Law for the Platform Economy

Julie E. Cohen[*]

This Article explores patterns of legal-institutional change in the emerging, platform-driven economy. Its starting premise is that the platform is not simply a new business model, a new social technology, or a new infrastructural formation (although it is also all of those things). Rather, it is the core organizational form of the emerging informational economy. Platforms do not enter or expand markets; they replace (and rematerialize) them. The article argues that legal institutions, including both entitlements and regulatory institutions, have systematically facilitated the platform economy's emergence. It first describes the evolution of the platform as a mode of economic (re)organization and introduces the ways that platforms restructure both economic exchange and patterns of information flow more generally. It then explores some of the ways that actions and interventions by and on behalf of platform businesses are reshaping the landscape of legal entitlements and obligations. Finally, it describes challenges that platform-based intermediation of the information environment has posed for existing regulatory institutions and traces some of the emerging institutional responses.

TABLE OF CONTENTS

 Mark Claster Mamolen Professor of Law and Technology, Georgetown Law. My thanks to Anupam Chander, Deven Desai, Kristen Eichensehr, Christoph Graber, Margot Kaminski, Paul Ohm, Rebecca Tushnet, Kevin Werbach, and participants in the UC Davis Law Review Symposium on Future-Proofing Law for their helpful comments, and to Jade Coppieters and Natalie Gideon for research assistance.

Platforms are big news and big business — and, some would say, the focus of overblown and unwarranted hype. Books by business scholars and tech-economy pundits tout the efficiency and generativity of platform-based business models, even though new platform ventures often struggle to turn profits after moving out of the startup phase. Tech journalists, activists, and scholars in a variety of academic fields argue that platforms are reshaping seemingly every area of human endeavor, from innovation to commerce to cultural production to social organization, but disagree on how to assess platforms' effects.

This Article takes claims about the transformativeness of platforms seriously and considers their implications for law. Its starting premise is that the platform is not simply a new business model, a new social technology, or a new infrastructural formation (although it is also all of those things). Rather, it is the core organizational form of the emerging informational economy.

In the book in progress from which this Article is adapted, I frame the emergence of informational capitalism in terms of three large-scale developments that parallel those identified by political economist Karl Polanyi as framing the emergence of industrial capitalism.[1] Polanyi mapped a "great transformation" in the system of political economy that involved appropriation of newly important resources but that also moved on conceptual and organizational levels. The basic factors of industrial production — land, labor, and money — were reconceptualized as commodities, while at the same time patterns of barter and exchange became detached from local communities and reembedded in the constructed mechanism of the market.[2] Three analogous shifts frame the transformation that is now underway: the propertization of intangible resources, the concurrent dematerialization and datafication of the basic factors of industrial production, and the embedding of patterns of barter and exchange within information platforms. Organizationally speaking, the platform is key: platforms do not enter or expand markets; they replace (and rematerialize) them.

[1] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTION OF INFORMATIONAL CAPITALISM (forthcoming). For a concise definition of informational capitalism, see MANUEL CASTELLS, THE INFORMATION AGE: THE RISE OF THE NETWORK SOCIETY 14-18 (1996). For helpful discussions of various manifestations of the shift from industrialism to informationalism as the dominant mode of economic development, see generally DANIEL BELL, THE COMING OF POST-INDUSTRIAL SOCIETY: A VENTURE IN SOCIAL FORECASTING (1973); JAMES R. BENIGER, THE CONTROL REVOLUTION: TECHNOLOGICAL AND ECONOMIC ORIGINS OF THE INFORMATION SOCIETY (1986); DAN SCHILLER, HOW TO THINK ABOUT INFORMATION 3-35 (2007).

[2] *See* KARL POLANYI, THE GREAT TRANSFORMATION: THE POLITICAL AND ECONOMIC ORIGINS OF OUR TIME 33-76 (Beacon Press 2d ed. 2001) (1944).

And platforms, unlike the fictional "market," have taken shape as discrete legal entities, with their own aims and agendas.

The role of law in this story is foundational but largely unremarked. Legal scholars who work on information policy have been intensely concerned with questions about how existing doctrinal and regulatory frameworks should apply to information, databases, technical protocols, and online behavior, perhaps undergoing some changes in coverage or emphasis along the way. For the most part, they have not asked the broader, reflexive questions about how core legal institutions *are already evolving* in response to the ongoing transformation in our political economy — questions, in other words, not about how law should apply to disputes over information, but rather about how disputes over information are reshaping the enterprise of law at the institutional level. That is a mistake. Law for the platform economy is already being written — not via discrete, purposive changes, but rather via the ordinary, uncoordinated but self-interested efforts of information-economy participants and the lawyers and lobbyists they employ.

Part I describes the evolution of the platform as a mode of economic (re)organization and introduces the ways that platforms restructure both economic exchange and patterns of information flow more generally. Part II explores some of the ways that actions and interventions by and on behalf of platform businesses are reshaping the landscape of legal entitlements and obligations. Part III describes challenges that platform-based intermediation of the information environment has posed for existing regulatory institutions and traces some of the emerging institutional responses. Part IV concludes and suggests some lessons for the project of "future-proofing law."

I. FROM MARKETS TO PLATFORMS

In the industrial-era economy, the locus for activities of barter and exchange was the market, an idealized site of encounter between buyers and sellers within which the characteristics, quantities, and prices of goods and services were regulated autonomically by the laws of supply and demand. In the emerging informational economy, the locus for those activities is the platform, a site of encounter where interactions are materially and algorithmically intermediated. Platforms — including online marketplaces, desktop and mobile computing environments, social networks, virtual labor exchanges, payment systems, trading systems, and many, many more — have become the sites of ever-increasing amounts of economic activity and also of ever-increasing amounts of social and cultural activity. The

emergence of platform-based business models has reshaped work, finance, information transmission, entertainment, social interaction, and consumption of goods and services, and has destabilized the locally embedded systems that previously mediated those activities in many different types of communities. Legal and economic constructs based on the idea of "markets" — whether in goods and services or in speech and ideas — have yet to adapt in response.

A. Prologue: Access and Legibility

No form of economic or social organization is ever wholly new. Preexisting modes of organization impose their own logics, and path-dependencies matter. It is important to begin by recognizing two important ways in which platforms represent continuity. The intertwined functions that platforms provide — intermediation that provides would-be counterparties with *access* to one another and techniques for rendering users *legible* to those seeking to market goods and services to them — have important antecedents in twentieth-century direct marketing and advertising practices.

To understand the pre-history of platforms, it is useful to consider two early precursors: the Sears, Roebuck catalog and the Nielsen ratings system. Over two decades at the turn of the twentieth century, entrepreneurs Richard Sears and Alvah Curtis Roebuck parlayed a mail-order watch and jewelry business into a wildly successful mail-order empire selling everything from jewelry to farm equipment. Inclusion of a product in the Sears, Roebuck catalog gave its manufacturer access to a marketing juggernaut with the ability to reach consumers nationwide, the range to offer concert grant pianos and engraved shotguns, and the power to undercut the prices charged by local "five-and-ten-cent stores" for everyday essentials.[3] Three decades later, Arthur Nielsen, a pioneer in the field of statistical market research, began to develop a system designed to give subscribing advertisers and their clients a different kind of access to consumers, based on aggregate measurements rather than solely on one-way communication. The system originated as a simple "audimeter" that recorded when household radios were on and the stations to which they were tuned; over time, the company expanded to television and developed techniques for correlating the recorded information with demographic information and individual viewing information collected from participating households via paper

[3] *See* BORIS EMMET & JOHN E. JUECK, CATALOGUES AND COUNTERS: A HISTORY OF SEARS, ROEBUCK AND COMPANY 59-99, 100-13 (1950).

