests that while this was "not a particularly large amount, . . . it was a strong enough sign to change the behavior of 2Channel's management."[166] The site's duty to remove the infringing posts was upheld on appeal.[167]

B. Copyright

1. European Union

Two directives help frame the inquiry of intermediary liability for copyright infringement in the European Union. As described above, the Electronic Commerce Directive of 2000 provided a set of exemptions from liability for "information society services" that store information at the request of users, including immunity from copyright infringement claims.[168] The 2001 Copyright Directive offered an enumerated and exclusive list of exceptions to the rights of copyright holders.[169]

---

[162] Masanobu Katoh, *Intellectual Property and the Internet: A Japanese Perspective*, 2002 U. ILL. J.L. TECH. & POL'Y 333, 340.

[163] Mehra, *supra* note 159, at 802.

[164] *Id.*

[165] *Id.*

[166] *Id.* at 802–03.

[167] *Id.* at 802 n.146 (citing *Doubutsu byouin tai 2channeru jiken*, 1816 HANREI JIHŌ [HANJI] 52 (Tokyo High Ct., Dec. 25, 2002)).

[168] *See supra* notes 128–42 and accompanying text.

[169] Directive 2001/29, of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L. 167) 10, 12 [hereinafter Copyright Directive]; Hector L MacQueen, *'Appropriate for the Digital Age'? Copyright and the Internet: 2. Exceptions and Licensing*, *in* LAW AND THE INTERNET 203, 206 (Lilian Edwards & Charlotte Waelde eds., 3d ed. 2009).

The two directives proved inferior to their U.S. counterparts from the perspective of Internet service providers for the opposite reasons. While the Electronic Commerce Directive followed the DMCA's Title II in granting Internet service providers certain immunities arising from web hosting activities, it did not specify the exact circumstances that would guarantee freedom from liability.[170] At the same time, the very specificity of the Copyright Directive undermined its usefulness to web enterprises.[171] Rather than an open-ended doctrine of fair use, European law allowed only specified exceptions to the exclusive rights of the copyright holder.[172] These proved less flexible in responding to technological developments than American fair use, which allowed a court to consider each new case individually based on multiple factors.[173] As one British scholar notes, fair use "provide[d] the courts with some flexibility of response to change in the way copyright works are disseminated and used, whether arising from new technologies, social behavior or institutional structures."[174]

Even as late as 2008, European lawyers could only advise, "[T]he scope of liability of Web 2.0 websites is an unsettled point of law."[175] It was only at the end of 2011 and the beginning of 2012 that the European Court of Justice made clear that Internet intermediaries could not be required to affirmatively filter their entire networks for copyright infringement. In cases brought by the Belgian collecting rights society, SABAM, against Internet access provider Scarlet and online social network Netlog, the court held that enjoining these companies to filter on behalf of copyright owners uploads by all users would violate the privacy and speech rights of users, and would be unduly costly and burdensome to the Internet enterprise.[176] While the judgments in *SABAM v.*

---

[170] Lilian Edwards also notes that the DMCA regime requires that the content provider be notified and allowed to contest the allegation of illegality, whereas the European regime does not. Lilian Edwards, *The Fall and Rise of Intermediary Liability Online*, *in* LAW AND THE INTERNET, *supra* note 169, at 47, 76.

[171] Martin Senftleben, *Bridging the Differences Between Copyright's Legal Traditions—The Emerging EC Fair Use Doctrine*, 57 J. COPYRIGHT SOC'Y USA 521, 522–23 (2010) (summarizing exceptions).

[172] *Id.* at 536 ("This more restrictive approach limits the room to manoeuvre for the courts. The District Court of Hamburg, for instance, refused to bring thumbnails of pictures displayed by Google's image search service under the umbrella of the right of quotation.").

[173] *Id.* at 527 ("Leaving this discretion to the courts reduces the need for constant amendments to legislation that may have difficulty in keeping pace with the speed of technological development.").

[174] MacQueen, *supra* note 169, at 209.

[175] Joslove & De Spiegeleer-Delort, *supra* note 131.

[176] Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, at paras. 46–48 (Feb. 16, 2012), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1315853; Case C-70/10, Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM),

Netlog and *Scarlet v. SABAM* clearly support Web 2.0 enterprises, they arrived nearly a decade after the rise of such companies across the ocean.

2. *South Korea*

Korean law offers only weak protection for Internet intermediaries accused of abetting copyright infringement. In 2003, Korea adopted special provisions to regulate and protect online service providers (OSPs). However, the liability limitation

> operates differently from the safe harbor provisions in the DMCA in that it does not provide a qualifying OSP with a complete indemnity against secondary liability: the preventive measures undertaken by the OSP only serve to limit or reduce its liability, and only provide a complete indemnity when these measures are 'technically' infeasible or ineffective to prevent or stop the infringing activity.[177]

Korean peer-to-peer file trading service Soribada, having been warned by the courts that it could be held liable for the copyright infringement of its users, instituted a filtering system that "would deny a user's request to download a file for which the copyright holder had specifically requested protection."[178] The Seoul High Court ruled against Soribada nonetheless, suggesting that Soribada could have designed its system to permit downloads only of music files for which the copyright owner had provided a license.[179] This legal entitlement creating an opt-in system rather than an opt-out system has tremendous market importance, as few people (or companies) alter the default setting.[180] This is what Lawrence Lessig characterizes as a "permissions culture"—ask first, before doing.[181] In 2009, Korea introduced the world's first graduated response law, a provision widely sought by the content industries.[182]

2011 E.C.R. I-11959 paras. 48, 52 (Nov. 24, 2011), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1317843.

[177] Daniel Seng, *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries*, at para. 104, WIPO, http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf (last visited Jan. 10, 2014) (preliminary version World Intellectual Property Organization study).

[178] *Id.* at para. 102.

