
FOREWORD: PAVING THE PATH OF CYBERLAW

Greg Lastowka[†]

HORSES

About sixteen years ago, Judge Frank Easterbrook explained to a group of early cyberlaw scholars that the field should be killed in its cradle.¹ The tendency of cyberlaw scholars to mix legal theory with technologies, he claimed, was little more than an excuse for dilettantism. Let the technologists focus on the technology, he argued, and let the law professors focus on the law's first principles: tort, contract, property, and the like. In Judge Easterbrook's opinion, writing about the law of cyberspace was no different than writing about the law of horses. There is no "law of the horse." The horse is just an animal governed by the laws that governed everything else. A legal focus on technology would not help shape the law, he stated, technology would simply receive the law we made for it.

It turned out Judge Easterbrook was dead wrong—and the starry-eyed cyberlaw visionaries he chided were dead right. This particular horse—the Internet—has indeed shaped the law and shaped it mightily. It has not only shaped the law, but it has shaped society generally. The cyberlaw pioneers addressed by Easterbrook could never have foreseen exactly how law and Internet technology would interact in coming years.² They couldn't even have seen where the technology was headed. In 1996, when Judge Easterbrook told them to do some real work, Steve Jobs had yet to

[†] Professor of Law, Rutgers School of Law—Camden.

1. Frank H Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207; see also Lawrence Lessig, *Law of the Horse: What Cyber Law Might Teach*, 113 HARV. L. REV. 501, 501–03 (1999) (recounting Easterbrook's address).

2. I should note that although the term "cyberlaw" originated in the 1990s, there were certainly a fair numbers of practicing lawyers and professors in the 1960s, 1970s, and 1980s who researched and wrote about the intersection of computers and the law. The popularity of "cyberlaw" as a term largely tracked the expansion of the dot-com boom. Today, many cyberlaw professors (myself included) use a less flashy term for the basic survey course: "Internet and Computer Law."

reclaim the helm of Apple, Google was still a graduate student project at Stanford, and Mark Zuckerberg was not even a teenager. But these legal scholars were onto something: they realized that powerful changes to society, and the law that governed it, were already underway.

It is hard to overstate how much has changed since 1996. Sixteen year olds in America today, born in the year of Easterbrook's address, arrived in a networked world. They grew up *without* my early conviction that all answers to tough questions must be buried in the stacks of distant, dusty libraries. The majority of them carry a gateway to universal knowledge (a.k.a. Google) on an always-handly cell phone. This device also serves to coordinate their universe of friends, tweets, likes, comments, and shares. It also, increasingly, is working on them, monetizing the data and preferences sprinkled through all of their social activity (often without their knowledge).

More than ever, our networked society needs good Internet laws and capable legal guides. It deserves a legal system that not only understands the way our key technologies operate, but has also considered carefully how best to protect those who use them. Legal scholars have a very important role to play in educating courts, practitioners, and society, a role that involves bridging the tricky gaps between legal theory, legal doctrine, and complex emerging technologies and practices. This issue continues the work of earlier cyberlaw scholars by presenting the reader with careful and thoughtful explorations of contemporary legal issues raised by cloud computing, social networks, virtual worlds, internet access rights, digital forensics, and search engines.

The path of cyberlaw is, at heart, about retooling our constantly changing laws for a constantly emerging future. The contributions in this volume work toward that end. They provide the reader with close analysis of a broad range of legal controversies. The work of paving the path of cyberlaw is not an easy task, but the authors in this issue tackle it with admirable skill and success.

Ideally, if we could just glimpse a bit further into the future, we might avoid the sort of mistake that Judge Easterbook made in 1996. Judge Easterbook did not see the future that was on its way. In 2012, neither do we. Surely, in the next sixteen years, some twelve year-old of today will upset the Internet's apple cart. Our digital technologies are not only complex, they are in a perpetual

state of evolution. Code, like law, is made of flexible materials.³ From the current vantage point of 2012, the technological landscape of 2028 is just as obscure as the current technological moment was in 1996. How can we do better, looking toward the future to come?