"diaries."[4] In this manner, it gradually began to develop more granular profiles of the viewing population.

Both the Sears, Roebuck catalog and the Nielsen ratings system provided access to vast pools of consumers, but the ways they provided access and the relationships they envisioned between and among manufacturers, intermediaries, and consumers were different. To use Dan Bouk's periodization, the catalog represents the era of the ideal customer as social imaginary. Sears, Roebuck & Co. lacked and likely could not imagine collecting precise, granular information about customer desires and resources, so it sold products it envisioned customers as wanting.[5] To the extent that measurements factored into those determinations, they did so as proxies for the ideal customer rather than as empirical representations of any particular customer. The Nielsen system represents the era of the mass audience, constructed on the basis of numerical aggregates that purported to represent the audience itself.[6] The era of the mass audience also represents a critical inflection point, in which the legibility rubric supplied by an intermediary became both an object of regularized economic exchange and an increasingly powerful, institutionalized arbiter of the knowledge upon which market participants relied. Legibility here connotes more than simple visibility; legibility rubrics incorporate both implicit epistemologies and associated action strategies. Like other such rubrics — for example, the charts and tables on which modern administrators rely to govern populations or the nodes and landmarks on which city dwellers rely to create cognitive maps of their surroundings[7] — the Nielsen ratings did not simply represent the mass audience but also encoded both a way of understanding it and strategies for managing it.

Platforms echo some aspects of these early precursors, but also rework the basic themes of access and legibility in ways that neither

---

[4] *See* HUGH MALCOLM BEVILLE, JR., AUDIENCE RATINGS: RADIO, TELEVISION, CABLE 34-38, 70-75 (2d rev. ed. 1988); JOSEPH TUROW, BREAKING UP AMERICA: ADVERTISERS AND THE NEW MEDIA WORLD 24-32 (1997).

[5] *See* EMMET & JUECK, *supra* note 3, at 39-40; Dan Bouk, *The History and Political Economy of Personal Data over the Last Two Centuries in Three Acts*, 32 OSIRIS (forthcoming 2017) (manuscript at 11-13) (on file with author).

[6] *See* Bouk, *supra* note 5, at 12-16. On television ratings as a technology of power, see generally IEN ANG, DESPERATELY SEEKING THE AUDIENCE 53-57 (1991).

[7] For foundational explications of the ways that legibility rubrics both assist and distort understanding in the contexts of state administration and urban planning, see generally KEVIN LYNCH, THE IMAGE OF THE CITY (1960); JAMES SCOTT, SEEING LIKE A STATE: HOW CERTAIN SCHEMES FOR IMPROVING THE HUMAN CONDITION HAVE FAILED (1998).

Richard Sears nor Arthur Nielsen could have envisioned. Selection of one's product for inclusion in the Sears, Roebuck catalog might have offered a ticket to marketplace success, but it was not essential for economic survival in an era in which much commerce remained local. Many manufacturers, moreover, refused the opportunity because of the production quantities demanded or because they feared that local retailers who opposed the spread of mail-order businesses would boycott their wares.[8] Access to basic communications infrastructures — the postal system and print advertising distributed via newspapers and magazines — was becoming more nearly essential for survival, but the relevant infrastructures were available to (almost) anyone willing and able to pay the required fees. As the relevant infrastructures — now digital and networked — have become platforms, both the conditions of access and the need for access have changed. Access to the facilities offered by Amazon or Google or Visa/Mastercard or the iOS operating system, for example, requires assent to complex sets of legal and technical protocols. And access to platforms — whether online marketplaces or search engines or payment systems or computing environments — is increasingly essential to reaching any customers at all.

The story of legibility is more complicated still. In the late 1980s, proprietary infrastructures for radio and television broadcast began to give way to a far more complex ecosystem that included proprietary infrastructures for cable television and Internet access and open protocols for Internet publishing. The proliferation of cable channels and home video recording technologies initially caused an existential crisis for advertisers, whose aggregate measures of the mass audience and its tastes began to dissolve into seemingly unmanageable fragments.[9] That fragmentation, however, also lent momentum to practices of targeted marketing that had originated earlier in the twentieth century, and that were premised on the importance of reaching specialized pools of desirable consumers.[10] New technologies for networked digital communication were emerging, and efforts to adapt those technologies for commercial exploitation ultimately produced new, highly granular ways of measuring audiences and predicting audience appeal.[11]

---

[8] *See* EMMET & JUECK, *supra* note 3, at 117-19, 150-68.

[9] *See* ANG, *supra* note 6, at 68-77.

[10] *See* TUROW, *supra* note 4, at 27-36.

[11] *See* Bouk, *supra* note 5, at 17-20.

At the same time, and reflecting the increasing normative force of legibility as an overarching frame for commercial endeavor, the legibility function began to burrow into the core of the infrastructure itself. The emergence of the commercial Internet, with its enormous number and variety of information sources, accelerated the centripetal movement. A world with a vast diversity of information sources required intermediation for those sources to be meaningfully accessible, and legibility became the essential function for an intermediary to provide to advertisers seeking access to users.

B. How Platforms Shape Information Flow, part 1: The Datafication of Everyday Life

Reorganization around intermediation and legibility has engendered profound structural changes in the architecture of contemporary networked communication. Platforms emerged at a point of fortuitous technological convergence: new techniques for customer tracking, immersive social design, and data analysis all promised new possibilities for profiting from targeted marketing in an increasingly fragmented media ecosystem. As legibility became a service most effectively and profitably provided at the infrastructural level, however, the demands of the platform business model rapidly began to drive infrastructure design. As a result of that shift, the everyday lives of network users have become increasingly datafied — converted into structured flows of data suitable for continuous collection and analysis at the platform level.

One important technological predicate for the emergence of platforms emerged in the mid-1990s, when researchers at the Netscape Corporation developed the first protocol for identifying visitors to web sites. The protocol, which involved insertion of a small piece of code called a "cookie" into the user's browser, enabled so-called "stateful" interactions, such as transactions involving use of a virtual shopping cart. Implemented in "persistent" form, it also could enable reidentification of those users when they returned to the site later on.[12] The resulting radical democratization of surveillance capability marks a critical inflection point in the pursuit of user legibility. Using cookie technology, anyone with a server connected to the Internet could become a data collector, and cookies also could be served and collected by third parties providing hosting, payment, or marketing services. Willingness to accept at least some kinds of cookies rapidly

[12] *See* David M. Kristol, *HTTP Cookies: Standards, Privacy, and Politics*, 1 ACM TRANSACTIONS ON INTERNET TECH. 151, 152-56 (2001).

became an increasingly necessary precondition for transacting online and participating in online communities. In addition, marketers and technologists in their employ developed a set of less-visible tracking techniques, known variously as "clear GIFs" or "web bugs," for surreptitiously collecting information about Internet users' behavior.[13]

In parallel with these developments, new platform-based environments for social sharing and massively multiplayer gaming were taking shape in ways that also relied on techniques for keeping track of users. The earliest online communities were organized around chat rooms, listservs, and communal bulletin boards, and had neither the desire nor the capability for built-in surveillance. In the late 1990s and early 2000s, however, the first true multimedia gaming platforms and social networking platforms began to emerge: graphically rich, hypertext-based environments that enabled customizable member profiles and relied on cookies to manage login information.[14]

At the same time, a variety of firms — including emerging platform firms, digital advertising specialty firms, and data brokers — were developing new and powerful data analysis capabilities. Those capabilities combined new configurations of information-processing hardware capable of sifting, sorting, and interrogating vast quantities of data in very short times with new machine learning techniques for identifying patterns, distilling the patterns into predictions, and continually adjusting the patterns and predictions in response to new data.[15] The result, popularized under the moniker "Big Data," was a technique for converting voluminous, heterogeneous flows of physical, transactional, and behavioral information about people (or about anything else) into a particular, highly data-intensive type of knowledge.[16]

---

[13] *See* Richard M. Smith, *The Web Bug FAQ*, ELEC. FRONTIER FOUND. (Nov. 11, 1999), https://w2.eff.org/Privacy/Marketing/web_bug.html.