[179] *Id.* (citing Seoul High Court [Seoul High Ct.], 2006La1535, Oct. 10, 2007 (S. Kor.)).

[180] *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 85–86 (2008).

[181] LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY, at xiv (2004).

[182] *See, e.g.*, Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373, 1376–77 (2010) (noting that South Korea has adopted a graduated response system).

Under the law, the Ministry of Culture, Sports, and Tourism can order a website hosting infringing material to remove that material, and to disable accounts of repeat offenders.[183] Furthermore, the government can shut down the website itself if it fails repeatedly to remove material, after warning.[184] Some suggested that graduated response could be used to silence political criticism "such as Agora, a discussion board operated by Daum (www.daum.net), which was a seedbed for anti-government criticism during the controversy over the beef issue."[185]

3. Japan

In Japan, developing a peer-to-peer file sharing service in the last decade might get you arrested. In 2002, Isamu Kaneko, a researcher at the University of Tokyo's School of Information and Science Technology, began distributing a peer-to-peer file-sharing program he wrote called "Winny."[186] In May 2004, he was arrested for copyright infringement because he continued to distribute his program, despite being aware that some used it to infringe copyrights.[187] After his arrest, Kaneko, an "idol" among programmers who had taught a series of lectures to nurture "superprogrammers," resigned from his University position.[188] In December 2006, the Kyoto District Court found him guilty, decrying his "selfish and irresponsible attitude" and concluding that he knew that Winny "was being used to violate the law and allowed users to do so."[189] Yet, the judge conceded that "Kaneko did not specifically intend to cause copyright violations on the Internet."[190] He was fined 1.5 million yen for the infringement.[191] The Japanese Supreme Court would ultimately clear him of all charges, but not until December 2011.[192]

Japan's 2001 law limiting liability for Internet service companies in certain circumstances was far less friendly to such companies than the DMCA. Rather than the relatively clear safe harbors of the DMCA, Japan's law removed any

---

183 *See* Kim Tong-hyung, *Upload a Song, Lose Your Internet Connection*, KOR. TIMES (May 4, 2009, 5:14 PM), http://www.koreatimes.co.kr/www/news/tech/2010/05/133_42594.html.

184 *Id*.

185 *Id*.

186 *File-Sharing Author Arrested*, DAILY YOMIURI, May 11, 2004, at 2.

187 *Id*.

188 *Winny Inventor Convicted*, DAILY YOMIURI, Dec. 14, 2006, at 1.

189 *Id*. (internal quotation mark omitted).

190 *Id*. (internal quotation marks omitted).

191 *Id*.

192 Editorial, *Absurd Arrest Rectified*, JAPAN TIMES (Dec. 26, 2011), http://www.japantimes.co.jp/opinion/2011/12/26/editorials/absurd-arrest-rectified/#.UlVbMGSSxJs.

protections if the provider knew *or should have known* of infringement occurring through its service, a far more uncertain standard, given the likelihood that some users will infringe on any Web 2.0 service.[193]

While legal clarity can sometimes help Internet companies, it can also undermine them. Like Europe, Japan enumerates specific exceptions to the rights of copyright holders, rather than the open-ended approach of American fair use law. This means that unless the particular action is authorized by an enumerated exception, it violates copyright. The lack of an explicit exception even made illegal the act of uploading a photo of artwork on an auction site in connection with its sale.[194] Because this act was not for news reporting, criticism, or research (the enumerated exceptions), it was declared illegal.[195] In 2009, the Diet finally amended the Copyright Act to allow the use of thumbnails of a copyrighted work for an online auction.[196] Acts that Americans take for granted—such as the posting on a blog of a souvenir picture of Disneyland—can also potentially run afoul of Japanese copyright law, even after the 2009 amendment.[197] The enumeration approach has led many to worry that new uses, especially ones made possible by new technologies, might not qualify for the exceptions.[198] As one Japanese academic notes, "[I]f copyright exceptions are interpreted strictly by courts, most daily use might be copyright infringements."[199] Japanese legal scholar Tatsuhiro Ueno portrays the end result of these rules: observing the existence of an American research website collecting cases of musical infringement stretching back over one hundred years, Ueno notes, "[I]f the same exact website were established in Japan, it would constitute an infringement of the right of public transmission."[200] Another Japanese intellectual property scholar concludes, "Without a proper balance [between copyright protection and innovation], any

---

193 *See* supra notes 161–62 and accompanying text.

194 Yeyoung Chang, *Debates on Introduction of "Fair Use" to the Copyright Act of Japan and Korea—Do Japan and Korea Need Fair Use?* 7 (Comparative IP Academic Workshop, Working Paper No. 2, 2009), *available at* http://www.law.washington.edu/Casrip/WWIP/Papers/2009/Debates on Introduction of Fair use to the Copyright Act of Japan and Korea - Do Japan and Korea need Fair use.pdf.

195 *Id*.

196 *Id*.

197 Tatsuhiro Ueno, *Rethinking the Provisions on Limitations of Rights in the Japanese Copyright Act—Toward a Japanese-Style "Fair Use" Clause*, 34 A.I.P.P.I. 159, 179 (2009); Chang, *supra* note 194, at 7.

198 Chang, *supra* note 194, at 5–6 (noting criticism that the enumeration list approach makes it "hard to cover the all new types of use," but preferring a "[b]alancing approach based on human rights" (internal quotation marks omitted)).

199 *Id*. at 7; *see also* Ueno, *supra* note 197, at 161 (noting that exception "provisions have been strictly (narrowly) interpreted").

