2021

Cyberlaw is Dead and We Will Kill It

Ira Steven Nathenson

bepress™

CYBERLAW WILL DIE AND WE WILL KILL IT

Ira Steven Nathenson[*]

ABSTRACT

Cyberlaw is not Computers and the Law or Intellectual Property on the Internet. It is something far richer and more important. But cyberlaw is also ephemeral, a temporary mode of analyzing technological disruption in real time, until the day when intermediated networks become ubiquitous and cyberlaw will simply become "law." At that time, cyberlaw will disappear, for the same reason that we no longer study "automobile law." But for now, cyberlaw remains an important waystation, a central hub, in the study of emergent and powerful networks. This chapter uses teachings from major philosophers of the 18th, 19th, and 20th centuries—namely Hume, Nietzsche, and Heidegger—to reconcile and build upon the writings of some of today's leading cyberscholars. Synthesizing these teachings, the chapter argues that cyberlaw should be understood as the study of how code, including intermediated networks, fosters disruptive feedback loops between power structures and prescriptive norms. Thus, although cyberlaw will someday merge into the general structure of the law, cyberlaw's lasting legacy will be a methodology for studying the disruptive interplay of prescriptive norms and power structures, and how they create, destroy, and create again.

Table of Contents

INTRODUCTION

In 1982, renowned science fiction author William Gibson coined the word "cyberspace" for a short story, intending it as a cool but "'meaningless' buzzword."[1] Despite Gibson's limited purpose, the word has grown long legs. By the 1990s, "cyberspace" had been adopted to refer to the burgeoning World Wide Web,[2] and later, academics started to use "cyberlaw" as the name of a burgeoning field of study,[3] which, in turn, has led to years of hand-

---

[1] *See* William Gibson, *Burning Chrome*, OMNI, July 1982, at 72, https://archive.org/stream/OMNI197908/OMNI_1982_07#page/n37/mode/2up; Wired Staff, *March 17, 1948: William Gibson, Father of Cyberspace*, WIRED.COM (Mar. 16, 2009), https://www.wired.com/2009/03/march-17-1948-william-gibson-father-of-cyberspace-2/.

[2] Mitchell Kapor & John Perry Barlow, *Across the Electronic Frontier*, ELEC. FRONTIER FOUND. (July 10, 1990), https://www.eff.org/pages/across-electronic-frontier.

[3] Attorney Jonathan Rosenoer applied in 1996 to register the mark CYBERLAW, claiming use as early as April 1992, but the application did not proceed to registration. *See* U.S. Trademark Application Serial No. 75,085,442 (filed Apr. 2, 1996). The earliest reference to "cyberlaw" that I could find in a law journal was an anonymous comment at an academic conference. *See* I. Trotter Hardy, *Electronic Conferences: The Report of an Experiment*, 6 HARV. J.L. & TECH. 213, 232 (1993) ("If cyberspace is a place, wouldn't it

writing over whether or not cyberlaw is even a real thing.

Fast-forward to the Twenty-First century. Is "cyberlaw" still a pertinent concept, one worthy of serious academic study? It is of course undeniable that numerous American law schools offer courses with the titles such as "cyberlaw," "internet law," "technology law," and "information law." Law professors publish casebooks and write voluminously about the legal implications of technology, networks, information, and other topics that would appear to fall under the moniker "cyberlaw."[4]

But not all fields of study last forever. Today, nobody would describe themselves as an "automobile law" scholar, even though 100 years ago, automotive law was an important topic. Thus, will cyberlaw continue to exist, or will we—as the title of this chapter suggests—eventually "kill" it, abandoning the study of cyberlaw due its eventual obsolescence? This chapter suggests that, for the time being, cyberlaw retains importance as a concept by eliciting frameworks for analysing and regulating legal disputes arising from disruptive networked technologies. At the same time, cyberlaw as a discrete field will eventually disappear as intermediated networks become ever more ubiquitous. As the teachings of cyberlaw become increasingly pertinent to broader issues of legal study, cyberlaw will become assimilated into the law in general. Cyberlaw as a discrete field will eventually become irrelevant, but its teachings will be long remembered.

Thus, what is cyberlaw? As a start, one might use the term to mean *the study of the behaviour and regulation of cyberspace*. But that is a useless definition, circular and empty. What we need now is a good theory of cyberlaw. Accordingly, this chapter asks whether it is possible to place cyberlaw on a more secure theoretical foundation. In seeking a better theory of cyberlaw, I use this chapter to borrow (i.e., steal) interesting ideas from

---

have its own law, Cyberlaw?"). Terms such as "computer law" have much earlier lineage. *See, e.g.*, Robert Stephens, *Computer Role Seen as Catalyst in Information Privacy Debate*, GLOBE & MAIL, Mar. 1, 1979, at B2, 1979 WLNR 204062 (referring to a "Computer Law Association").

[4] *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) [hereinafter LESSIG, CODE]; LAWRENCE LESSIG, CODE: VERSION 2.0 (2006) [hereinafter LESSIG, CODE: VERSION 2.0]; *see also* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019) [hereinafter COHEN, BETWEEN TRUTH AND POWER]; JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012) [hereinafter COHEN, CONFIGURING]; JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008).

pre-cyberlaw philosophers of the 18th, 19th , and 20th centuries, none of whom ever said anything directly about cyberspace, and all of whom have much to contribute. In particular, I focus on ideas from David Hume, Martin Heidegger, and Friedrich Nietzsche on topics of normativity, disruption, and power. I use these ideas to build upon some of the major theories put forth by notable cyberlaw scholars, particularly, Lawrence Lessig, Jonathan Zittrain, and Yochai Benkler. The writings of Julie Cohen also bear attention in my attempt to craft a more cohesive theory of cyberlaw.

Properly understood, cyberlaw is not a Law and "fill-in-the-blank" course. Nor is it Computers and the Law, or Intellectual Property on the Internet. Cyberlaw as a field of study is so much broader, interesting, and important. As this chapter suggests, *cyberlaw is the study of how intermediated networks foster disruptive feedback loops between power structures and prescriptive norms.*

Part I addresses the history of all things "cyber," including "cyberspace" and "cyberlaw." It considers the etymology of these terms, along with their treatment by notable scholars. Part II asks whether the ideas of Hume, Heidegger, and Nietzsche might shed light on the law-and-technology problems of the 21st century. Part III combines concepts from the cyberlaw scholars of Part I and the philosophers of Part II to create a new theory of cyberlaw, one that treats human norms and power structures as part of a dynamic feedback system, the contours of which are constantly shaped by the disruptive effects of intermediated networks and their users.

I. THE STORY OF CYBERLAW

This Part explores both milestones and shifting trends in the history of cyberlaw from the perspective of history, language, and legal scholars. It does so with an eye towards laying an opening for the ideas of the philosophers discussed in Part II and the theory proposed in Part III.

A. *History and Etymology*

In 1982, renowned science fiction author William Gibson coined the term "cyberspace" for a story titled *Burning Chrome* published in the now-defunct *Omni* magazine.[5] "I knew every chip in Bobby's simulator by heart; it looked like your workaday Ono-Sendai VII, the 'Cyberspace Seven.'"[6] Gibson later admitted that he created the word as "an 'evocative and essentially

---

[5] *See* Gibson, *supra* note 1; Wired Staff, *supra* note 1.
[6] Gibson, *supra* note 1, at 72.

meaningless' buzzword that could serve as a cipher for all of his cybernetic musings."[7] Put differently, he chose the word because it sounded cool.

In 1990, the term "cyberspace" was repurposed by digital public interest advocates John Perry Barlow and Mitchell Kapor, co-founders of the Electronic Frontier Foundation (EFF), to describe "a frontier region, populated by the few hardy technologists who can tolerate the austerity of its savage computer interfaces, incompatible communications protocols, proprietary barricades, cultural and legal ambiguities, and general lack of useful maps or metaphors."[8] Two short years later in 1992, thereafter, the term "cyberlaw" appeared in print.[9] One year after that, in 1993, the Mosaic web browser was released, leading to the explosion of the World Wide Web and the opening of a new era in digital communications and commerce.[10]

The term "cyberspace" was by no means our destiny. In the early 1960s, MIT researcher J.C.R. Licklider wrote memos in which he described a network "where everyone on the globe is interconnected and can access programs and data at any site from anywhere."[11] An even earlier description of a proto-internet can be found in the post-WWII writings of Vannevar Bush, who described a "memex" that seems eerily similar to today's hyperlinked communications networks.[12] Although Bush was decades ahead of his time in his thinking, the term "memex" never took flight, and by the 1990s, for better or worse, "cyberspace" started to grow very long, if gangly, legs.

What do words like cyberspace and cyberlaw mean? The *Oxford English Dictionary* (*OED*) defines "cyberspace" as "[t]he space of virtual reality; the notional environment within which electronic communication (esp. via the internet) occurs."[13] It further defines "cyberlaw" as "law or a law relating to

---

[7] Wired Staff, *supra* note 1.

[8] *See* Kapor & Barlow, *supra* note 2.

[9] *See supra* note 3.

[10] Michael Calore, *April 22, 1993: Mosaic Browser Lights up Web with Color, Creativity*, WIRED.COM (Apr. 22, 2010), https://www.wired.com/2010/04/0422mosaic-web-browser/ ("NCSA Mosaic 1.0, the first web browser to achieve popularity among the general public, is released. With it, the web as we know it begins to flourish.").

[11] *Internet History of 1960s*, COMPUT. HIST. MUSEUM (last visited Nov. 12, 2020), https://www.computerhistory.org/internethistory/1960s.

[12] *See* Vannevar Bush, *As We May Think*, ATLANTIC, July 1945, at 101, 106, https://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/; *see also* Ira S. Nathenson, *Internet Infoglut and Invisible Ink: Spamdexing Search Engines with Meta Tags*, 12 HARV. J. L. TECH. 43, 56 (1998) (discussing Bush and his memex).