[14] *See* TRISTAN DONOVAN, REPLAY: THE HISTORY OF VIDEO GAMES 289-319 (2010); Benjamin Hale, *The History of Social Media*, HISTORY COOP. (June 16, 2015), http://historycooperative.org/the-history-of-social-media; *The History of Social Networking*, DIG. TRENDS (May 14, 2016, 6:00 AM), https://www.digitaltrends.com/features/the-history-of-social-networking.

[15] *See generally* Dave Feinleib, *The 3 I's of Big Data*, FORBES (July 9, 2012, 4:05 PM), http://www.forbes.com/sites/davefeinleib/2012/07/09/the-3-is-of-big-data; Jeff Kelly, *Big Data: Hadoop, Business Analytics and Beyond*, WIKIBON (Feb. 5, 2014), http://wikibon.org/wiki/v/Big_Data:_Hadoop,_Business_Analytics_and_Beyond.

[16] *See generally* JAMES MANYIKA ET AL., MCKINSEY GLOBAL INSTITUTE, BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY (2011); Ibrar Yaqoob et al., *Big Data: From Beginning to Future*, 36 INT'L J. INFO. MGMT. 1231 (2016); Gil Press, *A Very Short History of Big Data*, FORBES (May 9, 2013, 9:45 AM), https://onforb.es/16jHac8 (last updated Dec. 21, 2013).

The platform business model emerged as these developments converged with one another and with the demands of capital markets. As they moved beyond the startup phase and sought stable sources of financing, new ventures in search, social networking, gaming, content provision, day trading, freelance work referral, and other areas gradually became entangled within commercial and extractive logics. Advertisers who might provide revenue wanted results and users were learning to value personalization. Personalized tracking and predictive modeling seemed the logical way to satisfy both imperatives.

Although many platform-based businesses have failed, when judged in aggregate, the platform business model is an undeniable commercial success. Google and Facebook together now command approximately 20% of global advertising revenue, 65% of digital advertising revenue, and 85% of every new dollar spent on advertising.[17] The dominant platform firms — Alphabet (Google), Amazon, Apple, Facebook, and Microsoft — have a combined market capitalization that (as of this writing) exceeds $3.5 trillion.[18] Although the dominant platform firms are all publicly traded companies, the relationships between platform firms and private flows of finance capital are also deep and complex.[19]

The commercial and extractive logics that drove emergence of the platform business model success now impose their own design imperatives, which demand continued evolution of the networked information environment toward ever more pervasive intermediation

[17] *See* Lucy Handley, *Google and Facebook Take 20 Percent of Total Global Ad Spend, Top List of World's Largest Media Owners*, CNBC (May 2, 2017, 8:46 AM), http://www.cnbc.com/2017/05/02/google-and-facebook-take-20-percent-of-total-global-ad-spend.html; Matthew Ingram, *How Google and Facebook Have Taken Over the Digital Ad Industry*, FORTUNE (Jan. 4, 2017), http://fortune.com/2017/01/04/google-facebook-ad-industry; Peter Kafka, *Google and Facebook Are Booming. Is the Rest of the Digital Ad Business Sinking?*, RECODE (Nov. 2, 2016, 1:55 PM), https://www.recode.net/2016/11/2/13497376/google-facebook-advertising-shrinking-iab-dcn.

[18] *See AAPL*, NASDAQ (June 2, 2017), http://www.nasdaq.com/symbol/aapl [https://perma.cc/6SDZ-VQFM] ($805,538,280,000); *AMZN*, NASDAQ (June 2, 2017), http://www.nasdaq.com/symbol/amzn [https://perma.cc/LGK3-33UW] ($480,972,978,949); *FB*, NASDAQ (June 2, 2017), http://www.nasdaq.com/symbol/fb [https://perma.cc/8L9N-S94N] ($442,928,382,963); *GOOG*, NASDAQ (June 2, 2017), http://www.nasdaq.com/symbol/goog [https://perma.cc/RU8L-Z6ZX] ($673,209,740,440); *GOOGL*, NASDAQ (June 2, 2017), http://www.nasdaq.com/symbol/googl [https://perma.cc/3KGJ-58AB] ($687,504,656,146); *MSFT*, NASDAQ (June 2, 2017), http://www.nasdaq.com/symbol/msft [https://perma.cc/TE7T-3XVJ] ($550,086,674,584).

[19] *See generally* Martin Kenney, Explaining the Growth and Globalization of Silicon Valley: The Past and Today (Jan. 12, 2017) (unpublished manuscript) (on file with author).

and datafication.[20] Those imperatives have shaped the emergence of smart mobile devices, wearable computing, and the Internet of things, dictating implementations that emphasize seamless tracking, fine-grained measurement of patterns of behavior and attention, extraction of continuous flows of data, and configuration of data flows into forms best suited to analysis and commercial exploitation.[21] As a result of these interdependent marketplace and infrastructural shifts, commercial information collection has become a nearly continuous condition. Communications networks have gradually been transformed into sensing networks, organized around always-on mobile devices that collect and transmit highly granular streams of structured information via proprietary interfaces and protocols to powerful, proprietary machine learning systems. Put differently, networked media infrastructures have become pervasively platformized.[22]

C. A Platform Is Not (Just) a Network

Over the past several decades, scholars in a wide variety of fields have identified networks and infrastructures as important organizing concepts for studying the information economy. In some discussions of the information economy, the terms "network," "infrastructure," and "platform" are used interchangeably, but platforms are not the same as networks, nor are they simply infrastructures. Platforms represent infrastructure-based strategies for introducing friction into networks. In theory, the twenty-first century communications infrastructure still known as the Internet is "open," and for some purposes, that characterization is accurate. For most practical purposes, however, the "network of networks" is becoming a network of platforms; Internet access and use are intermediated from beginning to end.

A *network* is a mode of organization in which hubs and nodes structure the flows of transactions and interactions. Network organization is not a unique property of digital information and communications networks; rather, as network scientists have shown, such networks simply make visible a latent characteristic of the many

[20] *See generally* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 73-97 (2013); Jose Van Dijck, *Datafication, Dataism, and Dataveillance: Big Data Between Scientific Paradigm and Ideology*, 12 SURVEILLANCE & SOC'Y 197 (2014).

[21] *See generally* Anne Helmond, *The Platformization of the Web: Making Web Data Platform Ready*, SOC. MEDIA & SOC'Y, July-Dec. 2015, at 1.