200 Ueno, *supra* note 197, at 181.

company that wants to introduce new technology services may be too cautious to start its business."[201]

Prime Minister Cameron's concern about whether English law would have permitted Google might have also held true for Japan until 2010. Because of the lack of a broad fair use provision in Japan, the copying required for a search engine to function needed an express exemption from the copyright holder's rights. Lacking such an express exemption, search engines faced the prospect of being illegal, until a 2009 amendment permitted search engines to copy copyrighted works for the purpose of displaying search results.[202] Before this amendment went into effect in 2010, Google's Fumi Yamazaki asked, "Did you know that running a search engine index server in Japan is illegal . . . ?"[203] Yamazaki reports that before the amendment went into effect, "search engines in Japan such as Google and Yahoo inevitably kept their servers outside of Japan."[204]

This was consistent with the damning advice of a programming professor in the wake of the Winny conviction. Shinji Yamane, a researcher at the International University of Japan's Center for Global Communications reported that after Kaneko's conviction, his own students were "concerned about their products potentially violating the law."[205] Yamane continued, "I tell them to release the software overseas."[206]

---

[201] Naoya Isoda, *Copyright Infringement Liability of Placeshifting Services in the United States and Japan*, 7 WASH. J.L. TECH. & ARTS 149, 152 (2011).

[202] Yoshiyuki Tamura, Law Professor and Dir. of Research, Inst. for Info. Law & Policy, Hokkaido Univ., Presentation at the Renmin University International Forum on the Centennial of Chinese Copyright Legislation: Rethinking Copyright Institution for the Digital Age: Japanese Perspective 7 (Oct. 14, 2010), *available at* http://www.ipr2.org/storage/Tamura-EN959.pdf (noting that under the Copyright Law Amendment Act of 2009, "Works may be reproduced where a search site retrieves data from other websites and displays a result of retrieval upon a user's request"); *see also* Teruo Doi, *Availability of the "Fair Use" Defense Under the Copyright Act of Japan: Legislative and Case Law Developments for Better Adapting It to the Digital/Network Environment*, 57 J. COPYRIGHT SOC'Y U.S.A. 631, 632 (2010) (describing the 2009 amendments); *Net-Savvy Copyright Bill Worthy of Quick Passage*, NIKKEI WEEKLY, Apr. 13, 2009 ("The bill would make it possible for search services to collect and analyze information without the permission of copyright holders.").

[203] Fumi Yamazaki, *Updated: Copyright Law Amendment*, WHAT'S HAPPENING IN JAPAN RIGHT NOW? (June 14, 2009, 8:40 PM), http://fumijp.blogspot.com/2009/06/copyright-law-amendment.html.

[204] *Id*.

[205] *Winny Ruling Shocks Industry*, DAILY YOMIURI, Dec. 15, 2006, at 3.

[206] *Id*. (internal quotation mark omitted).

This seems to have been the route followed by the popular Internet bulletin board, 2Channel, founded by Hiroyuki Nishimura in 1999.[207] In 2004, *The New York Times* reported that Nishimura paid $20,000 a month to a company in Palo Alto to host the Japanese language service.[208] While some might suggest that this simple sleight of hand might successfully avoid all the restraints I described earlier, that may not be so clear. In 2009, Nishimura sold the site to a Singaporean company, despite the fact that, according to *Wired*, the site generated 500 million page views per month.[209] His foreign webhost had not prevented a "sea of litigation" against him and judgments amounting to millions of dollars.[210] The legal risk involved in the operation may well have made it difficult for him to raise capital to, for example, take the site global.

C. Privacy

1. European Union

As James Whitman describes, European privacy law is a world away from the American laissez-faire approach.[211] In October 1995, at the same time that the Clinton Administration was declaring its support for industry self-regulation, the European Union was announcing its elaborate and demanding Data Protection Directive.[212] The 1995 Directive requires "unambiguous" consent before the automated processing of personal information.[213] It further requires that information that is gathered must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[214] Rather than a sectoral approach

---

[207] Norimitsu Onishi, *Japanese Find a Forum to Vent Most-Secret Feelings*, N.Y. TIMES, May 9, 2004, at N3.

[208] *Id.*

[209] Lisa Katayama, *Flame Warrior*, WIRED, June 2008, at 110; Alex Martin, *2channel Founder Ponders Next Step After Forum's Sale*, JAPAN TIMES (Jan. 24, 2009), http://info.japantimes.co.jp/text/nn20090124a1.html.

[210] Martin, *supra* note 209.

[211] *See* Whitman, *supra* note 21, at 1155–57.

[212] *See supra* notes 113–14 and accompanying text (discussing the Clinton Administration white paper on privacy). Both the American white paper and the European Directive are dated October 1995.

[213] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 40 [hereinafter Data Protection Directive]. For the implementing legislation within the European Union member states, see *Status of Implementation of Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm (last updated July 16, 2013).

[214] Data Protection Directive, *supra* note 213, at 40.

imposing obligations on certain health care and financial providers, European law offers omnibus protections covering all personal information. Certain categories of information processing—political, health, or sex-related information—are regulated even more tightly.[215] The Directive requires that data controllers secure personal data against accidental or unauthorized disclosure.[216] This Directive posed significant constraints on Web 2.0 enterprises, limiting their information-gathering and -sharing functions.[217]

A 2002 directive, the Privacy and Electronic Communications Directive (the E-Privacy Directive), added even more constraints.[218] The E-Privacy Directive included a broad requirement to ensure the confidentiality of communications, and banned the "surveillance of communications . . . without the consent of the user[]."[219] The Directive required "clear and comprehensive information" before a company could store information such as cookies (used to track web behavior), and required the site to offer the ability to opt out of cookies.[220] Such rules complicated the behavioral monitoring necessary for targeted advertising. They made it difficult to garner the datasets about an individual that might enable companies to know better how to cater to his or her interests (and means). Over the years, the E-Privacy Directive was interpreted and amended in ways that largely confirmed its constraints on tracking and information gathering, thus disabling sophisticated marketing capabilities.[221]

The astonishing reach of the Data Protection Directive can be seen in the case known as *Criminal Proceedings Against Bodil Lindqvist*.[222] Lindqvist was

---

[215] *See, e.g.*, *id.*

[216] *Id.* at 43.