Perhaps we might look to the past for inspiration. My small digression in this foreword will offer a tweak to Judge Easterbrook's 1996 pronouncement, one that I hope might provide some sense of continuity and tradition to balance cyberlaw's seemingly perpetual novelty. The past sixteen years of cyberlaw do not at all resemble the law of the horse. However, they do bear some resemblance to the law of the car.⁴

CARS

Judge Easterbrook's horse was already an antiquated technology in 1996. Most of us—unless we live in certain spacious states, or are equiphiles, or are parents of equiphiles—gained our knowledge of horses from history, not experience. The law of the car makes a far better foil for considering cyberlaw. The car is, after all, the premier popular technology of the twentieth century and the second most important financial asset of families. More importantly, the car was a technology that permanently stabled our horses and, in doing so, changed the face of the world.⁵

Initially, cars transformed the society by unleashing waves of human carnage. Tens of thousands of people lost their lives each year to automobile accidents in the 1930s, a death toll surpassing any prior class of calamity.⁶ (One might argue that more than half of insurance law today is really just the law of the car.⁷) Cars also changed the physical landscape in short order, giving birth not only to interstate highways but also to myriad new places of commerce and community: diners, motels, suburbs, gas stations, and strip malls. Cars even changed the nature of families,

3. James Grimmelmann, *Regulation by Software*, 114 YALE L.J. 1719 (2004).

4. I should note that other cyberlaw scholars have drawn similar connections between the car and the Internet. See Jay P. Kesan & Rajiv C. Shah, *Shaping Code*, 18 HARV. J.L. & TECH. 319 (2004); Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77 (2003) (describing the expansion of tort law specific to automobiles).

5. Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 WIDENER L.J. 667, 709–714 (2005).

6. RUDI VOLTI, CARS AND CULTURE: THE LIFE STORY OF A TECHNOLOGY (2006).

7. See Rustad & Koenig, *supra* note 5.

providing their owners with greater freedom and mobility in leisure, employment, and domicile.

A law of the car emerged piece by piece. Some of it was created via direct regulation, much like the direct regulations of the Internet we see today. It is due to positive law that we school children in traffic regulations and enforce licensing requirements, design regulations, and emissions controls.⁸ These are all developments of positive law. But much of modern autolaw was formed by judicial interpretation.

Privacy, a key issue in cyberlaw, is just one example: the law has interpreted the car as a sort of semi-private mobile home.⁹ (Today it is exactly that for many, especially those hardest hit by job losses and foreclosures.¹⁰) Accordingly, special laws of privacy had to be built around the car, separating, e.g., expectations of privacy in the trunk space from expectations of privacy on the floor space of the back seat.¹¹ The Supreme Court in 2012 will again be puzzling over cars and privacy, this time with respect to warrantless GPS transmitters.¹² Cyberlaw scholars have confronted similar puzzles regarding search and seizure in a digital world.¹³

The automobile, like cyberspace, also gave birth to various new forms of crime and violence, testing rules of jurisdiction. Individuals with cars could escape local control by fleeing to new geographic frontiers. This sort of freedom was especially alluring to criminals. The “getaway car” played a key role in bank robberies,

8. See Kesan & Shah, *supra* note 5.

9. Carol Sanger, *Girls and the Getaway: Cars, Culture, and the Predicament of Gendered Space*, 144 U. PA. L. REV. 705 (1995).

10. See CBS News, *Hard Times Generation: Families Living in Cars*, 60 MINUTES (Nov. 27, 2011, 8:01 PM), http://www.cbsnews.com/8301-18560_162-57330802/hard-times-generation-families-living-in-cars/.

11. See, e.g., *Wyoming v. Houghton*, 526 U.S. 295, 307 (1999) (“We hold that police officers with probable cause to search a car may inspect passengers’ belongings found in the car that are capable of concealing the object of the search.”); *California v. Acevedo*, 500 U.S. 565, 580 (1991) (“Until today, this Court has drawn a curious line between the search of an automobile that coincidentally turns up a container and the search of a container that coincidentally turns up in an automobile.”); *Chambers v. Maroney*, 399 U.S. 42, 51 (1970) (“[T]he opportunity to search is fleeting since a car is readily movable.”); *Carroll v. United States*, 267 U.S. 132, 153–56 (1925) (observing the jurisdictional fluidity of vehicles).

12. Adam Liptak, *Supreme Court Casts a Wary Eye on Tracking by GPS*, N.Y. TIMES, Nov. 8, 2011, <http://www.nytimes.com/2011/11/09/us/supreme-court-casts-a-wary-eye-on-tracking-by-gps.html>.

13. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

spurring state law enforcement to greater interstate coordination and ultimately requiring the expansion of federal police power. Cybercrime today is pushing governments in similar directions, as rogue online actors operate scams, steal data, and wage information wars from the relative safety of foreign jurisdictions.

But perhaps the most important thing the automobile did to the law was to change the notion of the good life among the populace and our civic leaders. Advertising of automobiles shaped our belief that our cars were not simply instrumental technologies, but desirable possessions as ends in themselves. Car ownership became an important aspect of membership in civil society. Furthering the popular ownership and use of cars became a commonsense goal of public policy. Similarly, today, consumers around the world still covet cars, but they also covet the latest smart phones and Internet gizmos, seeing them as passports to the good life of the twenty-first century. As commentators in this issue note, there is a sense today that today's firms and businesses must have a presence in social software—to ignore the technology is to be left behind.

Our cultural embrace of cars brought us many benefits, but also many problems: an ongoing toll of fatal accidents, the decline of urban centers, an increased national dependence on fossil fuels (and resulting international armed conflicts), and the transformation of our planet's environment. The technology of computers and the Internet has brought us a similar mixed bag: powerful information tools, but significant threats as well—many of which are set forth in this volume. Established understandings of privacy, copyright, evidence, ethics, human rights, and commerce have all been upended by cyberspace.

Comparing the path of cyberlaw to the law of the car should be both troubling and encouraging to cyberlaw scholars. It is troubling insofar as it illustrates how little influence law and government ultimately exerted on the tremendous social impact of automobiles. The law rounded many of the rough edges from the automobile, but society largely stumbled into our current relationship with cars. Market forces played a far greater role than rational deliberation. To the pessimist, the path of autolaw is a story of technology setting government back on its heels. The car transformed the world and for the most part, our legal system was powerless to foresee the vast changes the technology would unleash.

Yet the law of the car is encouraging insofar as it illustrates the potential of legal regulation to succeed in some contexts and for courts to produce just results. If we delve into the law of the car, we can find tales of public servants and legal reformers doing their best to make that technology better in terms of safety, efficiency, infrastructure, and equity, often in the face of powerful opposition.¹⁴ Not all stories concerning the law of the car recount successes, but much good legal work, devoted to the furtherance of the public welfare, was done in the case of the car.

This issue presents the same sort of important work in the field of cyberlaw, a field of considerably greater technological complexity and even more profound cultural implications. The authors lay down scholarly cobblestones for the path of cyberlaw, attempting to provide us with surer footing as we proceed with this momentous new technology.

EIGHT COBBLESTONES

The articles survey their technological fields, harvest the applicable caselaw, condense the issues, and ultimately produce the sort of sound advice that will help courts, practitioners, legislators, and policy makers to move forward. It is my pleasure to introduce them to the reader.

Jon Penney, currently a Graduate Fellow at Oxford University, opens the volume with his article, *Internet Access Rights: A Brief History and Intellectual Origins*. Penney discusses the recent Report filed by the United Nations Special Rapporteur on Freedom of Expression, Frank La Rue, which declares Internet Access to be a human right. Penney's article unpacks that statement's implications and its intellectual pedigree. As Penney explains, the right implies both a negative freedom from government inference as well as a positive entitlement of access to particular tools. As Penney explains, the historical right to the "free flow of information" has given greater weight to negative freedoms, an approach which accords with cyberlibertarian philosophies. However, an exclusive focus on negative freedoms leaves neglected an important part of the political picture of access rights.

14. RALPH NADER, UNSAFE AT ANY SPEED: THE DESIGNED-IN DANGERS OF THE AMERICAN AUTOMOBILE (1965); Jerry L. Mashaw & David L. Harfst, *Regulation and Legal Culture: The Case of Motor Vehicle Safety*, 4 YALE J. ON REG. 257 (1986).