[22] *See generally* Jean-Christophe Plantin et al., *Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook*, NEW MEDIA & SOC'Y, 2016, at 1.

human activities that rely on communication and interconnection.[23] Digital information and communications networks do, however, reduce many of the costs and lag times formerly associated with such activities. In addition, participants in networks reap generalized benefits (network externalities[24]) as those networks grow in size and scale, and the relatively low costs of digital interconnection have enabled digital networks to become very large.

Infrastructures are shared resources that facilitate downstream production of other goods.[25] Roads and electric power grids, for example, play essential roles as inputs into a variety of downstream goods, as do less tangible resources like linguistic and scientific conventions. Notably, infrastructures may be managed as commons but need not be: some infrastructures, such as the interbank wire transfer system, are club goods financed and controlled by their members; others, such as local electric power suppliers, are managed as utilities and financed based on metered consumption charges; and still others, including facilities for Internet access in most countries, are privately provided but subject to various regulatory obligations. Digital information and communications technologies function both as infrastructures and as networks. As scholars in fields ranging from industrial organization to geography to media and communications studies have shown, the forms of connectivity they provide have reshaped seemingly every area of human activity.[26]

Platforms exploit the affordances of network organization and supply infrastructures that facilitate particular types of interactions, but they also represent strategies for bounding networks and privatizing and controlling infrastructures. They operate with the goal of making clusters of transactions and relationships stickier — sticky enough to adhere to the platform despite participants' theoretical ability to exit and look elsewhere for other intermediation options. To accomplish that goal, platforms must provide services that participants view as desirable and empowering, thereby generating and enabling participants to leverage network externalities. But they also must

[23] *See generally* ALBERT-LASZLO BARABASI, LINKED (2014).

[24] Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP. 93, 94 (1994).

[25] *See generally* BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES 61-114 (2012).

[26] *See, e.g.*, CASTELLS, *supra* note 1; GLOBAL NETWORKS, LINKED CITIES (Saskia Sassen ed., 2002); JOSE VAN DIJCK, THE CULTURE OF CONNECTIVITY: A CRITICAL HISTORY OF SOCIAL MEDIA (2013); Laurel Smith-Doerr & Walter W. Powell, *Networks and Economic Life*, *in* THE HANDBOOK OF ECONOMIC SOCIOLOGY 379 (Neil J. Smelser & Richard Swedberg eds., 2d ed. 2005).

thwart certain other kinds of networking that might facilitate defection to rival platforms.

Platforms use technical protocols and centralized control to define networked spaces in which users can conduct a heterogeneous array of activities and to structure those spaces for ease of use. The vehicle for managing the tensions between heterogeneity and ease of use is modularity; platform protocols impose a modular structure that enables certain types of flexibility but at the same time forecloses others. Protocol-based control also enables intermediation and facilitates legibility, allowing the platform to serve its own priorities.[27] In Tarleton Gillespie's formulation, the term "platform" appears to offer users a "raised, level surface" on which to present themselves, but at the same time it elides the necessary work of defining and policing the platform's edges.[28] Platform protocols perform a double function, affording access but also points of contact for exercises of technological and political authority. The latter power is one that the fictionalized construct of the market lacked, and it comprehensively reshapes the conditions of economic exchange.

D. How Platforms Shape Economic Exchange

Economically speaking, platforms represent both horizontal and vertical strategies for extracting the surplus value of user data.[29] Because that goal requires large numbers of users generating large amounts of data, the platform provider's goal is to become and remain the indispensable point of intermediation for parties in its target markets. Commentators have begun to puzzle over the implications of the dominance and staggering market capitalization of the largest platform firms.[30] The characteristic "rich-get-richer" pattern of network organization, however, militates in favor of the emergence of

---

[27] *See* Plantin et al., *supra* note 22, at 5-9; *see also* Tarleton Gillespie, *The Politics of 'Platforms*,' 12 NEW MEDIA & SOC'Y 347 (2010).

[28] Gillespie, *supra* note 27, at 358-59; *see also* Jonas Andersson Schwarz, *Platform Logic: An Interdisciplinary Approach to the Platform-Based Economy*, POL'Y & INT. 4-13 (Aug. 3, 2017) (DOI: 10.1002/poi3.159).

[29] *Cf.* MARK ANDREJEVIC, iSPY: SURVEILLANCE AND POWER IN THE INTERACTIVE ERA (2007); Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 78-80 (2015). *See generally* NICK SRNICEK, PLATFORM CAPITALISM (2017); DANIEL TROTTIER, SOCIAL MEDIA AS SURVEILLANCE: RETHINKING VISIBILITY IN A CONVERGING WORLD (2012).

[30] *See, e.g.*, Alexis C. Madrigal, *Silicon Valley's Big Three vs. Detroit's Golden-Age Big Three*, ATLANTIC (May 24, 2017), https://www.theatlantic.com/technology/archive/2017/05/silicon-valley-big-three/527838.

dominant platforms, and platform firms also have devised a variety of other strategies for attaining and maintaining dominance, each targeting multiple user groups.[31]

To begin with, platforms both enable and benefit from competitive dynamics of economic exchange that differ in profoundly important ways from those of traditional, one-sided markets. The exchanges constituted by platforms are two- or multi-sided: they serve buyers, the sellers seeking to reach them, and often advertisers seeking the buyers' attention. Because the platform forms relationships with members of each group separately, it can define the terms of each relationship differently.[32] So, for example, it can charge little or nothing to participants on one side of a target market and make its profit on another side. A dominant platform can reduce prices to one group — for example, book buyers or consumers of professional networking services — below marginal cost and still maintain its dominance by charging fees to some other group, and a provider of free services to consumers can attain and maintain dominance by controlling access to the "market for eyeballs."

Another set of strategies for leveraging economies of scale into more durable patterns of competitive advantage involves preferential placement, and exploits a conundrum that confronts platform users as platform economies of scale become more and more overpowering. Platform users — whether buyers and sellers or social network members seeking their counterparts — seek access to platforms in order to be found. They soon discover, though, that while access to platforms is a necessity, access alone is insufficient; competitive or reputational success in a platform environment requires information-based strategies for boosting visibility. In theory, the platform's legibility function should provide effective matching in ways that take account of "long tail" patterns of supply and demand; in reality, the results of algorithmic matching often seem to prioritize the most popular results. Platforms have developed various techniques for offering and monetizing preferential placement, such as "sponsored search results" (e.g., Google's AdWords and AdSense programs) and "enhanced listing placement" (e.g., Amazon's Featured Merchant program).[33] Because of the platform environment's operational

[31] On the rich-get-richer principle, see BARABASI, *supra* note 23, at 79-92.

[32] *See generally* Jean-Charles Rochet & Jean Tirole, *Two-Sided Markets: A Progress Report*, 37 RAND J. ECON. 645 (2006); David S. Evans & Richard Schmalensee, *The Antitrust Analysis of Multi-Sided Platform Businesses* (Nat'l Bureau of Econ. Research, Working Paper No. 18783, 2013), http://www.nber.org/papers/w18783.