[217] *See, e.g.*, *id.* (requiring member states to implement technical and operational measures to protect the security of personal data).

[218] Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37.

[219] *Id.* at 43.

[220] *Id.* at 44.

[221] *See* Directive 2009/136, of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation No. 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11; *see also* Marie-Andrée Weiss, *Towards Mandatory Data Breach Notification Laws in the European Union*, J. INTERNET L., June 2011, at 24, 24 ("The 2009 Directive has been nicknamed the 'Cookie Directive,' as it requires end-user consent to the storing of cookies on their computers.").

[222] Case C-101/01, Criminal Proceedings Against Bodil Lindqvist, 2003 E.C.R. I-12971.

a Swedish parishioner who published a website to assist fellow churchgoers in their confirmation process.[223] She published personal information about her fellow parishioners on this site without their consent, including the fact that one person had "injured her foot."[224] For this, she was criminally prosecuted under the Swedish law implementing the Data Protection Directive.[225] The European Court of Justice held that Lindqvist had indeed violated European privacy law because she had processed personal information about others (by making it available on the web), without their permission.[226] What would have been readily protected under the First Amendment in the United States was subject to criminal prosecution in Europe.

In another notorious case, Google executives were convicted in Italy of crimes against privacy for not taking down rapidly enough a video ridiculing a disabled child.[227] The executives were convicted specifically of the crime of "illicit treatment of personal data" (*trattamento illecito dei dati*) because "with the purpose of obtaining a gain they participated in the processing of the video [by distributing it through YouTube] containing health data of the disabled teenager without his consent."[228] The February 2010 convictions were overturned on appeal in December 2012,[229] but the convictions demonstrated the ambiguities of a law that might sentence Internet executives for not policing their services sufficiently. This case again demonstrates what James Whitman describes as the "'radically different'" laws on both sides of the Atlantic on the liability of Internet providers for privacy offenses.[230]

---

[223] *Id*. at I-12981.

[224] *Id*. at I-13014.

[225] *Id*. at I-12981.

[226] Jacqueline Lipton suggests that Lindqvist's case is not instructive for information disclosed via social networks because those networks generally make information available only to one's "friends," rather than the public at large. Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 484 (2010) ("[T]he holding was limited to text-based information disclosed to the world at large on a publicly available website."). However, the charge against Lindqvist was not that she *disclosed* information to the public, but rather that she *processed* information about others without their permission. *See Lindqvist*, 2003 E.C.R. at I-13003. Furthermore, Facebook's and Google's social networks give a user the option to share not only with her friends, but also the general public.

[227] *See* Giovanni Sartor & Mario Viola de Azevedo Cunha, *The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*, 18 INT'L J.L. & INFO. TECH. 356, 356 (2010).

[228] *Id*. at 361–62.

[229] Eric J. Lyman, *Italian Court Overturns 2010 Convictions of Google Executives over Bullying Video*, 18 ELECTRONIC COM. & L. REP. 84, 84 (2013).

[230] Whitman, *supra* note 21, at 1200.

2. *South Korea*

South Korean law offers substantial omnibus protections for privacy online. South Korea's 2001 Network Act was modeled in part on the OECD Guidelines, as well as the German Online Service Data Protection Act (*Teledienstedatenschutzgesetz*) of 1997, which was itself passed to implement the 1995 European Data Protection Directive.[231] The Network Act requires data processors to "obtain as little amount of personal data as required for the provision of the services," obtain consent of the data subject for data processing, and safeguard security of the data.[232] Failure to comply can result in fines, imprisonment, or both.[233] In 2011, Korea passed an additional data protection law, the Personal Information Protection Act (PIPA), which, among other things, established a right to file class actions in court over alleged violations of the law.[234] The new law requires privacy assessments by large database developers.[235] Wherever there is an overlap between PIPA and other privacy protections, the stronger provisions will apply.[236]

Korean privacy law is not a paper tiger. The law establishes a standing committee to mediate personal information disputes, with the power to award enforceable awards once mediation is selected.[237] The committee awards compensatory damages "in almost all cases" where a privacy breach is found, with damages typically ranging from U.S. $100 to U.S. $10,000.[238] The Korean authorities receive more than 17,000 complaints per year.[239]

---

231 *See* Chan-Mo Chung, *Experiments with Cyberlaws in Korea*, INTERNET SOC'Y, http://www.isoc.org/inet2000/cdproceedings/8c/8c_3.htm (last visited Jan. 10, 2014).

232 *See id*.

233 DLA PIPER, DATA PROTECTION LAWS OF THE WORLD 305 (2013), *available at* http://www.dlapiper.com/files/Uploads/Documents/IPT_Data_Protection_Handbook_2013.pdf. By contrast, even the United States Children's Online Privacy Protection Act does not include criminal sanctions. *See* 15 U.S.C. §§ 6501–6506 (2012).

234 Hunton & Williams LLP, *South Korea Enacts Comprehensive Privacy Law*, PRIVACY & INFO. SECURITY L. BLOG (Apr. 1, 2011), http://www.huntonprivacyblog.com/2011/04/articles/south-korea-enacts-comprehensive-privacy-law/; *see also* Kwang Hyun Ryoo & Ji Yeon Park, Bae, Kim & Lee LLC, *Further Korean Data Privacy Rules Announced*, LEGAL UPDATE: KOREA, May 31, 2011, at 1, 1, *available at* http://www.bkl.co.kr/kor/_common/filedownload.asp?file=doc\bkl-koreanlawupdate-20110531.pdf.

235 *See* Ryoo & Park, *supra* note 234, at 1, 3.

236 BUSINESS SOFTWARE ALLIANCE, COUNTRY REPORT: KOREA 1 (2012), *available at* http://portal.bsa.org/cloudscorecard2012/assets/pdfs/country_reports/Country_Report_Korea.pdf.