[13] *Cyberspace*, OXFORD ENGLISH DICTIONARY, https://www.oed.com/view/Entry/240849 (last visited Nov. 13, 2020).

Internet and computer offences, esp. fraud, copyright infringement, etc."[14] Interestingly, the related English word "cybernetics," in turn, comes from the ancient Greek word κυβερνήτης, steersman, and κυβερνᾶν, to steer.[15]

It is fascinating that the etymology of "cyberspace"—and by extension, "cyberlaw" —has its roots in steerers and steering, of *movement*. As further explored this chapter, the principal teaching of cyberlaw is of movement: the shifting of norms and power structures, or more specifically, movement as *disruption*, how norms and power structures disrupt one another, whether for better or for worse. That a nascent conception of "cyber" as disruptive movement can be identified in the formative term's linguistic roots, so much the better.

The definition of "cyber" also hints at the transitory nature of cyberlaw. The *OED* illustrates "cyber" with a 1995 quotation that presciently underscores the likely short shelf-life of all things cyber: "Fifty years from now, the online world might seem quite natural; not necessarily technical, cyber or spacey."[16] Cyberlaw as a concept then, is doomed to be ephemeral, a temporary but important topic of study due to the near-constant disruptions caused by the emergence of intermediated technologies such as the internet, the web, social media, and the Internet of Things such as self-driving vehicles.

There is nothing, absolutely nothing exceptional about the emergence of disruptive technologies that eventually become unexceptional threads in a broader social tapestry. Over 100 years ago, the development of gasoline-powered automobile led to an explosion in "automobile law." The new horseless contraptions required re-examination of large swaths of American law such as torts, traffic, insurance, and more, to the emergence of the now-forgotten topic of "automobile law."[17] Someday, we too will forget about cyberlaw, because cyberlaw will simply be . . . law.

B. Early Cyberlaw Theorists

---

[14] *Cyberlaw*, OXFORD ENGLISH DICTIONARY, https://www.oed.com/view/Entry/250879 (last visited Oct. 14, 2020).

[15] *Cybernetics*, OXFORD ENGLISH DICTIONARY, https://www.oed.com/view/Entry/46486 (last visited Oct 20, 2020).

[16] *Cyber*, OXFORD ENGLISH DICTIONARY, https://www.oed.com/view/Entry/250878 (last visited Oct. 20, 2020) (quoting ALTERNATIVE PRESS, May 22, 1995, at 1).

[17] *See* Ira Steven Nathenson, *Best Practices for the Law of the Horse: Teaching Cyberlaw and Illuminating Law Through Online Simulations*, 28 SANTA CLARA COMP. & HIGH TECH. L.J. 657, 736 (2012).

Although he was not a law professor, the late John Perry Barlow reverberates throughout early cyberlaw scholarship. Barlow, a Grateful Dead lyricist who later co-founded the Electronic Frontier Foundation, wrote the famous *Declaration of Independence in Cyberspace*, declaring:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[18]

The *Declaration*, published in 1996, is a paradigm of internet exceptionalism, asserting that governments lack the authority to regulate in cyberspace. Another voice that echoes in cyberlaw scholarship, albeit discordantly, is that of Judge Frank Easterbrook, who rejected the very idea of a cyberlaw. In a passage annoyingly familiar to internet scholars, Easterbrook claimed that cyberlaw was no more useful than a "Law of the Horse."[19] Just like disputes over horses may involve tort law, contract law, property rights, and the like, said Easterbrook, and "[a]ny effort to collect these strands into a course on 'The Law of the Horse' is doomed to be shallow and to miss unifying principles."[20] He argued that law and fill-in-the-blank courses should have "unifying principles,"[21] concluding that cyberlaw may lack such principles, and that those writing about cyberlaw risked "multidisciplinary dilettantism."[22]

C. Later Cyberlaw Theorists

There are plenty of scholars who write about cyberlaw and internet issues, but in this section, I want to focus on three scholars whose work is particularly relevant to this chapter: Lawrence Lessig, Jonathan Zittrain, and Yochai Benkler. A thread that runs throughout is also that of Julie E. Cohen.

1. Lawrence Lessig: Modalities

---

[18] *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

[19] *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208.

[20] *Id.* at 207–08.

[21] *Id.* at 207.

[22] *Id.* One wonders whether Easterbrook's shaming of cyberscholars as dilettantes has turned some of us into turtles with our heads in our shells, lest we be accused of lacking sufficient expertise to speak about other areas that might shed light on our main field of study. Julie E. Cohen has criticised the "near complete isolation" of cyberlaw scholarship from other fields that might shed light. COHEN, CONFIGURING, *supra* note 4, at 26–27.

Of the many responses to Easterbrook, the most significant is Lawrence Lessig's theory of "Code," most famously espoused in *Code and Other Laws of Cyberspace.*[23] As stated by Julie E. Cohen, *Code* "has become the foundational text for theories about the architecture and governance of the networked information society."[24] In *Code*, Lessig argued that cyberlaw shows how law is only one of several regulators of human conduct, and that each regulator, or "modality of regulation," also serves to dynamically regulate human activity: namely, law, as well as social norms, markets, and architecture.[25] In the case of cyberspace, the relevant architecture is one of *code*. Like law, code "embeds certain values or makes certain values impossible."[26] In addition, "[c]hanges in any one [modality of regulation] will affect the regulation of the whole. Some constraints will support others; some may undermine others."[27]

Thus, the various types of regulators work together and affect one another. And on the internet, perhaps the most important of them was code (which could be hardware, software, or both). The importance of Lessig's framework cannot be overstated. Pretty much any theory of internet regulation arising since then is in some way a response to it. One such response is Jonathan Zittrain, to whom we turn next.

2. Jonathan Zittrain: Generativity

Another notable scholar of cyberspace is Jonathan Zittrain, the author of *The Future of the Internet—And How to Stop It*.[28] Whereas Lessig focused on modes of regulation, Zittrain focused on what he dubbed "generativity." As a start, he noted the differences between the old-school Apple II, which had an open architecture that anyone could program for, and the original iPhone, which could only run applications provided by Apple. Whereas the Apple II was a "blank slate" and therefore "*generative*," the iPhone was "preprogrammed" and "*sterile*."[29] Zittrain bemoaned the wide emergence of

---

[23] LESSIG, CODE, *supra* note 4; *see also* LESSIG, CODE: VERSION 2.0, *supra* note 4; Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661 (1998); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 555, 570 (1998) (arguing that "the set of rules for information flows imposed by technology and communication networks form a 'Lex Informatica' that policymakers must understand, consciously recognize, and encourage").

[24] COHEN, CONFIGURING, *supra* note 4, at 13.

[25] LESSIG, CODE, *supra* note 4, 86–90.

[26] *Id.* at 89.

[27] LESSIG, CODE: VERSION 2.0, *supra* note 4, at 123.

[28] ZITTRAIN, *supra* note 4.

[29] *Id.* at 1–2.

sterile technology: "The future is not one of generative PCs attached to a generative network. It is instead one of sterile *appliances* tethered to a network of control."[30]

Zittrain admitted that sometimes a sterile appliance, such as a Swiss Army knife, can be useful, and even safer and easier to use than a generative counterpart.[31] Indeed, it makes sense not to sell multifunction knives that people can easily disassemble and hurt themselves with. Similarly, in terms of today's IoT (Internet of Things) technology, a simple, secure, and non-programmable internet-connected doorbell camera might be better as an appliance. Simplicity and security are paramount. The same might be said of a pacemaker accessible through an external wireless device. You do not want to make it easy for third parties to "generatively" hack your doorbell or pacemaker. Nevertheless, Zittrain seemed to prefer technology that is generative, such as a Windows PC that can run many applications (or better, a Linux computer that itself has an open-source operating system). Such devices are more malleable and far more generative, or put differently, *disruptive*. He defined generativity as "a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences."[32] Zittrain provided factors for discerning the level of a technology's generativity:

> (1) how extensively a system or technology leverages a set of possible tasks; (2) how well it can be adapted to a range of tasks; (3) how easily new contributors can master it; (4) how accessible it is to those ready and able to build on it; and (5) how transferable any changes are to others—including (and perhaps especially) nonexperts.[33]

Each and every one of these factors is about the *disruption* of existing structures, relations, and norms.[34] *Leverage* is about using one system to do many things, to effect change: "the more a system can do, the more capable it is of producing change."[35] *Adaptability* is about repurposing a system to "broaden its range of uses."[36] *Ease of mastery* is about how easy it might be for the technology to be broadly adopted and adapted.[37] The similar-sounding

---

[30] *Id.* at 3.

[31] *Id.* at 73.

[32] *Id.* at 70 (italics removed).

[33] *Id.* at 71.

[34] *Id.* at 74 ("The more that the five qualities are maximized, the easier it is for a system or platform to welcome contributions from outsiders as well as insiders. Maximizing these qualities facilitates the technology's deployment in unanticipated ways.").

[35] *Id.* at 71.

[36] *Id.*

[37] *Id.* at 72.

Accessibility factor is about external factors that ease or restrict access to the technology.[38] Finally, *Transferability* is about the virality of the technology, "how easily changes in the technology can be conveyed to others."[39]

That Zittrain's factors seem to characterize aspects of disruption should be unsurprising. He seemed to generally favour disruption, even equating it with innovation, stating that "a *generative* Internet . . . fosters innovation and disruption."[40] His concern? Sterile technology that leads to an *appliancized* network that is less innovative and more easily regulated.[41] To his credit, Zittrain conceded that not all disruption is good: "Disruption benefits some while others lose, and the power of the generative Internet, available to anyone with a modicum of knowledge and a broadband connection, can be turned to network-destroying ends."[42] Zittrain further recognised that his framework was not by itself capable of addressing all moral issues arising from the spread of generative technologies:

> Generative outputs can also be judged as good or bad by reference to external values. If people use a generative system to produce software that allows its users to copy music and video without the publishers' permissions, those supportive of publishers will rationally see generativity's disruptive potential as bad. When a generative system produces the means to circumvent Internet filtering in authoritarian states, people in favor of citizen empowerment will approve.[43]

Thus, Zittrain serves as the next piece of the puzzle—the puzzle being a broader, unified theory of cyberspace and cyberlaw. Whereas Lessig focuses on the regulators, Zittrain seems to generally favour generative disruption over sterile appliances. But as the next section suggests, there are consequences to the power of successful generative technologies. We turn next to Yochai Benkler.