[33] *See, e.g.*, *Buy Box Eligible Status*, AMAZON, http://smile.amazon.com/gp/help/

secrecy, however, purchasers of these services cannot easily monitor the quality of what they have purchased; more generally, platform users cannot easily determine whether platform firms are engaging in other, undisclosed varieties of preferential placement.[34]

A third set of strategies for leveraging economies of scale into more durable patterns of competitive advantage involves interplatform affiliation. Smaller and more specialized platforms may contract with more dominant platforms to provide particular services — e.g., payment processing, streaming video, games for social network users, and so on. Such arrangements benefit both dominant and niche platforms, giving niche platforms access to a larger pool of users and dominant platforms access to a larger and deeper pool of information about users' online activities.[35] It is unsurprising, then, that the interrelationships among platforms have become increasingly dense and complex. Such agreements, though, also create risks for all parties. A dominant platform must consider the possibility that what had been envisioned as a niche or add-on service will become a new species of

customer/display.html?nodeId=200418180 (last visited July 20, 2017); *Enhanced Listing Placement*, AMAZON, https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_ac?ie=UTF8&nodeId=200572340 (last visited July 20, 2017); *How It Works*, GOOGLE ADSENSE, https://www.google.com/adsense/start/how-it-works (last visited July 20, 2017); *How It Works*, GOOGLE ADWORDS, https://adwords.google.com/home/how-it-works (last visited July 20, 2017); *see also* Karla Lant, *Everything You Need to Know About Amazon Featured Merchant Status*, APPEAGLE, http://blog.appeagle.com/amazon-featured-merchant-status (last visited July 20, 2017); Chuck Topinka, *How Exactly Does Google AdWords Work?*, FORBES (Aug. 15, 2014, 12:04 PM), https://www.forbes.com/sites/quora/2014/08/15/how-exactly-does-google-adwords-work. *See generally* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 774-83 (2017) (discussing Amazon's services and their profitability).

[34] *See, e.g.*, Julia Angwin & Surya Mattu, *Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't*, PROPUBLICA (Sept. 20, 2016, 8:00 AM), https://www.propublica.org/article/amazon-says-it-puts-customers-first-but-its-pricing-algorithm-doesnt; Benjamin Edelman, *Hard-Coding Bias in Google "Algorithmic" Search Results*, BEN EDELMAN (Nov. 15, 2010), http://www.benedelman.org/hardcoding; Julia Greenberg, *Google Will Now Favor Pages That Use Its Fast-Loading Tech*, WIRED (Feb. 24, 2016, 10:00 AM), https://www.wired.com/2016/02/google-will-now-favor-pages-use-fast-loading-tech; Daniel Trielli et al., *Why Google Search Results Favor Democrats*, SLATE (Dec. 7, 2015, 11:48 AM), http://www.slate.com/articles/technology/future_tense/2015/12/why_google_search_results_favor_democrats.html. *See generally* ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY 35-81 (2016) (discussing collusion-based strategies within platform environments).

[35] *See generally* MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 293-99 (2016); Bertin Martens, *An Economic Policy Perspective on Online Platforms* (Inst. for Prospective Tech. Studies Dig. Econ., Working Paper No. 2016/05, 2016).

dominant intermediary in its own right, as Internet browsers, search engines, social networks, and mobile operating systems all have done. Niche platforms, meanwhile, are no better placed than platform users to monitor the behavior of dominant platforms. They may find themselves receiving fewer or different benefits than expected or competing with the dominant platform's own offerings under conditions that seem to place them at a disadvantage.[36]

From the perspective of users, advertisers, and niche platforms, dominant platforms like Google and Facebook function in a manner analogous to utilities, supplying basic information services now deemed essential to a wide variety of economic and social activities. At the same time, dominant platforms also constitute vast and highly differentiated information ecosystems. The tools for effecting legibility constructed by such businesses extend globally, subsuming and rematerializing not only markets but also patterns of social and political interaction.

E. How Platforms Shape Information Flow, part 2: Personalization, Polarization, and Volatility in the Networked Public Sphere

Massively intermediated, platform-based media infrastructures have reshaped the ways that narratives about reality, value, and reputation are crafted, circulated, and contested. Platforms enhance the ability to form groups and share information among members, to harness the wisdom of crowds, and to coalesce in passionate, powerful mobs, but they also magnify the dark side of each of these forms of collective action. The massive intermediation and datafication of networked media infrastructures, meanwhile, shifts the tenor of much networked interaction into the domains of the affective, instinctual, and unreasoning.

The dominant cultural narratives about the cultural and political effects of platforms have been celebratory. Just as networked digital

[36] *See, e.g.*, David Pierce, *Pandora Premium Can't Hang with Spotify and Apple*, WIRED (Mar. 13, 2017, 9:00 AM), https://www.wired.com/2017/03/pandora-premium; John Patrick Pullen, *Streaming Showdown: Apple Music vs. Spotify vs. Pandora vs. Rdio*, TIME (June 9, 2015, 9:25 AM), http://time.com/3913955/apple-music-spotify-pandora-rdio-streaming; Janko Roettgers, *Pandora Adds Continuous Playback Feature to Sidestep Apple, Tidal Exclusives*, VARIETY (June 8, 2017, 10:00 AM), http://variety.com/2017/digital/news/pandora-autoplay-exclusives-1202458470; Gerry Shih, *Facebook App Makers Struggle with How Fickle Facebook Can Be*, HUFFINGTON POST (Mar. 11, 2013, 1:09 AM), http://www.huffingtonpost.com/2013/03/11/facebook-apps_n_2850893.html; Edward Wyatt & Noam Cohen, *Comcast and Netflix Reach Deal on Service*, N.Y. TIMES (Feb. 23, 2014), https://nyti.ms/2mtBXtH.

platforms have lowered the costs of identifying and connecting with commercial counterparties, so they also have lowered the costs of forming affinity groups of all kinds. Platform users can more easily find and connect with others who share their hobbies and passions, their political affiliations and goals, their racial, religious, or gender identities, their affiliations with real-world communities (such as neighborhood or parent-teacher associations), and many more. Networked, platform-based digital media infrastructures also facilitate distributed, peer-based production of information.[37] As a result, the Internet era has witnessed the emergence of a vast, diverse, and eclectic range of cultural production, ranging from open source software developed according to the maxim "given enough eyeballs, all bugs are shallow" to wikis and fanworks reflecting multiple contributions.[38] The landscape of networked collective action also encompasses new forms of collective meaning-making, such as memes and flash mobs; new infrastructures for facilitating both traditional charitable giving and other types of "pay-it-forward" generosity; and new capacities for rapid organization of mass protests, such as those of the Occupy Wall Street and Black Lives Matter movements and the Arab Spring uprisings.[39]

Other implications of the contemporary, platform-based digital environment's affordances for group-formation, distributed peer production, and collective action are less rosy. Crowd-based judgments about relevance can create information cascades that lend sensationalized, false, and hatred-inciting online material extraordinary staying power.[40] Efforts to remove hurtful material

[37] *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006).

[38] *See* ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR 30 (1999); *see, e.g.*, AXEL BRUNS, BLOGS, WIKIPEDIA, SECOND LIFE, AND BEYOND 101-36 (2008); FAN FICTION AND FAN COMMUNITIES IN THE AGE OF THE INTERNET (Karen Hellekson & Kristina Busse eds., 2006); Jason Mittell, *Wikis and Participatory Fandom*, *in* THE PARTICIPATORY CULTURES HANDBOOK 35-42 (Aaron Delwiche & Jennifer Jacobs Henderson eds., 2012).

[39] *See* DEEN FREELON ET AL., BEYOND THE HASHTAGS: #FERGUSON, #BLACKLIVESMATTER, AND THE ONLINE STRUGGLE FOR OFFLINE JUSTICE 5, 14 (2016); REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 15-25 (2012); Elizabeth Day, *#BlackLivesMatter: The Birth of a New Civil Rights Movement*, GUARDIAN (July 19, 2015, 5:00 AM), http://www.theguardian.com/world/2015/jul/19/blacklivesmatter-birth-civil-rights-movement.