237 *Id*.

238 Graham Greenleaf, *Major Changes in Asia Pacific Data Privacy Laws: 2011 Survey*, at 3 (Univ. of N.S.W. Faculty of Law Research Series, Paper No. 3, 2012), *available at* http://law.bepress.com/cgi/viewcontent.cgi?article=1335&context=unswwps-flrps12.

239 *Id*.

3. Japan

Japan enacted an omnibus privacy statute, the Personal Information Protection Act, in 2003.[240] While explicit consent does not seem to be required before the collection of personal information, businesses cannot obtain personal information from individuals by "fraudulent or other unfair means."[241] The data collector must provide notice of the intended uses of the data.[242] If plans change for the use of the information, "the change must not exceed the scope 'reasonably recognized as having an appropriate connection with the original [p]urpose of [u]se.'"[243] Businesses cannot share personal information with third parties without the consent of the data subject.[244] Businesses also have security obligations with respect to the personal data.[245] Japan does not provide a private cause of action for data privacy violations,[246] and even though consumer centers and the government receive over 12,000 complaints per year, the enforcement record remains unclear.[247]

D. Application: Social Networks

The legal regime has influence in ways that are often difficult to perceive. Consider Facebook's signal feature—its "News Feed," which automatically supplies to your own Facebook page all the activity of your Facebook "friends." Introduced in 2006, the feature met loud protests. Some mocked

---

240 Asim Z. Haque & Mathiew H. Le, Recent Development, *Privacy Year in Review: Canada's Personal Information and Protection and Electronic Documents Act and Japan's Personal Information Protection Act*, 1 I/S: J.L. & POL'Y FOR INFO. SOC'Y 477, 494 (2005).

241 *Summary and Discussion of the New Act*, PRIVACY & AM. BUS., Nov. 2003, at 17, 18 (internal quotation marks omitted).

242 Haque & Le, *supra* note 240, at 501 (citing Personal Information Protection Act, ch. 4, subch. 1, art. 18).

243 *Id*. at 500 (alterations in original) (citing Personal Information Protection Act, ch. 4, subch. 1, art. 15).

244 *Id*. at 502 (citing Personal Information Protection Act, ch. 4, subch. 1, art. 23); *see also* Rudy Guyon, *Outline of Privacy Laws in Japan, Australia, APEC and Selected Other Asian Countries (from a Company Perspective)*, 902 PLI/Pat 481, 491 (2007) ("Specific consent must be obtained before transfer of personal information to a third party . . . . To obtain specific consent, in advance the data gatherer must notify the person providing the personal data of . . . [t]he specific items that will be provided to the third party . . . .").

245 *See* Guyon, *supra* note 244, at 489.

246 Graham Greenleaf, *Country Studies: B.5–Japan*, *in* EUR. COMM'N DIRECTORATE-GENERAL JUSTICE, FREEDOM & SEC., COMPARATIVE STUDY ON DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS 23 (2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B5_japan.pdf.

247 *Id*. at 26; *see also* Greenleaf, *supra* note 238, at 6. Greenleaf writes that, even with limited evidence of enforcement, "it is possible that Japan's legislation is observed by many companies and agencies, simply because it is the law." Greenleaf, *supra* note 238, at 6.

Facebook as "Stalkerbook," and some called for a "cyber-revolt."[248] A student at the University of Illinois, Kiyoshi Martinez, summarized the concern: "Every change I make becomes broadcasted with a bullhorn to everyone—all my friends."[249] Even though the information broadcast through the news feed was technically available to everyone who took the trouble to check out each of their friend's homepages, this changed the valence of activity on Facebook. Individuals who had posted to their webpage, expecting that they were sharing information only with those who would take the trouble to come visit their site, now found that their information was being shared among their friends without their friends' having to leave their own homepages. Many people belonged to school networks, so that any relationship changes were broadcast essentially to the entire student body. Responding to the protests, Facebook offered users the ability to limit the feature somewhat.[250]

Could Facebook have introduced such a feature if it had been a European company? The feature did not pose any real technological hurdle (though Facebook now owns a patent for it[251]). The idea and the willingness to implement it were all that were necessary. The European Data Protection Directive requires an individual's "unambiguous" consent before any automated processing of personal information about that person.[252] Facebook certainly did not ask its users to opt into this feature—it automatically included all of its users in broadcasting their information to their network, unless they opted out of such disclosures. The public protest in the United States at Facebook's chutzpah (as it was then decried, now what many might consider prescience) was not followed by governmental action. Could a European social network have adopted such an innovation?[253] Could Korea's Cyworld social network, launched in 1999, have introduced such a feature without meeting the ire of the Korean authorities? Could Japan's Mixi social network, launched at the same time as Facebook in February 2004, have tested the law with such a move?

---

248 Lauren K. Meade, *A Little Too in Their Face?*, BOS. GLOBE, Oct. 5, 2006, at 1.

249 Janet Kornblum, *Facebook Alters Info Feature That Angered Users*, USA TODAY, Sept. 8, 2006, at 4B (internal quotation marks omitted).

250 Warren St. John, *When Information Becomes T.M.I.*, N.Y. TIMES, Sept. 10, 2006, at 8.

251 *See* U.S. Patent No. 7,669,123 (filed Aug. 11, 2006) (issued Feb. 23, 2010).

252 Data Protection Directive, *supra* note 213, at 40.

253 Consider the letter sent by officials representing twenty-four European states to Google in October 2012 complaining that Google's "[p]rivacy policy suggests the absence of any limit concerning the scope of the [data] collection and the potential uses of the personal data." Letter from Art. 29 Data Prot. Working Party to Larry Page, Google, (Oct. 16, 2012), http://www.dataprotection.ie/documents/press/Letter_from_the_Article_29_Working_Party_to_Google_in_relation_to_its_new_privacy_policy.pdf.