3. Yochai Benkler: Power

A final major cyberscholar to discuss is Yochai Benkler and his book, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*.[44] The book is careful, thoughtful, and cautiously optimistic. His major premise was that "[i]nformation, knowledge, and culture are central to

---

[38] *Id.* at 72–73.

[39] *Id.* at 73.

[40] *Id.* at 8 (italics in original).

[41] *Id.*

[42] *Id.* at 97.

[43] *Id.* at 80.

[44] BENKLER, *supra* note 4.

human freedom and human development."[45] Benkler argued that "the diversity of ways of organizing information production and use opens a range of possibilities for pursuing the core political values of liberal societies— individual freedom, a more genuinely participatory political system, a critical culture, and social justice."[46] The "networked information environment," he suggested, is "a more attractive cultural production system" because of its transparency and malleability.[47]

Despite his optimism, Benkler acknowledged weighty counterarguments about the power and dangers of intermediated networks. He noted, as had others before him, that information overload and internet centralization might lead to fragmentation of attention and discourse, as well as polarization.[48] With such concerns in mind, Benkler turned a concept important to this chapter, that of "power law," which arose from studies showing that internet users tend to "congregat[e] in a small number of sites."[49] Under power law, *the more powerful a site becomes, the even more powerful it gets.* "[T]he rich get richer."[50] Under power law, just a few sites or networks might become winners because new sites tend to connect to well-known sites, leading an open network to eventually converge into something similar to traditional mass media.[51]

By Benkler's admission, power law "presents a serious theoretical and empirical challenge to the claim that Internet communications . . . . meaningfully decentralize democratic discourse."[52] For example, with Google's search algorithm—where search results might be ranked based on how many oncoming links each site has—"[t]he implication for democracy that comes most immediately to mind is dismal."[53] Benkler's prediction was prescient, considering that *Wealth of Networks* was published in 2006, a mere two years after Facebook's debut, the same year as Twitter's, and a decade before the election of Donald Trump.[54]

---

[45] *Id.* at 1.

[46] *Id.* at 7–8.

[47] *Id.* at 15.

[48] *Id.* at 233–37 (citing CASS R. SUNSTEIN, REPUBLIC.COM (2001)).

[49] *Id.* at 241.

[50] *Id.* at 244.

[51] *Id.* at 242.

[52] *Id.* at 241.

[53] *Id.* at 245.

[54] Since then, Benkler and several co-authors have written about network propaganda, including propaganda leading up to and past the 2016 election. *See* YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN

Like other writers of his era, however, Benkler was optimistic. He somewhat brushed aside the dangers of power law winners by suggesting that even though the winners might take the lion's share of internet views, there would remain a long tail: "clusters of moderately read sites" would have far more users in the aggregate than existed under traditional mass media.[55] Comparing the web to traditional and more limited mass media, Benkler argued that the proper question was "whether the networked public sphere provides broader intake, participatory filtering, and relatively incorruptible platforms for creating public salience."[56] Benkler essentially concluded that even under a power-law regime, smaller sites and more speakers would still be heard, with the internet providing "an effective nonmarket alternative for intake, filtering, and synthesis outside the market-based mass media."[57]

But Benkler's caution was tempered, noting that "things can change," and "supernodes" (such as what Google, Facebook, and Twitter have since become) might emerge, leading to a mass-media model of information exchange that utterly changes the politics of the internet.[58] Benkler nevertheless closed the book with cautious optimism for the "possibility of genuine gains in the very core of liberal commitments, in both advanced economies and around the globe."[59]

As I noted above regarding Zittrain, Benkler's optimism is at best debatable, and I question whether he places too much faith in the power of networks. Indeed, considering that today's big networks are themselves power structures with tremendous potential to disrupt other power structures, it would seem prudent to pay attention to the interrelations and interactions between *norms*, *disruption*, and *power*. With such questions in mind, we now turn to the philosophers.

II. PRE-INTERNET "CYBERLAW PHILOSOPHERS"

In Part II, I explore the contributions that long-departed philosophers might make to 21st century cyberlaw theory. Specifically, I explore David Hume's "is-ought" problem, reminding us of the dangers of conflating the descriptive with the normative, which bears relevance to what may be incompleteness in Lessig's framework. It also addresses Martin Heidegger's

---

AMERICAN POLITICS (2018).

[55] BENKLER, *supra* note 4, at 242–43.

[56] *Id.* at 247.

[57] *Id.* at 260.

[58] *Id.* at 261.

[59] *Id.* at 472.

somewhat obtuse understanding of the relationship between tools and users, which may shed some light on Zittrain's views of disruption. Finally, Friedrich Nietzsche's aphoristic writings on power may be useful in confronting issues of power, overload, and polarisation that Benkler grappled with.

A. David Hume and the Is/Ought of Code

David Hume was known as an empiricist as well as a writer on morals. In some loose ways, then, his philosophy might parallel that of Lessig, a cyberscholar who considered regulation as it was actually experienced by people, whether by legal edict or code-based constraint. Lessig was also concerned with morals, noting that the architecture of the world (and code in particular) affects values, noting that "[i]n cyberspace in particular, but across the Internet in general, code embeds values."[60]

Let's pause for a moment on that phrase: *code embeds values.* Hume would likely agree with Lessig that rules often embed human values, such as fairness, or efficiency, or the like. Hume would also caution that we should be wary of rules that embed values when the justification for those values is missing. This takes us to Hume's famous "Is/Ought problem," also known as "Hume's Law." In Book III of his *Treatise of Human Nature*, Hume argued:

> In every system of morality, which I have hitherto met with, I have always remark'd, that the author proceeds for some time in the ordinary way of reasoning . . . or makes observations concerning human affairs; when of a sudden I am surpriz'd to find, that instead of the usual copulations of propositions, *is*, and *is not*, I meet with no proposition that is not connected with an *ought*, or an *ought not*.[61]

Hume noted that many writers leap from an "is" to an "ought" without justification:

> This change is imperceptible; but is, however, of the last consequence. For as this *ought*, or *ought not*, expresses some new relation or affirmation, 'tis necessary that it shou'd be observ'd and explain'd; and at the same time that a reason should be given, for what seems altogether inconceivable, how this new relation can be a deduction from others, which are entirely different from it.[62]

Philosophers continue to debate the meaning of Hume's distinction.[63]

---

[60] LESSIG, CODE: VERSION 2.0, *supra* note 4, at 114.

[61] DAVID HUME, A TREATISE OF HUMAN NATURE: BOOK III (OF MORALS) 469 (1740) (L.A. Selby-Bigge ed., 1888, revised, P.H. Nidditch 1978) (emphasis in original).

[62] *Id.* (emphasis in original).

[63] Harold Noonan says, "This passage has attracted enormous discussion, but it seems

Arthur C. Danto explained what Hume may mean through this distinction: "[M]ost moral descriptions suddenly move from description to exhortation—from statements about what is the case to injunctions about what we ought to do."[64] Danto further noted that mathematician and philosopher of science Henri Poincaré expanded on Hume's proposition and concluded that "science, capable at best of describing the world, cannot really tell us what we ought to do."[65] Claudia M. Schmidt suggested that "[w]e can at least say that in the is-ought paragraph Hume is criticizing one approach to deriving statements of moral obligation from factual statements, without offering any alternative or indicating whether he intends to provide such an alternative."[66]

For current purposes, I understand Hume's Law to mean that you can't move from the "is" of the existing world to the "ought" of a better world without explaining *why* that world would be preferable to some other alternative, some other articulable world. One can never derive the justification for a moral argument solely based on the facts of the world as it is. Put differently, *one cannot deduce a moral "ought" from a descriptive "is" statement without providing a rationale.*

Understood this way, there is a close affiliation between Hume's Law and legal reasoning. In fact, Hume received early legal training at Edinburgh University, but hated his legal training and abandoned it.[67] Perhaps some of his legal training stuck, though, because Hume's Law seems to be a philosophical way of expressing the shortcomings of poorly reasoned judicial opinions. Even more so, violating Hume's Law parallels the legal sin of judicial *ipsie dixit*, which means "he said it himself." *Ipsie dixit* reasoning is when a judge announces the law without explanation, essentially saying that the law is now going to be what I think it ought to be, because I said so!

Hume's is/ought distinction also sheds light on Lessig's analytic

---

clear that it adds nothing but an eloquent summary to what has gone before." HAROLD NOONAN, HUME 158 (2007).

[64] ARTHUR C. DANTO, CONNECTIONS TO THE WORLD: THE BASIC CONCEPTS OF PHILOSOPHY 65 (1997).

[65] *Id.*

[66] CLAUDIA M. SCHMIDT, DAVID HUME: REASON IN HISTORY 229 (2003). Schmidt notes other interpretations as well, such as (1) that Hume claims that it is impossible to derive an "ought" from an "is"; (2) that Hume claims that it is difficult, but not impossible, to derive an "ought" from an "is"; and (3) that Hume rejects the traditional conception of a moral ought. *Id.* at 228.