Professor Josh Fairfield's contribution, *Nexus Crystals: Crystallizing Limits on Contractual Control of Virtual Worlds*, takes up the intersection of online contracts and digital copyright in the context of a recent case involving the massively-multiplayer game World of Warcraft. Fairfield sketches out the complicated legal landscape that governs claims of infringement based on the breach of software licenses. He then explains how the Ninth Circuit's recent opinion in *MDY v. Blizzard Entertainment* required copyright owners to establish a copyright "nexus" in order to level infringement claims based on the breach of specific contractual provisions. Fairfield explains how this ruling may, if nourished by subsequent jurists, ameliorate doctrinal imbalances currently plaguing copyright law. As he explains, digital copyright in recent history has been unfortunately interpreted to invite software owners to engage in socially undesirable forms of anti-competitive behavior.

Professor Eric Goldman, in his essay entitled *Revisiting Search Engine Bias*, considers one of the major players in today's cyberlaw landscape, Google, which increasingly is becoming something more than a search engine company. As Goldman explains, Google's domination of the search engine market has fueled increasing scrutiny of potential bias in the results it provides to users. Professor Goldman updates his former critique of search engine bias claims in light of recent changes in the market, changes in Google's business practices, and changes in the political climate. Taking stock of these he concludes that his position has changed very little: he finds no basis in law or policy for more closely regulating how Google displays search results.

Roland Trope and Sarah Jane Hughes are both cyberlaw practitioners and scholars. Their contribution, *Red Skies in the Morning—Professional Ethics Issues at the Dawn of Cloud Computing*, looks at the emerging challenges that cloud computing and Web 2.0 pose to professional ethics. Trope and Hughes first consider the professional obligation of lawyers to stay abreast with current technologies. Then they carefully outline the broad spectrum of risks to clients that is largely inherent to attorney use of cloud computing services. Finally, they offer extensive advice regarding best practices for attorneys who choose to use cloud computing and Web 2.0 technologies.

Katheryn Andresen is a practicing cyberlawyer and the author of *The Law and Business of Computer Software*. Her contribution to

this issue, *Marketing Through Social Networks: Business Considerations—From Brand to Privacy*, documents the commercial expansion of social networks, surveying the legal risks inherent in conducting business via these platforms. As she explains, the law of privacy is an important consideration for any business adopting these technological tools. In particular, those businesses subject to GLBA and HIPPA need to pay careful attention to the information they expose via social networks. Anderson accepts that social networks are now a requirement of doing business with consumers, but advises companies on how they might craft policies to minimize their exposure.

Robert Larson and Paul Godfread are practicing attorneys specializing in the law of intellectual property. Their article, *Bringing John Doe to Court: Procedural Issues in Unmasking Anonymous Internet Defendants*, explores the legal problems facing those wishing to maintain anonymity on the Internet. As they describe, many procedural tools are available for those who wish to pierce anonymity online. Some of these tools abuse legal process to the detriment of anonymous speakers. The authors suggest that both the judiciary and the legislature have failed to confront these sorts of abuses. They offer four suggestions to courts wishing to curb inequitable litigation tactics in this arena.

Sean Harrington is law student and an expert in digital forensics. His contribution, *Collaborating with a Digital Forensics Expert: Ultimate Tag-team or Disastrous Duo?*, explores the fascinating range of legal and procedural questions being presented to courts and practitioners by the incredible volume of information being captured and stored on digital machinery and networks. As Harrington describes, lawyers are being urged to work more closely with technologists, which raises important new legal questions about professional ethics, expertise, privilege, anti-hacking laws, the adversarial process, and third-party obligations. Harrington's article provides a comprehensive tour of the range of issues now facing lawyers collaborating with digital forensic experts.

Adam Pabarcus, a recent graduate of the William Mitchell College of Law, contributes an electronic privacy article: *Are "Private" Spaces on Social Networking Websites Truly Private? The Extension of Intrusion upon Seclusion*. Pabarcus's article closes the issue by reversing Penney's opening article. Instead of the right to communicate, Pabarcus explores the right to be let alone. He does so by applying the common law privacy tort of "intrusion upon

seclusion” to virtual spaces, such as social networks. After surveying the law, theory, and secondary literature on point, Pabarcus concludes that extension of the privacy tort to virtual spaces is warranted. He sees support for this in the language of the Restatement, in the prior case law, and in the goals of public policy.

The contributions to this issue are clear evidence that cyberlaw is not only alive and well, but that it is entering into its full maturity. These scholarly contributions do vital work by endeavoring to legally channel the use of powerful technologies to better serve the public good. This is the path of cyberlaw.