An exception to my general claim (also involving Facebook) demonstrates the rule. When Netflix, the world's most popular Internet movie service, rolled out its integration with Facebook, the world's most popular social network, it offered the service in forty-four of the forty-five countries in which it operated.[254] The missing country? The United States.[255] An obscure, narrow privacy statute proved what Netflix described as an insurmountable block to information sharing between Netflix and Facebook. In 1988, in the wake of the revelations of Supreme Court nominee Robert Bork's video rental records, Congress made it illegal for a video rental service to reveal video rental records of any customer without that customer's *contemporaneous* permission.[256] This Video Privacy Protection Act had an unexpected consequence some two decades later—effectively barring Netflix from sharing the video rental records of one Facebook user with that person's Facebook network unless the first user consented to the sharing for each video (rather than through a blanket prior consent). Congress provided for a private cause of action, with minimum statutory damages of $2,500 for each violation.[257] For a company like Netflix, with some twenty million American subscribers,[258] the fines for ignoring the statute could conceivably entail a judgment in excess of its market capitalization.[259] A relatively obscure and narrow privacy statute had foiled the social networking plans of two enormous multinational corporations (at least until they lobbied to have the law changed[260]). Imagine the consequences of far broader and more demanding privacy laws outside the United States.

***

---

[254] Ronny Kerr, *Spotify, Netflix Snuggle Up to the New Facebook*, VATORNEWS (Sep. 22, 2011), http://vator.tv/news/2011-09-22-spotify-netflix-snuggle-up-to-the-new-facebook.

[255] *Id*. Whether European data privacy rules would foil Facebook–Netflix integration has yet to be tested because Netflix is not currently available in most European countries. *See* Catherine Shu, *Netflix Will Launch in the Netherlands Later This Year as Its International Expansion Slows*, TECHCRUNCH (June 18, 2013), http://techcrunch.com/2013/06/18/netflix-will-launch-in-the-netherlands-later-this-year-as-its-international-expansion-slows/ (explaining that the Netherlands will be Netflix's seventh European country).

[256] 18 U.S.C. § 2710(b)(2)(B) (2006) (permitting disclosure of video rental records "with the informed, written consent of the consumer given at the time the disclosure is sought").

[257] *Id*. § 2710(c). The statute authorizes courts to impose punitive damages and attorneys' fees in addition to statutory damages.

[258] Netflix, Inc., Annual Report (Form 10-K) 24 (Feb. 10, 2012).

[259] *Netflix, Inc. Stock Chart*, YAHOO! FINANCE, http://finance.yahoo.com/q?s=NFLX (last visited Jan. 10, 2014) (reporting daily dynamic stock information for Netflix, specifically including a market capitalization of $19.68 billion as of the close of business on Jan. 10, 2014).

[260] *See* Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, § 2, 125 Stat. 2414 (2013) (amending 18 U.S.C. § 2710(b)(2)) (permitting prior consent for video sharing for a period of up to two years).

But what of Germany's StudiVZ, Japan's Mixi, Spain's Tuenty, and South Korea's Daum and Naver? Should not these services be illegal as well? How can we explain the emergence and persistence of indigenous European Web 2.0 enterprises if the local law is so adverse to their existence? In part, these companies can shelter under the operations of their American counterparts, at least now that the American firms are well established. If local authorities challenge them, those authorities may be implicitly threatening the American colossi. Legal risks may well make it more difficult for them to raise capital to scale up.[261] Perhaps even more importantly, the law hampers their ability to innovate, to offer new services (e.g., a map of their world, a timeline of their life, a tracking of their movements, a seamless link between the individual and corporations with whom she relates). One might note that Facebook and Google have come to increasingly dominate in both Germany and Spain, despite what one might suppose to be the local advantages of StudiVZ and Tuenty.[262]

III. AVOIDING "FROM WOW TO YUCK"

Innovation scholar Vicki Colvin warns about a "wow" to "yuck" trajectory for nanotechnology.[263] Speaking before Congress in 2003, she worried that the early enthusiasm for this new technology would be replaced by popular revulsion in the face of its unintended consequences.[264] Colvin advised, "The good news is that it is not too late to ensure that nanotechnology develops responsibly and with strong public support."[265]

---

[261] *See* Maija Palmer, *A Future Alongside Facebook*, FIN. TIMES, Feb. 25, 2010, at 10. *The Financial Times* offered backhanded support for local alternatives to the American services, observing that "they can be viable little businesses." *Id*. (internal quotation mark omitted).

[262] *See Daten und Fakten*, STUDIVZ, http://www.studivz.net/l/about_us/1/ (last visited Jan. 10, 2014) (providing German language services and programs to 16 million users). StudiVZ lost one million users from 2010 to 2011. *See id*. (last updated Mar. 3, 2011), http://web.archive.org/web/20110303060121/http://www.studivz.net/l/about_us/1 (accessed by searching for the website in the Internet Archive) (noting StudiVZ served seventeen million users in 2010); *see also* FITTKAU & MAAß CONSULTING, W3B REPORT ON FACEBOOK GOOGLE+ & CO.: NUTZER, NUTZUNG, POTENTIALE 8 (2011), *available at* http://www.lebensmittelzeitung.net/studien/pdfs/380_.pdf (reporting that in mid-2011, Facebook had 44.3% of the German market, with the highest local competitor attaining only 9.5%); Palmer, *supra* note 261 (noting that French social network Skyrock "has lost about a third of its audience" to Facebook).

[263] *Hearings*, *supra* note 23, at 49 (statement of Vicki L. Colvin, Executive Director, Center for Biological and Environmental Nanotechnology).

[264] *Id*.

[265] *Id*.