[67] NICHOLAS PHILLIPSON, DAVID HUME: THE PHILOSOPHER AS HISTORIAN 5–6 (2012). That makes Hume not unlike many law professors, who too are trained in the law and abandon active practice for more . . . academic pursuits.

framework. Lessig treated his four modalities as being distinct forms of regulation, but at their core, each modality—law, code, markets, and social norms—are simply forms of human *regulation*. Although each regulator differs in its means, each has one thing in common: it *regulates*. Each is a type of *prescriptive norm*, which I define as a simultaneous declaration of how the world *is and how it ought to be.*

Take law, for example. Law is a prescriptive norm. It is part of the world that exists, and it tells you how you ought to behave. Under the law, if you run a red light while speeding without a lawful justification, you have broken the law. We expect laws to be written and made publicly available, along with justifications, such as through legislative reports and reasoned judicial opinions. In such cases, the law is attempting to both provide an explication of the newly existing legal rules (the *is*) as well as the underlying rationale for why the law needed to be changed (the justification for the leap to the *ought*). However, as noted above, sometimes laws are announced *ipsie dixit*, without explanation, such as a court opinion that announces a new rule of law without supplying the justifying rationale.[68] Such unexplained pronouncements violate Hume's Law.

The same observations can be made about code, which can be simultaneously world-building as well as provide a moral prescription of how that world should be. Code takes input and decides—based on the hardware and software configuration—what the output *ought* to be (and, therefore, is). But code is also fraught with the danger of is/ought conflation, even more so than law. Like law, code embeds values. But unlike law, code is far less likely to be shared transparently with the public, or justified in the way that we are accustomed to with law. Hume might find code's lack of justification to be an improper leap from is to ought. Or perhaps he would find it to be a violation of his law, but a backwards leap, an unjustified leap from "ought" to "is." That is because a coder decides how the world ought to be, and then decides to "make it so," as Captain Picard from *Star Trek: The Next Generation* might say. The is and the ought become one.

Thus, code both creates a structure and tells you what you ought to do

---

[68] One dissertation notes ways "oughts" might function in law, such as moral, prescriptive, determinate, and more. *See* Shalina Stilley, Natural Law Theory and The Is-Ought Problem: A Critique of Four Solutions 10 (Aug. 2010) (Ph.D. dissertation, Marquette Univ.), https://epublications.marquette.edu/cgi/viewcontent.cgi?article=1059&context=dissertations_mu (discussing Allan Gewirth, *The "Is-Ought" Problem Resolved*, 47 Proceedings & Addresses Am. Phil. Ass'n 34 (1974)).

with that structure: code is a prescriptive norm that fuses the is with the ought.[69] The rules and algorithms used by code for creating a world (a program, or a protocol, or a game) establish what that world *is* and how one *ought* to act within it. Indeed, a coder is often called a "world-builder" and is the architect of the code and gets, by definition, to make the rules. But unlike law, code is even more fraught with the dangers of is-ought fallacies, because coders typically do not explain why they have made their architectural choices. As Frank Pasquale said in *The Black Box Society*, we often lack knowledge of what is even happening with code, leading to the "black box" problem of a lack of algorithmic accountability.[70] *Code can therefore be the ultimate "ipsie dixit" of prescriptive norms.* Hume, therefore, helps to flesh out Lessig's framework, teaching us that we should parse out the descriptive aspects of code from its normative aspects, paying careful attention to the justifications for the worlds being built through code.[71]

B. Martin Heidegger and Disruptive Feedback

Next, we turn to Martin Heidegger and the light he may shed on Zittrain's disruptive generativity. Heidegger was a 20th-century German phenomenologist. A former student of the Jewish phenomenologist Edmund Husserl, Heidegger succeeded Husserl as Professor of Philosophy at the University of Freiburg in 1928. Several months after Hitler became Chancellor in 1933, Heidegger become rector of the University; a few weeks later, he joined the Nazi Party.[72] Heidegger's Nazi party membership remains

---

[69] "In legal theory, two opposite perceptions of the *is-ought* relationship have emerged: one, the fission of *is* from *ought*; the other, the fusion of *is* and *ought*." S. Prakash Sinha, *The Fission and Fusion of Is-Ought in Legal Philosophy*, 21 VILL. L. REV. 839, 840 (1976). It would appear that my view, in the context of code, is the latter, a fusion of *is* and *ought*, a view ascribed to Lon Fuller and others. *Id.*; *id.* nn. 10–12. Under the fusion view, "the very distinction between is and ought disappears in a certain type of activity." *Id.* at 848. Code is exactly that kind of activity: a world-building *is* with the normative *oughts* embedded in the code. However, just because the *ought* of code may be embedded in its *is* does not eliminate the need for some sort of moral justification. As Lessig notes, code embeds values. If we do not know what values are embedded in code, then we navigate our lives blindly, trusting code to make our choices for us. Indeed, today's broken society is a consequence of blind living navigated by secret code.

[70] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

[71] *Cf.* Stephen G. Salkever, *"Cool Reflexion [sic]" and the Criticism of Values: Is, Ought, and Objectivity in Hume's Social Science*, 74 AM. POL. SCI. REV. 70, 70 (1980) (arguing that Hume's "rejection of value neutrality as a goal of social science is not inconsistent with his rejection on logical grounds of the deduction of *ought* from *is*, of value from fact").

[72] Adam Kirsch, *The Jewish Question: Martin Heidegger*, N.Y. TIMES (May 7, 2010), https://www.nytimes.com/2010/05/09/books/review/Kirsch-t.html.

appalling—he told students in a November 1933 speech that "the Führer and he alone is the present and future German reality and its law"—but "by the time of his 80th birthday, in 1969, Heidegger had largely succeeded in detaching his work and reputation from his Nazism."[73]

Although Heidegger wrote and lectured voluminously, his most famous work is his 1927 masterpiece, *Sein und Zeit*, known in the English-speaking world as *Being and Time*.[74] The book has a somewhat undeserved reputation as being filled with obtuse terminology, but in reality, Heidegger is a poet. His wordplay is awkward and beautiful all at once, which is unsurprising because he constantly pushes the boundaries of what is possible to express with language. Although *Being and Time* does not focus on technology, some of Heidegger's ideas in the book serve as useful tools for reconstructing the concept of cyberlaw.[75]

The major ideas underlying *Being and Time* are about Heidegger's concepts of "Dasein" (or "Being There") and "Befindlichkeit" (or "Being-in-The-World"). In my own reading, these concepts essentially capture the duality of person and world, the idea that one has meaning only by reference to the other. Things are not normally experienced as things in themselves, but as part of a world of meaning. As John Haugeland describes it, to understand a chess piece such as a rook, one must also understand chess, and, in turn, to understand chess as a game that people can play.[76] It's like a version of the "dictionary" game, where no one word has any meaning without reference to other words. They all stand together, and none may be understood in isolation. Thus, humans typically encounter what we might normally call "things" only in a context, and those things only have meaning as part of those contexts, which, in turn, beg understanding of broader contexts, such as the world in which we live, eat, and play games.

---

[73] *Id.* Not all writers agree that Heidegger can be disentangled from his Nazi past. For example, Emmanuel Faye argues that Heidegger's work represents a "deliberate introduction of the foundations of Nazism and Hitlerism into philosophy and its teaching." EMMANUEL FAYE, HEIDEGGER: THE INTRODUCTION OF NAZISM INTO PHILOSOPHY xxv (2009).

[74] MARTIN HEIDEGGER, BEING AND TIME (John Macquarrie & Edward Robinson trans., 1962) [hereinafter HEIDEGGER, BEING AND TIME].

[75] Here, I am using the word "technology" in its normally understood sense and not in the senses that Heidegger later discussed in *The Question Concerning Technology*, where he addressed "the essence of technology[, which was] by no means anything technological." *See* MARTIN HEIDEGGER, THE QUESTION CONCERNING TECHNOLOGY AND OTHER ESSAYS 4 (William Lovitt trans., 1977).

[76] *See* Joseph Rouse, *Heidegger's Philosophy of Science*, *in* A COMPANION TO HEIDEGGER 175 (Hubert L. Dreyfus & Mark A. Wrathall eds., 2005) (citing JOHN HAUGELAND, HAVING THOUGHT: ESSAYS IN THE METAPHYSICS OF MIND (1998)).

Such ideas should be incorporated into cyberlaw theory. Although *Being and Time* doesn't really discuss technology all that much, it nevertheless provides crucial insights to the roles played by networked technology as experienced by humans.[77] The most pertinent portions of the book, vis-à-vis technology, are those portions where Heidegger discusses "Das Zeug," which was translated by Macquarrie & Robinson in 1962 as "equipment."[78] The translators point out, however, that the word Zeug "has no precise English equivalent" and can mean "any implement, instrument, or tool."[79] Heidegger usually uses "Das Zeug" as a collective noun, such as "gear" as in "gear for fishing," or "stuff" as in "there is plenty of stuff lying around."[80] In addition, sometimes he uses the term with an indefinite article to refer to "some specific tool or instrument."[81]

What is "equipment?" Think of equipment or tools for writing, sewing, and the like, the myriad stuff you use to *do* things in the world. Thus, when Heidegger discusses equipment, he is considering how we really conceive of tools. Do we think of them as things? Are we even normally *aware* of equipment *as a thing* when we are using it? According to Heidegger, the answer to both questions is "no." "[E]quipment works best when we needn't think about it at all, and can focus on the task at hand . . . ."[82] We just use it, like a steering wheel or a Bic pen: "the more we seize hold of it and use it, the more primordial does our relationship to it become."[83] Equipment or tools "might refer to as 'situated' or 'embedded' objects."[84] Or as put by Hubert Dreyfus, when we use equipment, "it has a tendency to 'disappear,'" becoming "transparent."[85]

---

[77] With one minor exception, "[t]echnology is not an important theme in *Being and Time*." TOM ROCKMORE, ON HEIDEGGER'S NAZISM AND PHILOSOPHY 208 (1992). Nevertheless, Heidegger's "basic conceptual framework" for a theory of technology can be found in the book's discussion of equipment, as discussed in the text above. *Id.*

[78] *See* HEIDEGGER, BEING AND TIME, *supra* note 74, at 97, 97 n.1. Macquarrie and Robinson also suggest "stuff" as a useful translation. This makes great sense to me, as the meaning of "stuff" always hinges on an understanding of the context in which the "stuff" exists or is used. *See id.*

[79] HEIDEGGER, BEING AND TIME, *supra* note 74, at 97 n.1.