[40] *See* April Mara Barton, *Application of Cascade Theory to Online Systems: A Study of Email and Google Cascades*, 10 MINN. J.L. SCI. & TECH. 473 (2008-2009); Timur Kuran & Cass R. Sunstein, *Availability Cascades and Risk Regulation*, 51 STAN. L. REV. 683 (1999); Gilad Lotan, *Fake News is not the Only Problem*, DATA & SOC'Y: POINTS (Nov. 22, 2016), http://points.datasociety.net?fake-news-is-not-the-problem-f00ec8cdfcb.

typically backfire by drawing additional attention to it, intensifying and prolonging the unwanted exposure.[41] Additionally, because of the way that platform-based, massively-intermediated environments work, networked spaces both expose and intensify political and ideological polarization around multiple, assertedly equivalent truths. A wealth of social science research shows that more homogenous groups can more easily become polarized in both their beliefs and their perceptions of reality.[42] Such polarization is not new, but over the last several decades, the percentages of those reporting strongly negative feelings about those with opposing views have skyrocketed.[43] Algorithmic mediation of information flows intended to target controversial material to receptive audiences intensifies such feelings, reinforcing existing biases, inculcating resistance to facts that contradict preferred narratives, and encouraging demonization and abuse.[44] New data harvesting techniques designed to detect users' moods and emotions and messaging techniques that rely on "clickbait" exacerbate these problems; increasingly, today's networked information flows are optimized for subconscious, affective appeal.[45] As in-group, perspectival "filter bubbles" become more pronounced, crossing cultural and ideological lines becomes more difficult. Exposure to opposing views is more likely to trigger automatic, instinctual rejection and anger than it is to promote reasoned engagement.[46]

[41] *See Streisand Effect*, WIKIPEDIA, https://en.wikipedia.org/wiki/Streisand_effect (last updated July 6, 2017, 7:37 PM).

[42] For helpful summaries, see DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 56-72 (2014); Cass Sunstein, *Believing False Rumors*, *in* THE OFFENSIVE INTERNET 91, 91-106 (2010); Ana Lucía Schmidt et al., *Anatomy of News Consumption on Facebook*, 114 PROC. NAT'L ACAD. SCI. 3035, 3035-38 (2017); Walter Quattrociocchi et al., *Echo Chambers on Facebook* 1-2, 4-13 (John M. Olin Ctr. for Law, Econ. & Bus., Harvard Law Sch., Discussion Paper No. 877, 2016).

[43] *See* Matthew Gentzkow, *Polarization in 2016*, TOULOUSE NETWORK INFO. TECH. (2016), https://web.stanford.edu/~gentzkow/research/PolarizationIn2016.pdf.

[44] *See generally* MARK ANDREJEVIC, INFOGLUT: HOW TOO MUCH INFORMATION IS CHANGING THE WAY WE THINK AND KNOW 42-61 (2013).

[45] *See id.* at 96-100, 106-10; Tasha Glenn & Scott Monteith, *New Measures of Mental State and Behavior Based on Data Collected from Sensors, Smartphones, and the Internet*, CURRENT PSYCHIATRY REP., Oct. 12, 2014, at 5-6; Franklin Foer, *When Silicon Valley Took Over Journalism*, ATLANTIC (Sept. 2017), https://www.theatlantic.com/magazine/archive/2017/09/when-silicon-valley-took-over-journalism/534195. *See generally* Hilke Plassmann et al., *Consumer Neuroscience: Applications, Challenges, and Possible Solutions*, 52 J. MARKETING RES. 427 (2015); Vinod Venkatraman et al., *New Scanner Data for Brand Marketers: How Neuroscience Can Help Better Understand Differences in Brand Preferences*, 22 J. CONSUMER PSYCHOL. 143 (2012).

[46] *See, e.g.*, Emma Grey Ellis, *The Seth Rich Conspiracy Theory: A Tale of Two Filter Bubbles*, WIRED (May 18, 2017, 10:30 AM), http://www.wired.com/2017/05/seth-rich-

Platform-based information feeds also flatten communicative hierarchies in a way that challenges traditional heuristics for judging credibility and may undermine claims to objective and/or empirical authority; within a Facebook or Twitter feed, for example, all sources are (or appear to be) epistemologically equivalent.[47]

Notably, platform affordances for volatility, polarization, and relativization are easily manipulated for malicious or simply self-interested purposes. As is now widely known, in the months preceding the 2016 U.S. presidential election, web sites peddling "fake news" stories — such as allegations that Democratic candidate Hillary Clinton and her campaign manager, John Podesta, were running a child pornography ring out of the basement of a Washington, D.C., pizza restaurant — earned their distributors millions of dollars in advertising revenues. According to their own statements, at least some distributors had no particular political axe to grind, but instead were simply exploiting the affordances of the network by circulating "clickbait" carefully designed to earn the clicks, views, shares, and retweets that generate advertising revenue. Others, we have come to learn, were sponsored by state actors with grander hopes and ambitions.[48] As they had hoped, groups predisposed to believe the worst of Clinton and her team shared, up-voted, and retweeted the stories.[49] Experts in election law and digital voting, watching carefully

filter-bubble; Jon Keegan, *Blue Feed, Red Feed: See Liberal Facebook and Conservative Facebook, Side by Side*, WALL ST. J. (May 18, 2016, 8:00 AM), http://graphics.wsj.com/blue-feed-red-feed; Quattrociocchi et al., *supra* note 42, at 12-13. The term "filter bubble" has entered the popular lexicon as a way of conveying these effects, see generally ELI PARISER, THE FILTER BUBBLE (2011), but it may also be misleading; people do encounter opposing views and inconvenient facts online. The bubble consists of the priors that determine what they make of those views and facts. The filter (the algorithm) reinforces the bubble by playing to the priors.

[47] For a useful introduction to the literature on how social media users assess credibility, with discussions of unanswered questions, see Miriam J. Metzger & Andrew J. Flanagin, *Credibility and Trust of Information in Online Environments: The Use of Cognitive Heuristics*, 59 J. PRAGMATICS 210 (2013).

[48] Sam Levin, *Facebook to Give Congress Thousands of Ads Bought by Russians During Election*, GUARDIAN (Sept. 21, 2017, 4:16 PM), https://www.theguardian.com/technology/2017/sep/21/facebook-adverts-congress-russia-trump-us-election; Julia Carrie Wong, *Russia's Election Ad Campaign Shows Facebook's Biggest Problem Is Facebook*, GUARDIAN (Sept. 21, 2017, 9:10 PM), https://www.theguardian.com/technology/2017/sep/21/facebook-russia-advertising-mark-zuckerberg.