Silicon Valley too has captivated the world, becoming the paragon of a knowledge economy. Its enterprises have utilized the Internet and the World Wide Web to develop history's most powerful and popular platforms for instant communications. These firms improve the productivity of workers and disseminate knowledge across the world. Individuals increasingly learn through tutorials posted on YouTube. Facebook, YouTube, and Twitter played key roles in mobilizing support for those seeking to depose Arab tyrants by allowing citizens to express their grievances, inform each other, and organize together.[266]

At the same time, by becoming the global engines for communication, Silicon Valley enterprises have also become hosts for insults, lies, and hate speech. The enterprises know more about us than other companies, or even most governments, have ever known, holding dossiers that might have impressed the Stasi.[267] Today, companies know what you read,[268] what you search for, who your friends are, what you buy or browse, your politics, and your sexual orientation.[269] Armed with this information, American Internet companies have helped to rat out dissidents in authoritarian states.[270] In the hands of an authoritarian (or even democratic[271]) government, "does the Internet render an entire population prisoner to a national Panopticon?"[272] An example from the brick-and-mortar world hints at the concern: the American retail store Target figured out a teenager was pregnant before her father did, likely based on monitoring of in-store purchases.[273] This clearly falls on the "yuck" side of customer profiling.

The legal historian Morton Horwitz decried what he believed to be the subsidies that the law implicitly offered to industrialists in the nineteenth

---

[266] *See generally* Anupam Chander, *Jasmine Revolutions*, 97 CORNELL L. REV. 1505 (2012) (discussing the role of the Internet in the Arab revolutions).

[267] Anupam Chander, *Facebookistan*, 90 N.C. L. REV. 1807, 1825 (2012) (describing Facebook's dossier on one Austrian student as some 1,200 pages long); Anupam Chander, *Googling Freedom*, 99 CALIF. L. REV. 1, 14 (2011) (describing the tactics of the Stasi).

[268] *See* Alexandra Alter, *Your E-Book Is Reading You*, WALL ST. J., June 29, 2012, at D1.

[269] Heather Kelly, *Facebook 'Likes' Can Reveal Your Secrets, Study Finds*, CNN TECH (Mar. 11, 2013, 12:30 PM), http://www.cnn.com/2013/03/11/tech/social-media/facebook-likes-study/index.html.

[270] *See* Chander, *supra* note 266.

[271] Revelations about domestic spying even in the United States during the course of this writing have proved disturbing. *See, e.g.*, Barton Gellman, *NSA Repeatedly Broke Privacy Rules*, WASH. POST, Aug. 16, 2013, at A1 (detailing oversteps by government agencies in regard to privacy controls since 2008).

[272] Chander, *Googling Freedom*, *supra* note 267, at 10.

[273] Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

century: "forced subsidies to growth coerced from the victims of the process," he charged.[274] Horwitz argued that the "tendency of subsidy through legal change during [the antebellum years] was dramatically to throw the burden of economic development on the weakest and least active elements in the population."[275]

The subsidies offered to Silicon Valley enterprises through legal privileges were not without their costs. Return to the plight of actress Christianne Carafano, subjected to a "cruel and sadistic identity theft."[276] A malicious person using a computer in Berlin posted a false dating profile of her, providing her actual address.[277] Once the website learned of the wrongdoing, it hid the profile and later deleted it.[278] When she sued Metrosplash for permitting such a profile in the first place, her case was thrown out, barred by § 230.[279] Even with a notice-and-takedown regime, as preferred by some critics, Carafano would not have had a case, given that Metrosplash seems to have promptly corrected the falsehood. But § 230 would likely have immunized Metrosplash even if it had left the material up because it did not have a hand in producing it. And chasing the wrongdoer utilizing a computer in Berlin might have proven difficult.

The costs of the privileges provided to Silicon Valley were widely dispersed. The victims included individuals whose privacy was jeopardized and others who were defamed through web services. In Mancur Olson's terms, they (or perhaps we) are a classic "latent group," dispersed and unorganized, and thus at risk of losing in the political process.[280] Yet, the political economy is not entirely so clear. A large, well-organized, and economically powerful constituency—Hollywood—did in fact lobby against Silicon Valley's exemptions. This resulted in a stricter intermediary liability regime for copyright than for tort.[281] The political economy analysis is complicated further by the fact that the results are not consistent across jurisdictions. The

---

274 HORWITZ, *supra* note 17, at xvi.

275 *Id*. at 101.

276 Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1120 (9th Cir. 2003); *see supra* notes 64–68 and accompanying text.

277 *Carafano*, 339 F.3d at 1121.

278 *Id*. at 1122.

279 *Id*. (noting the dispositive question on appeal was whether the suit was properly barred by § 230).

280 MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS 50 (1965) (internal quotation marks omitted).

281 The DMCA's Title II regulated intermediary liability in copyright, the common law regulated intermediary liability in trademark, and § 230 provided immunity for torts.

intermediary liability rules in Europe, South Korea, and Japan proved quite different, as we have seen.

A focus on costs alone would be woefully incomplete. While the costs of Silicon Valley's privileges were widely dispersed, it is important to note that so were their benefits. Most of us have gained from our greater access to knowledge, and from our ability to speak directly to the world and to hear directly from it, and to engage and enlarge our social networks. Imposing strict obligations on intermediaries might well come at the price of both speech and innovation.

Are there ways to minimize the negative consequences of a no-liability, laissez-faire regime for Internet firms yet preserve the "breathing space" that such firms clearly need to innovate?[282] Some have suggested that the notice-and-takedown regime employed for copyright should be extended to defamation.[283] Some law and economics scholars (including Nobel economics laureates Kenneth Arrow and Gary Becker) have suggested that Internet intermediaries can deter copyright infringement "at low cost and without any significant interference with non-infringing uses."[284] Others would suggest that the law tilts too strongly in favor of copyright holders: Pam Samuelson has argued that the DMCA's Title I favored the copyright industries, harming the information technology industries in the process.[285] Many have bemoaned the lack of substantial privacy protections in the United States, arguing that we should "renegotiat[e] [the] Faustian bargain" struck between web users and websites.[286] These are all controversial suggestions, some of which might even pose an existential threat to a free Internet (here I mean free, as in beer).