[80] *Id.*

[81] *Id.*

[82] Rouse, *supra* note 76, at 178.

[83] HEIDEGGER, BEING AND TIME, *supra* note 74, at 98; Brian Leiter, *Heidegger and the Theory of Adjudication*, 106 YALE L.J. 253, 265 (1996) (quoting same passage).

[84] Michael J. Madison, *Law as Design: Objects, Concepts, and Digital Things*, 56 CASE W. RES. L. REV. 381, 452 (2005) (citations omitted).

[85] HUBERT L. DREYFUS, BEING-IN-THE-WORLD: A COMMENTARY ON HEIDEGGER'S *BEING AND TIME*, DIVISION 1, at 64–66 (1991).

Heidegger provides his famous example of a hammering with a hammer:

> [W]here something is put to use, our concern subordinates itself to the "in-order-to" which is constitutive for the equipment we are employing at the time; the less we just stare at the hammer-Thing, and the more we seize hold of it and use it, the more primordial does our relationship to it become, and the more unveiledly is it encountered as that which it is—as equipment. . . .[86]

Thus, when a tool (a hammer, a sewing needle) is used as "equipment," we do not grasp it theoretically; instead, the hammer *withdraws* in a sense because "[t]hat with which we concern ourselves primarily is the work."[87] As John Haugeland put it, "what a hammer is *for* is driving in nails."[88]

One might view Heidegger's conception of "Das Zeug" as a form of instrumentalism, but his interpretation is so much richer. A typist who writes with a well-functioning laptop, that person is not aware of the keys. Their laptop becomes a tool, transparent, and the typist is aware only of their work.[89] In more modern terms, such tools allow *flow*: you use the tool without noticing it, like a touch typist and his keys, a race car driver and her paddle shifters, and a tennis player whose racquet is an extension of their arm. *Such stuff becomes a part of you*. For Heidegger, equipment shows how we *experience* things without *contemplating* things *as* things.[90]

Much of our day-to-day experience of the internet can be described in terms of Heideggerian equipment. Such is the case with an internet browser and a stable internet connection. We don't have to understand *how* it works, we only care *that* it works. Such is the case with a computer mouse or smartphone touchscreen. We don't think of them as things. We think of them as extensions of ourselves. As Heidegger says, we use them "in-order-to" do

---

[86] HEIDEGGER, BEING AND TIME, *supra* note 74, at 98.

[87] *Id.* at 99.

[88] *See* John Haugeland, *Dasein's Disclosedness*, 28 S.J. PHIL. 51 (1989), *reprinted in* JOHN HAUGELAND, DASEIN DISCLOSED 24 (Joseph Rouse ed., 2013).

[89] *See* Gavin Byrne, *The Self and Strong Legal Theory: A Heideggerian Alternative to Fish's Scepticism*, 19 CAN. J.L. & JURISPRUDENCE 3, 6 (2006) ("We perceive the things that we come across in terms of how they might be put to practical use.").

[90] Heidegger also discusses the related concept of "signs," which are things that function as both equipment and referent. HEIDEGGER, BEING AND TIME, *supra* note 74, at 114 ("A sign is something ontically ready-to-hand, which functions both as this definite equipment and as something indicative of . . . the ontological structure of readiness-to-hand, of referential totalities, and of worldhood." (emphasis removed)). A stop sign instructs us to do something; a road sign tells where to get off. I will reserve discussion of signs for a future paper but would note that internet tools such as domain names and IP addresses likely serve as Heideggerian signs. This is yet another example of why cyberscholars need to embrace their inner dilletante.

whatever tasks we have at hand.

But sometimes tennis racquets break and race cars stall. Internet browsers crash and computer mice batteries die. Touchscreens become unresponsive. Sometimes equipment *doesn't* work, can't be found, or is missing. In such cases, our workflow stops and we become acutely aware of the equipment or its absence.[91] We need to fix or replace the obstacles to our activities. According to Heidegger, *this* is when we become aware of such items in a second sense—as objects—rather than something to be used. Heidegger gives three examples of ways in which the *ready* can become *un-ready* by being conspicuous, obtrusive, or obstinate.[92]

- A thing is *conspicuous* when it does not work, is damaged, or is unsuitable for the task at hand.[93] An example would be trying to open a door lock that is jammed, or finding a flat-head screwdriver when a Phillips-head screwdriver is needed. In terms of cyberspace, it would be like a browser that crashes or a Mac program that won't run on a Windows PC.
- A thing is *obtrusive* when it is missing, such as realising that your car lacks a spare tire when you have a flat.[94] In cyberspace, a website that is blocked by a DDOS attack would be obtrusive. So would a computer that won't boot when a start-up file is deleted.
- Something is *obstinate* when it is not unusable or missing but instead "'stands in the way'" and disturbs us, such as when you buy a new sweater at a store and the clerk forgets to remove the anti-theft device.[95] In cyberspace, think of pop-ups that block your view, or spam that gets in the way of wading through the 1000-plus emails sitting in your inbox.

As hinted through the examples above, concepts of working and non-working equipment may be of great value in crafting a new theory of cyberlaw.[96] Although cyberlaw is ostensibly about law and disruptive

---

[91] In the case of a broken smartphone or simply a drained phone battery, our world may come to a temporary and crashing end.

[92] HEIDEGGER, BEING AND TIME, *supra* note 74, at 102–07. Dreyfus prefers the terms "malfunction" (rather than conspicuousness), "total breakdown" (for obtrusiveness), and "temporary breakdown" (for obstinacy). DREYFUS, *supra* note 85, at 70–83.

[93] HEIDEGGER, BEING AND TIME, *supra* note 74, at 102, 104 n.1; DREYFUS, *supra* note 85, at 70–83; *see also* WILLIAM BLATTNER, HEIDEGGER'S *BEING AND TIME* 57–59 (2006).

[94] HEIDEGGER, BEING AND TIME, *supra* note 74, at 103, 104 n.1.

[95] *Id.* at 103–104, 104 n.1.

[96] Along analogous lines, Brian Fitzgerald uses Heidegger's concepts to "break with the traditional definition of software as a program of directions to a computer system and to posit

network technology, Heidegger's teachings on equipment remind us that Code is something that we generally use without thinking about it.[97] Thus, cyberspace—when functioning—is an invisible tool for the user. As Julie Cohen argues, lawmaking works best when it "attend[s] to the ordinary, everyday ways [that people] experience their culture," and when lawmakers "consider the ways in which networked information technologies reshape everyday experience."[98] Heidegger's phenomenological approach is tailormade for considering how people actually use and experience networked technologies.

And just as cyberspace is often invisible and working, it is often, to some, either broken or breaking things. For them, cyberspace is often *disruptive.* Heideggerian disruptions are everywhere in cyberspace, including spam, cybersquatting, hacking, DDOS attacks, viruses, and much more. Cyberspace is thus both a place in which we work,[99] as well as a source of significant frustration. From the early years of the digital era through today, scholars, pundits, legislators, and the public remain engrossed in cyberspace issues *because* cyberspace is so very often *broken* or *breaking things* in a Heideggerian sense.

But broken to *whom*? An additional observation should be made. Heidegger's discussion of equipment focuses on how equipment can be either useful or disruptive to a particular *user* of that equipment. But cyberspace teaches us that the concepts of utility and disruption can sometimes be two sides of the same coin: a tool that is seamless and useful to one person can be highly disruptive to another. A radar detector might help a driver get away with speeding, but it prevents the police from enforcing the law. In cyberspace, a P2P network allows seamless transfers of copyrighted files but may wreak havoc on record and movie industries. So, in cyberspace, Heideggerian tools can *both* allow flow and disruption. One person's *flow* is another person's *frustration*. Code can act as both feature and flaw,

---

software as a form of discourse, something that allows things to be seen or appreciated." Brian F. Fitzgerald, *Software as Discourse: The Power of Intellectual Property in Digital Architecture*, 18 CARDOZO ARTS & ENT. L.J. 337, 346 (2000).

[97] Orin Kerr's description of the "internal perspective" of internet users rings similarly; he says, "The internal perspective adopts the point of view of a user who is logged on to the Internet and chooses to accept the virtual world of cyberspace as a legitimate construct." Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 359 (2003).

[98] COHEN, CONFIGURING, *supra* note 4, at 6.

[99] Especially during the 2020 COVID-19 pandemic, when I and so many other academics taught classes from home using Zoom, a form of Heideggerian equipment that tends to malfunction (i.e., become conspicuous) at inopportune times.

depending on the worlds enabled or frustrated by that very code.

Thus, Heidegger's teachings about working and broken equipment may shed fresh light on Zittrain's concept of generativity, a concept that Zittrain generally views as a social good that fosters innovation. But whether a generative technology is good or bad depends on whose work is being enabled or disrupted. Some generative technology may be particularly disruptive to third parties even when the code works flawlessly. A musician who cannot pay the heating bill because their music is downloaded freely via P2P does not want to hear "but P2P is generative!"

Mark Zuckerberg may have said, "Move fast and break things."[100] But in the real world, generative disruption can lead to real winners and losers. Using the label "innovation" for disruption—or worse, the even more annoying moniker "*creative* disruption"—presumes that all disruption is "good." But we should always ask, "Good for *whom*?" The effects of disruption may be felt by the vested interests of existing power structures and, in turn, might lead to new power structures that compete with or even replace them. Such disruption can topple one industry (newspaper reporting and newspaper advertising) in favour of another (Facebook algorithmic aggregation and online advertising). At the largest scales, disruptions can be affirmatively destructive to those vested in the world-as-it-was (as was the case for the United States prior to 2016 Russian election interference). Indeed, the entire field of cybersecurity seems to be rooted in anticipating and preventing disruptions that lead to Heideggerian failures of equipment.