[49] *See* Hunt Allcott & Matthew Gentzkow, *Social Media and Fake News in the 2016 Election*, 31 J. ECON. PERSP. 211, 223-24 (2017); David A. Graham, *The 'Comet Pizza' Gunman Provides a Glimpse of a Frightening Future*, ATLANTIC (Dec. 5, 2016), http://www.theatlantic.com/politics/archive/2016/12/the-inevitability-of-more-comet-pizza-incidents/509567; Lotan, *supra* note 40; *see also Tall Tales Spread by Alex Jones*

for signs of fraudulent tampering with digital voting machines, were unprepared for a new kind of digital tampering campaign that took aim directly at voters' minds. But perhaps no-one should have been surprised; the earlier "Brexit" vote in the United Kingdom had followed a similar pattern.[50]

With increased volatility and polarization also has come a rise in identity-based harassment, mob aggression, nationalism, and organized hate. Affordances for collective action have enabled the rapid formation of angry, vengeful mobs, eager to shame real or apparent transgressors or to engage in identity-based harassment and intimidation. Women and members of racial, religious, and/or sexual minorities who have become prominent in media and journalism or in hacker and gaming communities are especially frequent targets of such campaigns.[51] More generally, organized hate against racial and religious minorities is on the rise, aided by algorithmic processes that amplify bigoted diatribes, magnify conspiracy theories, and propel coded memes into the limelight.[52] Nativist hate-mongering online has bled inexorably into political discourse and public life, adopting sophisticated and ironic new forms, gaining in strength as outraged responses generate new information cascades, and fueling the rise of the self-designated "alt-right" as a political force.[53]

Breed Dangerous Plots, SOUTHERN POVERTY L. CTR.: INTELLIGENCE REP. (Feb. 15, 2017), http://www.splcenter.org/fighting-hate/intelligence-report/2017/tall-tales-spread-alex-jones-breed-dangeorus-plots.

[50] *See* Carole Cadwalladr, *The Great British Brexit Robbery: How Our Democracy Was Hijacked*, GUARDIAN (May 7, 2017, 4:00 AM), http://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy; Katherine Viner, *How Technology Disrupted the Truth*, GUARDIAN (July 12, 2016, 1:00 AM), http://theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth.

[51] *See generally* CITRON, *supra* note 42; WHITNEY PHILLIPS, THIS IS WHY WE CAN'T HAVE NICE THINGS (2015).

[52] *See, e.g.*, ALICE MARWICK & REBECCA LEWIS, MEDIA MANIPULATION AND DISINFORMATION ONLINE (2017); Emma Grey Ellis, *The Internet Protocols of the Elders of Zion*, WIRED (Mar. 12, 2017, 7:00 AM), http://www.wired.com/2017/03/internet-protocols-elders-zion; Mark Potok, *The Year in Hate and Extremism*, SOUTHERN POVERTY L. CTR: INTELLIGENCE REP. (Feb. 15, 2017), http://splcenter.org/fighting-hate/intelligence-report/2017/year-hate-and-extremism.

[53] *See* George Hawley, *The Alt-Right Is Not Who You Think They Are*, AM. CONSERVATIVE (Aug. 25, 2017), http://www.theamericanconservative.com/articles/the-alt-right-is-not-who-you-think-it-is; Ben Schreckinger, *The Alt-Right Comes to Washington*, POLITICO (Jan./Feb. 2017), http://www.politico.com/magazine/story/2017/01/alt-right-trump-washington-dc-power-milo-214629; Jason Wilson, *Hiding in Plain Sight: How the Alt-Right Is Weaponizing Irony to Spread Fascism*, GUARDIAN (May 23, 2017), https://www.theguardian.com/technology/2017/may/23/alt-right-online-humor-as-a-weapon-facism.

The increasingly polarized, volatile, and unreasoning character of interaction in online, platform-based digital environments complicates accounts of the democratizing potential of information networks. Networked, platform-based information and communication technologies are crowd-enhancers; they boost the amplitude of collective actions and counter-actions, making networked spaces sites of both extraordinary generativity and extraordinary volatility. Undeniably, such technologies have important affordances for bottom-up organizing, collective creativity, and crowd-sourced, democratic action. Collective meaning-making and collective action, however, can be directed toward a variety of ends. The particular configurations that those technologies have assumed within the political economy of informational capitalism also make them sites of extraordinary manipulability, creating new risks to the human project of democratic, inclusive, sustainable coexistence. Accounts of the promise or peril of networked communication and production have tended to downplay one or the other face of networked communication and collective action, but — at least for the present — the two are inextricably linked.

II. PLATFORM ENTITLEMENTS

As platforms have interacted with the legal system, their efforts have begun to reshape the landscape of baseline entitlements (and disentitlements) in informational resources. A useful starting point from which to begin thinking through the issues is the classic taxonomy developed by Wesley Hohfeld over a century ago.[54] Hohfeld's central insight was that entitlements are relational, and that the rights-duties relationship — i.e., the relationship that arises when one person has a right that others must respect — is only one of the possibilities. Entitlements also may take the form of privileges, powers, or immunities, each of which affects others in different kinds of ways. If one takes that insight seriously, it follows that law might shape the transition to an information economy in multiple ways. It might define rights and correlative duties in new informational resources, but it might also, for example, recognize privileges to appropriate certain new and valuable resources and/or confer legal immunity for certain types of informational harm. As we are about to

[54] *See generally* Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16 (1913); *cf.* Pierre Schlag, *How to Do Things with Hohfeld*, 78 L. & CONTEMP. PROBS. 185 (2015) (arguing that Hohfeldian analysis is best understood as a method of deconstructing legal relations to identify the imprint of power).

see, it has done all of those things — and has done them in ways that systematically facilitate the platform economy's emergence.

A. Points of Access (Rights to Control Entry)

Among intellectual property lawyers, it is a truism that data and algorithms — the building blocks of innovation and competition — cannot themselves be the subjects of property rights. Appearances can be deceptive, however. The movement to an informational economy is reconstructing data and algorithms as appropriable inputs to new and highly informationalized modes of profit extraction. Data flows from the dematerialization of labor, land, and money have been joined by a new and highly lucrative fourth factor of production: personal information gathered from and about individuals and groups. Property formalism notwithstanding, these resources are the subjects of active appropriation strategies. As the perceived imperatives of access to data and to data processing capacity have sharpened, platform-driven cycles of dis- and re- intermediation have emerged as a recurring motif in information-economy narratives about competition, innovation, and access.

Platform-based competitive strategies revolve fundamentally around control of access in two different and complementary senses. Platform users seek access to the essential social, commercial, and cultural connectivity that platforms provide, while platform providers seek access to the data necessary to create and sustain competitive advantage in their chosen field(s) of intermediation. The result is a bargain that appears relatively straightforward — access for data — but that in reality is complex and importantly generative. One important byproduct of these access-for-data arrangements is a quiet revolution in the legal status of data as (de facto if not de jure) proprietary informational property.

A principal worry for any platform is disintermediation by a would-be competitor, and so platform providers work to define both collected data and algorithmic logics as zones of exclusivity. In particular, platforms use contracts systematically to facilitate and protect their own legibility function, extracting transparency from users but shielding basic operational knowledge from third-party vendors, users, and advertisers alike. The particular form of the access-for-data contract — a boilerplate terms-of-use agreement not open to negotiation — asserts a nonnegotiable authority over the conditions of access that operates in the background of even the most generative information-economy service. Boilerplate agreements are contractual in form but mandatory in operation, and so are a powerful tool both

for private ordering of behavior and for private reordering of even the most bedrock legal rights and obligations.[55]

From an intellectual property perspective, the terms-of-use agreements crafted by platforms and other information intermediaries function as points of entry for institutional entrepreneurship targeting the form and substance of legal entitlements in information. In a process that is fundamentally performative, the terms-of-use agreement steps in where the map of formal legal entitlements ends, providing a vehicle for leveraging trade secrecy entitlements into de facto property arrangements that affect large numbers of people with no direct relationship with the platform owner. The contracts themselves, of course, are "only words" — and, for that matter, words that most users do not read — but they gain powerful normative force from both their continual assertion and reassertion and their propagation within environments that use technical protocols to define the parameters of permitted behavior.[56] The combination of asserted contractual control and technical control becomes the vehicle through which the platform imposes its own logics on the encounters that it mediates.