Should we see these legal privileges as a way to kick-start an infant industry (and thus temporary), or as a response to the fundamentally new

---

[282] *See supra* note 125 and accompanying text (quoting British Prime Minister David Cameron).

[283] *See, e.g.*, Nancy S. Kim, *Web Site Proprietorship and Online Harassment*, 2009 UTAH L. REV. 993, 1023; Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335 (2005); *cf.* Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293 (2011).

[284] Brief of Amici Curiae Kenneth J. Arrow et al. in Support of Petitioners at 9, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (No. 04-480).

[285] Samuelson, *supra* note 95, at 523–24 ("One would have thought, given the Framework's principles and the Administration's enthusiasm for the strong economic performance of the information technology sector, that the Administration would have taken a more balanced position on these issues."); *accord* Anupam Chander, *Exporting DMCA Lockouts*, 54 CLEV. ST. L. REV. 205 (2006).

[286] Zimmer, *supra* note 119; *see also* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1287–94 (1998) (proposing a draft privacy statute).

nature of such enterprises (and thus permanent)? Was a modification to tort law the best way to subsidize the new industry of Internet services? Economists often prefer subsidization through direct transfers, rather than the relatively opaque adjustment of the law.[287] But given the fact that liability exposure might have shuttered the business entirely, only very large direct transfers might have served to counter the legal risks entailed in continuing.[288] Indeed, bringing on new users might have generally proven uneconomical because statutory damages were far in excess of actual damages.

It is possible that the promise of strong privacy-protective legal framework might be attractive to consumers. Viviane Reding, the EU Commissioner responsible for Justice, Fundamental Rights and Citizenship, justified a stronger, unified European privacy regime, in terms starkly resounding in regulatory competition: "The new rules . . . give EU companies an advantage in global competition. . . . [T]hey will be able to assure their customers that valuable personal data will be treated with the necessary care and diligence. Trust . . . will be a key asset for service providers and an incentive for investors . . . locating services."[289] However, thus far there seems to be little migration from American social networks to European or Asian ones, drawn by stronger privacy regimes.

The legal moves described here in the United States have helped facilitate the "wow" of the World Wide Web, but they might also usher in the "yuck." We need to ensure that in our zeal for promoting Internet enterprise, we do not haphazardly create the conditions for a dystopia.

---

[287] Louis Kaplow & Steven Shavell, *Fairness Versus Welfare*, 114 HARV. L. REV. 961 (2001); Anupam Chander & Madhavi Sunder, *Foreword: Is Nozick Kicking Rawls's Ass? Intellectual Property and Social Justice*, 40 U.C. DAVIS L. REV. 563, 575 (2007) (critiquing reliance on taxation to incorporate distributive concerns).

[288] This serves also to suggest a response to the claim that the assignment of the legal privilege will prove irrelevant to the efficient distribution of resources in conditions of negligible transactions costs. *See generally* Ronald H. Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1 (1960) (discussing the collective action problems surrounding transaction costs). Transaction costs here are in fact quite significant, often involving millions of people in highly diverse conditions and across multiple jurisdictions. The task of privately assembling the requisite rights with respect to such a broad array of persons—some of whom would not be on the system at all—seems quite overwhelming.

[289] Viviane Reding, *The European Data Protection Framework for the Twenty-First Century*, 2 INT'L DATA PRIVACY L. 119, 129 (2012).

CONCLUSION: THE HACKER WAY

Mark Zuckerberg calls his approach to innovation the "Hacker Way."[290] "Move fast and break things," he tells Facebook's designers and engineers.[291] But because of Clinton, Congress, and the Courts, most of the time Facebook's amazing innovations did not break the law.

In the same month that Zuckerberg revealed this in the company's IPO prospectus, another major investment was made in a social media enterprise. The Japanese firm Rakuten led a $100 million investment into Pinterest, a website that allows an individual to copy any image across the web to post on one's own scrapbook page.[292] Were it not for safe harbors in the law, Rakuten would likely have been loath to invest in a company whose business model relied on its users' engaging in rampant copyright infringement. Even more important, without such safe harbors, people everywhere would have been denied a simple way to express themselves and to share what they love with the world.

Facebook and Pinterest exemplify the "democratic experimentation" that Lawrence Lessig foresaw in 1995 arising from the new cybertechnologies.[293] While Lessig worried about stultifying regulation of this new medium,[294] over the next half-decade, we saw active intervention by both Congress and the Courts, but largely designed to *limit* the reach of existing law. This made possible the democratic experimentation of companies like Facebook and Google, which introduced innovations subject largely to the approval or disapproval of users rather than the law. A brilliant Japanese entrepreneur during the same period might find the police knocking on the door.[295]

---

[290] Facebook, Inc. Registration Statement, *supra* note 127, at 69 (letter from Mark Zuckerberg).

[291] *Id*. at 70.

[292] Tim Bradshaw, *Rakuten Leads $100m Pinterest Investment*, FIN. TIMES, May 17, 2012, http://www.ft.com/intl/cms/s/0/440374a8-9ffa-11e1-94ba-00144feabdc0.html#axzz2fFRqUnZz.

[293] Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1753 (1995). Jonathan Zittrain labels the extent of the possibilities permitted by the legal and technological architecture "generativity." JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 70 (2008).

[294] Lessig, *supra* note 293, at 1752–53 ("A prudent Court—Supreme Court, that is—would find ways to let these questions simmer for a while, to let the transition into this new space advance, before venturing too boldly into its regulation.").

[295] *See supra* notes 158–67, 186–92 and accompanying text.