In short, a theory of cyberlaw needs to tie together Lessigian normativity (as viewed through Hume) as well as Zittrainian disruption (as illuminated by Heidegger). But these are only two parts of the cyberlaw puzzle. We also need to consider what it is that *causes* disruption and what is *caused by* disruption. What "it" is, is oftentimes *power*. We therefore turn to Friedrich Nietzsche.

C. *Friedrich Nietzsche and Power*

Finally, we turn to Friedrich Nietzsche and how his view of power may shed light on cyberlaw and on Benkler's discussion of power theory. Nietzsche, born in 1844, was a nineteenth-century philosopher whose

---

[100] The full quote is "Move fast and break things. Unless you are breaking stuff, you are not moving fast enough." Zoë Henry, *Mark Zuckerberg's 10 Best Quotes Ever*, INC. (Oct. 14, 2014), https://www.inc.com/zoe-henry/mark-zuckerberg-move-fast-and-break-things.html.

aphoristic and often cryptic writings were later popular with the Nazis, but Nietzsche was not antisemitic, and in more recent years, contemporary philosophers have largely rescued Nietzsche's reputation as a creative and important thinker.[101] Nietzsche's writings include many provocative ideas, such as "God is dead,"[102] the Übermensch,[103] and the eternal recurrence,[104] but few concepts are more central to his thinking than the *Wille zur Macht*, or the "Will to Power." This concept appears in a number of his writings,[105] including a posthumous collection of unpublished notes assembled for publication by his undeniably antisemitic sister Elisabeth.[106]

It is difficult to discern how seriously we should take the concept of Will to Power. As Alexander Nehamas pointed out, the Will to Power might be read "at best" as a "horrible theory" of ruthlessness and, "at worst," a "no less horrible" and implausible picture of "unending struggle" to increase power and "to suppress everything else by any conceivable means."[107] Such readings are of little use except a movie villain who twirls his waxed moustache while explaining their nefarious plot to the hero.

But I believe there is something to be found in Nietzsche's writings that bears relevance to cyberlaw. In selecting relevant passages and ideas, I recognise that a writer as elegant, elusive, and aphoristic as Nietzsche practically screams out for others to cherry-pick his ideas to suit nearly any purpose (as his antisemitic sister and the Nazis surely did). Having said that,

---

[101] WALTER KAUFMANN, NIETZSCHE: PHILOSOPHER, PSYCHOLOGIST, ANTICHRIST 42 (4th ed. 1974); *see also id.* at 45–46 (noting writings and correspondence where Nietzsche expressed his disgust for antisemitism).

[102] *See* FRIEDRICH NIETZSCHE, THUS SPOKE ZARATHUSTRA 41 (R.J Hollingdale trans., 1961) [hereinafter NIETZSCHE, ZARATHUSTRA]; FRIEDRICH NIETZSCHE, THE GAY SCIENCE: WITH A PRELUDE IN RHYMES AND AN APPENDIX OF SONGS ¶ 108, at 167 (Walter Kaufmann trans., 1974) [hereinafter NIETZSCHE, THE GAY SCIENCE].

[103] *See* NIETZSCHE, ZARATHUSTRA, *supra* note 102, at 41; NIETZSCHE, THE GAY SCIENCE, *supra* note 102, ¶ 143, at 191–92.

[104] *See* NIETZSCHE, THE GAY SCIENCE, *supra* note 102, ¶ 341, at 273–74.

[105] *See, e.g.*, FRIEDRICH NIETZSCHE, THE WILL TO POWER (Walter Kaufmann ed., Walter Kaufmann & R.J. Hollingdale trans., 1967); FRIEDRICH NIETZSCHE, BEYOND GOOD AND EVIL: PRELUDE TO A PHILOSOPHY OF THE FUTURE, ¶ 13, at 21 (Walter Kaufmann trans., 1966) [hereinafter NIETZSCHE, BEYOND GOOD AND EVIL].

[106] NIETZSCHE, THE WILL TO POWER, *supra* note 105. Arthur C. Danto writes that although Elisabeth has been subject to criticism for using "Will to Power" as the title of this posthumous compilation of aphorisms, it was not without justification considering that Nietzsche was planning on using that title for a future book, and "his most creative thinking" in later years was devoted to the concept. ARTHUR C. DANTO, NIETZSCHE AS PHILOSOPHER: AN ORIGINAL STUDY 214 (1965). Danto described Nietzsche's Will to Power as "the key to his own thought and to the way things are." *Id.* at 214–15.

[107] ALEXANDER NEHAMAS, NIETZSCHE: LIFE AS LITERATURE 75 (1985).

I am confident that there are parallels between Nietzsche's ideas about the Will to Power, and themes regarding power that run through cyberlaw.

In *Beyond Good and Evil*, Nietzsche said, "A living thing seeks above all to *discharge* its strength—life itself is *will to power*; self-preservation is only one of the indirect and most frequent *results*."[108] Then, what *is* the Will to Power? The German word he used is "Macht," which does mean "power," but is also the noun form of the verb "machen," which means "to make" or "to do." So, it may be that Macht here means something broader than mere power. In some senses, perhaps the "Will to Do" is an equally apt translation.

Interestingly, Nietzsche seemed to equate the Will to Power with creation, lawmaking, and more: a "genuine philosopher" has a task: genuine philosophy "demands that he *create values*."[109]

> *Genuine philosophers . . . are commanders and legislators:* They say "*thus* it *shall* be!" They first determine the Whither and For What of man, and in so doing have at their disposal the preliminary labor of all philosophical laborers, all of whom have overcome the past. With a creative hand they reach for the future, and all that is and has been becomes a means for them, an instrument, a hammer. Their "knowing" is *creating*, their creating is a legislation, their will to truth is—*will to power*.[110]

Nietzsche seemed to equate genuine philosophy with issuing commands and making laws. To my lawyer/professor eyes, that looks an awful like the job of a legislature or a judge. Also, it sounds like *ipsie dixit* lawmaking.

Additionally, consider the Will to Power in the context of cyberspace. As Danto said, the Will to Power "is the teaching that the world is something we have made, and must remake, and it has no structure and no meaning other than what we can impose on it."[111] Nietzsche's genuine philosophers, therefore, create and issue *prescriptive norms*. They tell others what the world *ought* to be, and what the world therefore *is*. This concept of prescriptive world-building aptly fits the job of a Coder. Code-builders are world-builders. Networks are the essence of things that both have "effects on other things" while also being the "sum of their effects."[112] When we build

---

[108] NIETZSCHE, BEYOND GOOD AND EVIL, *supra* note 105, ¶ 13, at 21 (emphasis in original).

[109] *Id.* ¶ 211, at 136.

[110] *Id.*

[111] DANTO, *supra* note 106, at 227–28.

[112] *Cf.* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479 (1998).

networks, we build worlds. Coding is an expression of the Will to Power.

Nietzsche's writings on the Will to Power describe—almost painfully well—the willingness of Alpha Coders such as Mark Zuckerberg to push boundaries. Nietzsche said in *The Gay Science*: "It will be the strong and domineering natures that enjoy their finest gaiety in such constraint and perfection *under a law of their own . . . .* Even when they have to build palaces and design gardens *they demur at giving nature freedom*."[113] Even more directly, in *The Will to Power*, Nietzsche seemed to reject any need to justify a leap from "is" to "ought," saying, "To transform the belief 'it *is* thus and thus' into the will 'it *shall become* thus and thus.'"[114]

Such aphorisms sound like they could have been uttered by a Gilded Era steampunk baron. In more recent times, Zuckerberg infamously said, "Move fast and break things."[115] Nietzsche would likely be sympathetic, saying that the "means by which a stronger species maintains itself" include "grant[ing] oneself the right to exceptional actions; as an experiment in self-overcoming and freedom."[116] Put differently, the rules don't apply to the powerful. Instead, the powerful are *exceptional*, and they *make* the rules: "the stronger becomes master of the weaker, in so far as the latter cannot assert its degree of independence—here there is no mercy, no forbearance, even less a respect for 'laws.'"[117] This suggests that Alpha Coders need have no respect for rules other than those made by the Coders themselves.[118]

These Nietzschean ideas—power, exceptionalism, and rule-making—fit so very well with the internet, except today we call these concepts "intermediary power," "internet exceptionalism," and "Coder as world-builder." Such thinking dates back to the earliest days of the internet when

---

[113] NIETZSCHE, THE GAY SCIENCE, *supra* note 102, ¶ 290, at 232 (emphasis added).

[114] NIETZSCHE, THE WILL TO POWER, *supra* note 105, ¶ 593, at 324 (emphasis in original).

[115] Henry, *supra* note 100.

[116] NIETZSCHE, THE WILL TO POWER, *supra* note 105, ¶ 921, at 487 (emphasis removed).

[117] *Id.* ¶ 630, at 336; *see also* GUSTAVE LE BON, THE CROWD: A STUDY OF THE POPULAR MIND (1895); AMY CHUA, POLITICAL TRIBES: GROUP INSTINCT AND THE FATE OF NATIONS (2018).

[118] Other aphorisms even seem to anticipate the role that "fake news" might play in an information ecosystem run by social networks. "[R]everence for truth is already the consequence of an illusion—and that one should value more than truth the force that forms, simplifies, shapes, invents. 'Everything is false! Everything is permitted!'" NIETZSCHE, THE WILL TO POWER, *supra* note 105, ¶ 602, at 326. "There are no facts, everything is in flux, incomprehensible, elusive; what is relatively most enduring is—our opinions." *Id.* ¶ 604, at 327. "On a yet higher level is to *posit a goal* and mold facts according to it; that is, active interpretation and not merely conceptual translation." *Id.* ¶ 605, at 327.

Barlow declared the "independence" of the internet from the tyranny of governmental oversight. The users of the internet, declared Barlow, they would make the rules! Early internet-related laws such as CDA 230 and the takedown provisions of the DMCA also permitted unfettered development and private ordering.[119] Nietzsche similarly said, "The highest men live beyond the rulers, freed from all bonds; and in the rulers they have their instruments."[120]

But at what point do networks become so strong that they become threats to existing power structures, whether businesses, whole industries, or even governments? Even today, governments can topple due to the power of a large network.[121] Might a network *itself* become so powerful—even if not self-aware (yet) in an AI sense—that the network nevertheless has the functional equivalent of a Will to Power? A Will to *Network* Power? Modern networks such as Twitter and Facebook are complex organisms that can behave in chaotic and unpredictable ways: fostering disruption, toppling existing power structures, and creating new repositories of power. Perhaps a sufficiently complex network is capable of exercising its own Will to Power, regardless of the contrary or even benevolent intentions of its Coders.

These questions of unbridled network power, these are question that I want to explore here and in future writings. Recall Benkler's discussion of power laws in Part I.C.3. The more powerful a site or network gets, the even more powerful it gets; as Benkler said, "the rich get richer."[122] Consider the outsized that role social networks played in the Arab Spring and in the 2016 Presidential election. As Julie Cohen says: "Legal institutions . . . offer multiple points of entry for economic and political power, and as they are enlisted to help produce the profound economic and sociotechnical transformations that we see all around us, they too are being changed. . . . Slowly but surely, that process is restructuring the legal system itself."[123]

---

[119] *See* 17 U.S.C. § 512(c) (2018) (notice and takedown provisions of the Copyright Act); 47 U.S.C. § 230(c)(1) (2018) (immunity for interactive service providers).

[120] NIETZSCHE, THE WILL TO POWER, *supra* note 105, ¶ 998, at 519.

[121] *See* Paul Mozur, *A Genocide Incited on Facebook, With Posts From Myanmar's Military*, N.Y. TIMES (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html; Bani Sapra, *The Last Decade Showed How Social Media Could Topple Governments and Make Social Change—And It's Only Getting Crazier From Here*, BUS. INSIDER (Jan. 14, 2020), https://www.businessinsider.com/social-media-activism-facebook-twitter-youtube-power-2019-12.

[122] *See* BENKLER, *supra* note 4, at 244.

[123] COHEN, BETWEEN TRUTH AND POWER, *supra* note 4, at 2.

Today's Facebook and Twitter represent Benkler's power law run amok.

Indeed, the concept of Will to Power aptly captures the life journey of some online networks and services as they make the shift from small and new to large and powerful. Nietzsche spoke of three people: the oppressed, the "stronger," and the "strongest." The first wants freedom, the second desires to overpower others, but lacking that, wants justice. The third, which he also described as "the richest, most independent, [and] most courageous," seeks the "love of mankind" but also views others as objects to overpower.[124] The third category also ably captures the problems of today's "super-intermediaries" that treat its users *as* the product, who monetise their data, and who turn their services into addictive attention-grabbers, without sufficient regard to whether those services foster tribalism, autocratic behaviour, and violence.

The problem of power that Nietzsche described and Benkler explored has only become more pressing in recent years. In 2013, former Google CEO Eric Schmidt co-authored a book on digital policy.[125] Consciously or subconsciously, "power" was a theme that ran heavily through the book, with the word "power" and variants appearing 142 times; in contrast, "human rights" and the like appeared less than five times.[126] When asked what Google's former (and unofficial) slogan—*Don't Be Evil*—means, Schmidt once replied that evil "is what [Google co-founder Sergey Brin] says is evil."[127] It is hard to imagine any statement that is more Nietzschean, or more troubling, when coming from leaders at one of the world's most powerful corporations. It is no surprise that antitrust law may soon become as important in this "New Gilded Age" as it did a century ago.[128]

In short, a more complete theory of cyberlaw needs to account for the roles played by powerful intermediaries, as well and how such intermediaries used their emergent power to disrupt existing norms and power structures.

III. A DISRUPTIVE FEEDBACK THEORY OF CYBERLAW

Much of today's study of cyberlaw seems to have splintered into silos,

---

[124] NIETZSCHE, THE WILL TO POWER, *supra* note 105, ¶ 776, at 407 (emphasis removed).

[125] *See* ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS (2013).

[126] *See* Ira Steven Nathenson, *Super-Intermediaries, Code, Human Rights*, 8 INTERCULTURAL HUM. RTS. L. REV. 19 (2013).

[127] Josh McHugh, *Google vs. Evil*, WIRED (Jan. 1, 2003), https://www.wired.com/2003/01/google-10/.

[128] TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE (2018).

such as intellectual property, intermediary immunities, privacy, cybercrime, and cybersecurity. This is a natural trend in a maturing field of academic study. New issues arise, and further regulations and decisions are aimed at those issues. Fresh scholars enter the fray to critique solutions and criticise others. A once-broad discipline—cyberlaw or internet law or whatever you want to call it—slowly becomes a taxonomy of related topics, with scholars writing increasingly detailed pieces in their subspecialties. Eventually some parts splinter off and others fade away. This is the natural course of a maturing field of study.

But some have sought to reframe and refocus the inquiry in hopes of articulating a cohesive theory of cyberlaw. For example, Jacqueline Lipton argued for reframing cyberlaw "as a law of intermediated information exchange," focusing on intermediaries to better "clarif[y] the legal issues raised by online interactions."[129] Sharon Sandeen and David Levine created the first casebook dedicated to "information law."[130] The last Part contributes to such efforts by tying together the ideas of the cyberscholars and the philosophers discussed in this chapter to create a unified theory of cyberlaw.

A. *Three Cyberscholars and an Elephant*

Each of the cyberscholars makes important contributions. Lessig is right to note the role played by regulators, particularly code. Zittrain is right to note the disruptive effects of generativity. And Benkler's observations about power theory have become even more important in the years since he made them. But in reading them, I am reminded of the ancient Hindu parable about blind persons examining an elephant:

> One person touches the elephant's tail and says the elephant is like rope. Another touches its trunk and says it is like a snake. Another touches the elephant's leg and says the elephant is like a tree. Yet another touches the elephant's side and says it is like a wall. They are all experiencing the same elephant but in very different ways.[131]

I do not mean to say these scholars are unaware of the contributions voiced by the others. They are. But I do think that each scholar's core thesis represents only part of a broader theory of cyberlaw. For example, although Lessig makes important observations by distinguishing the four modalities of

---

[129] Jacqueline D. Lipton, *Law of the Intermediated Information Exchange*, 64 FLA. L. REV. 1337, 1343 (2012).
[130] SHARON SANDEEN & DAVID LEVINE, INFORMATION LAW, GOVERNANCE, AND CYBERSECURITY (2019).
[131] CHAD MEISTER, PHILOSOPHY OF RELIGION 11–12 (2014).

regulation, distinguishing them may obfuscate their important similarities. The lines between each regulator are sometimes quite blurry.[132] As Julie Cohen notes, "To the extent that [Lessig's framework] offers the vectors of law, code, market, and norms as ontologically distinct tools capable of deployment by disinterested, autonomous regulators, the *Code* framework lends itself to precisely this sort of oversimplification."[133]

Indeed, the similarities between Lessig's modalities are as important as their differences, if not more so. Even though there are distinctions to be made between law and code (or markets and social norms), each is at its core a type of prescriptive norm. A norm, of course, is a "directive," something that "tells people more than what they must do, under pain of compulsion; it tells them in a sense what they also 'ought' to do."[134] Law is just one kind of prescriptive norm. Code regulates through algorithms embedded in hardware and software. Social norms regulate through the power of group cohesion. And markets regulate through economic forces.

But "modalities of regulation" do not regulate from above like Greek gods. They only have power to constrain when used by *power structures*, such as governments (with their ability to use violence to enforce the law), social groups (social structures that have the tribal ability to enforce social norms through shaming and shunning), economies (which their power to reward and punish market actors), and of course, networks (which use a combination of hardware- and software-based code to create a world and enforce its rules). Each of Lessig's regulators is, in sum, part of a *power structure* with *enforcement mechanisms*. My critique of Lessig is thus twofold. First, he conflates the regulators when all are variations on a theme. Second, we need to pay as much, or more, attention to the power structures wielding the regulators. Lessig risks losing sight of the power structures that create prescriptive norms, benefit from those norms, and are sometimes destroyed by such norms.[135]

---

[132] Pricing structures and market activity are shaped by laws such as securities laws. Internet architecture is oftentimes a reaction to legal guidelines such as the Communications Decency Act and the Digital Millennium Copyright Act.

[133] COHEN, CONFIGURING, *supra* note 4, at 156. Indeed, laws oftentimes codify social norms (think of "not committing murder" as both law and social norm) and oftentimes make sense only in the context of market forces (such as the interplay between antitrust law and market competition). Law itself is a form of "code," albeit one that operates in realspace rather than digitally. At best then, the types of regulators are at best a loose taxonomy, with substantial overlap and fuzzy boundaries.

[134] GEORGE C. CHRISTIE, LAW, NORMS AND AUTHORITY 2 (1982).

[135] "The credo that 'code is law' recognizes that Internet technologies encode an

Zittrain makes a similar elephant-observing move by his seeming overoptimism in the disruptive nature of generative internet technologies. Although he admits that increased generative disruption is not by itself always good, his writing seems to side strongly in favour of disruptive generativity. But it seems to me that any theory of cyberlaw cannot focus just on disruption but must also consider what *causes* the disruption and what *is caused by* the disruption. Heidegger tells us that when something in the world disrupts, others notice. They also react. Disruption does not occur in a vacuum, and there are winners and losers. Some of those winners are new power structures with new prescriptive norms, and some of the losers are former power structures with their prescriptive norms ignored or tossed to the side.

That is where Benkler and Nietzsche come in. Benkler reminds us of the role that power plays in the growth of internet networks. Nietzsche argues that humans (and perhaps their institutions or even their code) trend towards the grasping of increased power. Benkler may be too quick to minimize concerns over polluted information ecosystems caused by information overload, echo chambers, and fragmentation, as raised by other writers such as Cass Sunstein.[136] A more comprehensive theory of cyberspace therefore needs to pay attention not just to disruption and forms of prescriptive norm regulation, but also to the power structures that rise and fall as part of the power law model of network growth.

Tying it together, Lessig's *Code* is an exercise in prescriptive world-building that can cause Zittrainian disruption, effecting changes not just to other Lessigian regulators but also to Benklerian power structures themselves. Old power structures are wiped out (think the music industry and newspapers), and new ones emerge (think Spotify and Facebook). Indeed, coding can be an exercise in naked rule-making and world-building. Coding determines both how the world ought to be and how the world is. These acts are far more than a possibly unjustified moral leap. *They are a raw assertion of power*. Put differently, the Alpha Coder has combined the Humean Is and Ought, disrupted the Heideggerian tools used by others, and established and

---

especially powerful and peculiarly invisible form of behavioral discipline, but it does not acknowledge that these technologies also form the material substrate within which complex social patterns take root." COHEN, CONFIGURING, *supra* note 4, at 27.

[136] Regarding the 2016 elections, Benkler argues that it would be "naïve" to place too much weight on internet polarization, which "understates the degree to which institutions, culture, and politics shape technological adoption and diffusion patterns." BENKLER ET AL., *supra* note 54, at 8.

even supplanted Nietzschean power structures.

B. *Cyberlaw Lives: A Theory of Disruptive Feedback*

Let's match the three cyberscholars up with their respective philosopher counterparts. Consider Table X.1.

Table X.1: Cyberscholars and Philosophers

CYBERSCHOLAR	PHILOSOPHER
Lessig's modalities of regulation	Hume's Is/Ought problem
Zittrain's generativity	Heideggerian disruption
Benkler's power laws	Nietzsche's Will to Power

Hume argued that it is improper, perhaps impossible, to derive a moral prescription, an "ought," from a description of the state of the world, an "is." Yet, Lessig teaches us that each of us are regulated by law, social norms, market forces, and code. What is striking about Lessig's regulators is that each combines ought and is, making each a prescriptive norm about how humans should behave, while also creating an existential space in which we all live. Sometimes Lessigian regulators do not commit the sin of unjustified leaps from is to ought, such as when Congressional laws are supported by hearings and reports, or well-reasoned judicial opinions show why their edicts are well supported by sound policy and existing precedent. But just as legal pronouncements may be *ipsie dixit*, so too can code hide in a black box, neither understood nor justified.

Zittrain argued that generativity was usually a positive thing and generally preferable to sterile appliances. Yet, Heidegger teaches us that tools, such as computers and networks, have the potential to enable the seamless conduct of some human activities in a way that interrupts or prevents other activities. In more modern terms, Heidegger's nascent view of technology is that it can either allow "flow" or be "disruptive." Or depending on one's perspective, it can allow both. Thus, P2P file-sharing programs that allow smooth exchange of files have also decimated the music industry, forcing incredible changes to other prescriptive regulators, namely social norms (because copying became routine for young people) and market forces (because the record industry was decimated, and later supplanted by iTunes and Spotify).

Benkler put his faith in a broadening of speech made possible by networked technologies, even while admitting that power law allows most of

the spoils to go to the bigger networks, which in turn may become bigger and bigger. Nietzsche teaches us that the powerful see themselves as exceptions to the rules because the powerful are the rule-makers. Thus, Benkler, as viewed through Nietzsche, takes us full circle, all the way back to John Perry Barlow's *Declaration of Independence of Cyberspace*. Filled with techno-utopianism, Barlow declared, "We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different."[137]

Cyberspace provides an ongoing 25-plus year case study in how prescriptive norms, disruption, and power structures intertwine to shape and reshape society. Consider Table X.2.

Table X.2: The Feedback Bubble

PRESCRIPTIVE NORMS	*Disruption and Feedback loops Between Norms and Power Structures*	POWER STRUCTURES
Code		Networks
Law		The State
Social norms		Social groups
Markets		Economic actors

Table X.2 takes the teachings of the six thinkers and reworks them into a broader theory of cyberlaw. Tying together the scholars and philosophers, I suggest that *cyberlaw should be understood as the study of how intermediated networks foster disruptive feedback loops between power structures and prescriptive norms*. The theory is Lessigian in its pedigree but fleshes out the dynamic and structural components. Put differently, Lessig focuses too much on just the four regulators. But the four regulators are all different types of prescriptive norms.[138] As Zittrain and Heidegger point out, we also need to closely construe the mechanisms by which one regulator disrupts or reinforces another. Such disruption could be *negative feedback*, by which the force of a law (copyright) is lessened by code (P2P networks). Such disruption could also be *positive feedback*, by which code (automated

---

[137] Barlow, *supra* note 18.

[138] As Robert M. Cover famously said, "principles of justice, the formal institutions of the law, and the conventions of a social order are, indeed, important . . . ; they are, however, but a small part of the normative universe that ought to claim our attention." Robert M. Cover, *Foreword: Nomos and Narrative*, 97 HARV. L. REV. 4, 4 (1983). Law is the most important prescriptive norm for lawyers because it is our *raison d' être*, our bread and butter. But law is just one tool for building a world.

copyright enforcement) might increase the regulatory power of another regulator (copyright law).[139]

Lessig does point out that one regulator may reinforce or undercut another, but focusing on how one regulator affects another provides an incomplete view of the "elephant," of the dynamics of cyberspace. When P2P undercuts the enforceability of copyright law, it also affects the *power structures* that benefitted from such laws. When code undercuts copyright, that in turn affects economic actors such as record industries. It also affects the legitimacy of the State, when the legitimacy of courts is called into question for permitting suits against private non-commercial file sharers.[140]

Thus, although Lessig's modalities remain a foundational part of any theory of cyberlaw, they are only part of the picture. I think that the study of cyberlaw extends beyond just the fact of regulation and should include study of the nature of disruption and how such disruption affects power structures. This view of cyberlaw would be relevant to any area of cyberlaw that I can think of. Examples abound:

- Intellectual property: how do changes in networks affect the scope of copyright law? How do changes in copyright law affect the development of networks?
- Data privacy: would the GDPR have passed in Europe if the big social networks had been based there? How can the power of American networks be tamed in order to obtain better protections privacy protections in the United States?
- Algorithmic accountability: does "black box" code cause businesses and governments to demand less accountability, undercutting democratic norms?
- Information overload: have search engines and social networks, which were created in part to manage information overload, exacerbated the problem to the benefit of those networks, along with encouraging autocrats and hostile foreign actors?

---

[139] *See* Ira S. Nathenson, *Civil Procedures for a World of Shared and User-Generated Content*, 48 U. LOUISVILLE L. REV. 911, 919 (2012) (arguing that extrajudicial IP enforcement procedures can led to de facto IP rights that exceed the scope of de jure IP rights).

[140] *See, e.g.*, J.R. Raphael, *Has the RIAA's Fight Against File Sharing Gone Too Far?*, TECHHIVE (June 19, 2009, 2:48 PM), https://www.techhive.com/article/167058/Riaa_file_sharing.html (noting that "almost everyone inside [the courtroom] uttered an audible gasp" when a file-sharer was held liable for "$2 million for downloading 24 songs").

- CDA 230 reform: has CDA immunity created a toxic infosphere of fake news and echo chambers that is decimating democratic norms and splintering society into tribal sub-groups? If so, is the fix in code, law, or some other mix? Or is code itself the problem?
- Freedom of expression: are traditional First Amendment principles consistent with an information ecosystem polluted with propaganda, echo chambers, and information overload?
- Surveillance and biometrics: can economic actors and the State be trusted to wield biometrics and other surveillance technologies? How has social behaviour changed in response to such technologies, and how might future technologies affect society?
- Artificial intelligence: can de facto personhood be created through code, and if so, what implications does that have for legal personhood and State citizenship? Would it change the very idea of the "State?"
- Intermediary power: If powerful networks have State-like power, should they be subject to State-like obligations and limitations as well? Does the very concept of "State" need to be revisited?

As the listing above suggests, Lessig got it right but only in part. It is true, as Lessig argues, that a change in code can change law, social norms, and markets. But such changes can affect broader power structures as well, such as by undercutting (or emboldening) governments, social groups, or market participants. These changes to power structures can loop back, changing the norms themselves. This is essentially Lessig's framework with some notable additions intended to turn his regulatory framework into a more dynamic system that addresses the effects of cyberspace on society and vice-versa.

C. And Cyberlaw Will Die

Cyberlaw will die. My theory, though focused on cyberspace, is not cyberspace-dependent. Instead, it is simply a dynamic theory of change, looking to the disruption and feedback—whether positive or negative—that occurs between types of regulation and the power structures that use those types of regulation. Lessig's theory is not really cyberspace-dependent but is instead *applicable* to cyberspace. The same is true of my extension of his and others' thinking. This is nothing more than a theory of how disruptions interact with existing norms and power structures, causing upheaval and change. Major new technologies tend to do that. The creation of automobiles created new problems and exacerbated old ones. New laws had to be written. Old power structures (the horse industry) were affected and new ones (the auto industry, roadbuilders, the oil industry, and more) arose in their ashes.

Similar upheavals took place with the development of electric grids, and railroads before that, and the printing press prior to that. Each of these disruptive technologies led to changes in society, as does cyberspace today.

Eventually, the upheavals caused by cyberspace will ebb as intermediated networks become more ubiquitous. By then, the problems of cyberspace, and its lessons, will be broadly felt and spread throughout power structures and various modalities of regulation. What had once been "cyberlaw" will become subsumed into other areas of law and will eventually become invisible, forgotten as the once-discrete area of law it initially was. At that point, cyberlaw will simply be . . . law. Eventually, something new—perhaps AI, perhaps bioengineering—will be the next great disruption, at which point the teachings of cyberspace—and hopefully, this theory of disruption—will become useful once again.

CONCLUSION

Judge Easterbrook suggested that cyberlaw was simply a "law of the horse," lacking in unifying principles that could illuminate the entire law. He was wrong. With the right theory, cyberlaw is not only capable of illuminating the law, but also of showing us in real time how law—and the world—is made and broken and made anew.