The *logic of performative enclosure* that infuses terms-of-use agreements also carries over into platform enterprises' dealings with developers and commercial counterparties, where it is paired with subsidiary strategies of performative openness. Even as they jockey with one another to become the intermediary of choice for more and more users' networked interactions, dominant platforms understand the risk of disintermediation as a continuing threat. Successful platforms jealously guard access to both data collected from users and the algorithms used to process the data — and at the time same entice developers and commercial counterparties with promises of access. So, for example, Facebook's promise not to share users' data with advertisers is true; it offers advertisers placement precisely targeted to the inferred needs and desires of its billions of users but never direct access to the data or algorithms themselves. Application developers receive access to carefully curated data sets, data structures and

---

[55] *See generally* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013).

[56] *Cf.* Nicholas Blomley, *Disentangling Law: The Practice of Bracketing*, ANN. REV. L. & SOC. SCI., Nov. 2014, at 133 (describing the ways that legal practices and distinctions themselves produce the perceived reality within which those distinctions matter); Nicholas Blomley, *Performing Property: Making the World*, 26 CAN. J.L. & JURIS. 23, 39-40 (2013).

programming interfaces.[57] Google's vaunted commitments to open data and open code do not extend to its algorithms or to the data it collects about its users, and it imposes other restrictive conditions on developers seeking to offer Android devices or Android-compatible applications.[58]

Traditional intellectual property rights play helpful but only secondary roles in the process of de facto propertization, functioning as sources of leverage that can be invoked to channel would-be users toward entering the access-for-data bargain on the platform's terms and/or to prevent would-be competitors from gaining access to information stored on the platform by other means. For example, access to a branded exchange may enable third-party vendors to position their products and services as more desirable to consumers. When access to a platform requires technical interoperability — as is the case, for example, with apps for desktop and mobile operating systems — patents and copyrights can supply important points of leverage against unauthorized access by third-party vendors and would-be platform competitors. As the example of Google shows, however, not all platform businesses consider copyrights a necessary tool for limiting access.

In sum, the access-for-data arrangement is both a concrete bargain and a complex act of institutional entrepreneurship, with a number of interrelated implications for the intellectual property system that are still playing out. In addition to their other roles, platforms are in an important sense intellectual property entrepreneurs, working to refine and propagate appropriation strategies that serve their economic interests. Yet the investigation in this section also has surfaced additional questions: Where do the data that feed platformized logics of appropriation come from, and who decides on their allocation? What accounts for the startling power of platforms to command adherence to their terms? Have any countervailing obligations emerged that platforms are bound to respect? Who or what determines the proper allocation of accountability for harms flowing from datafication and platformization? As we will see in the remainder of

[57] *See generally* Helmond, *supra* note 21; Plantin et al., *supra* note 22, at 11-12.

[58] *See generally* Benjamin Edelman, *Does Google Leverage Market Power through Tying and Bundling?*, 11 J. COMPETITION L. & ECON. 365, 389-91 (2015); Plantin et al., *supra* note 22, at 13-14; Christian Sandvig, *Seeing the Sort: The Aesthetic and Industrial Defense of "The Algorithm,"* MEDIA-N (2014), http://median.newmediacaucus.org/art-infrastructures-information/seeing-the-sort-the-aesthetic-and-industrial-defense-of-the-algorithm.

this Part, answering those questions requires moving beyond investigations of rights and correlative duties to respect them.

B. Points of Extraction (Privileges to Appropriate)

As Part I explained, the data extracted from individuals plays an increasingly important role *as raw material* in the political economy of informational capitalism. Scholarship on the relationship between law and the collection and processing of personal information typically considers such activities as raising problems of privacy or data protection, and typically has focused on regulation of such activities after the fact. But the legal framework within which the collection, processing, and use of personal data occur is not simply a reactive framework, nor is it simply concerned with the relationship between policing (or employment, consumer finance, or medical research) and privacy. Understood as processes of resource extraction, the activities of collecting and processing personal information mobilize a very different legal construct — one foreign to privacy and data protection law but commonplace within intellectual property law. Contemporary practices of personal information processing constitute a new type of public domain: a source of raw materials that are there for the taking and that are framed as inputs to particular types of productive activity.[59]

A public domain is not a naturally occurring phenomenon. It is first and foremost an idea: a culturally-situated way of understanding patterns of resource ownership and availability. But a public domain also is much more than an idea: the construct of a public domain both designates particular types of resources as available and suggests particular ways of putting them to work.[60] In Hohfeldian terms, a public domain is a zone of legal privilege: it demarcates conduct as to which no-one has a right to object. It thereby legitimates the resulting patterns of appropriation and obscures the distributive politics in which they are embedded.

We have already seen that the *logic of productive appropriation* from a public domain of personal data has catalyzed sweeping reorganizations of sociotechnical activity to facilitate cultivation,

---

[59] The discussion in this section is adapted from Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, PHIL. & TECH., Mar. 28, 2017, http://dx.doi.org/10.1007/s13347-017-0258-2.

[60] *See generally* Anupam Chander & Madhavi Sunder, *The Romance of the Public Domain*, 92 CALIF. L. REV. 1331 (2004); Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965 (1990).

harvesting, and appropriation of personal data. Notably, participants in the personal data economy — including platform providers but also data brokers and digital analytics firms — have systematically devised data collection strategies that route around the obstacles posed by privacy and data protection frameworks devised for an earlier era. In the United States, most privacy statutes are sector-specific; many apply only to certain entities and most contain exceptions allowing consent to information collection and processing. Platforms in particular have structured their information-collection activities around broad presumptive consent and have configured the world of networked digital infrastructures and artifacts in ways that make user enrollment seamless and near-automatic. The resulting sociotechnical processes work both to generate large quantities of personal information and to make public domain status the default condition for the information that is generated.

The logic of productive appropriation from a public domain of personal data also does epistemological work. It frames the personal information harvested within networked information environments as raw, creating the backdrop for new algorithmic techniques of knowledge production that operate as sites of legal privilege. Within intellectual property circles, that narrative is entirely commonplace. In 1984, John Moore sued the Regents of the University of California and a UCLA doctor who had treated his leukemia for conversion (wrongful appropriation) of his personal property. The property identified in his complaint was his cancerous spleen, which had been removed from his body and used to develop a valuable, patented cell line. The lawsuit reached the California Supreme Court, which rejected Moore's conversion theory on the ground that diseased tissue removed from the human body could not be the subject of a property interest (though it allowed Moore to maintain an action for failure of informed consent).[61] The *Moore* opinion is routinely included in first-year property casebooks, where it stands for the principle that anti-commodification values can (sometimes) prevent the propertization of human tissue. But the court did not hold that human tissue could not be the subject of any proprietary claims. Rather, it contrasted Moore's claim to that of the research scientists who had labored to develop the patentable byproduct. And, even as it took for granted the wisdom of granting patents on medical research byproducts, it worried fretfully

[61] Moore v. Regents of the Univ. of Cal., 793 P.2d 479 (Cal. 1990).

about the costs to innovation of allowing proprietary claims to the raw materials used in medical research.[62]

One can trace a similar elaboration of relative privilege and disentitlement in the evolving debate about the future of fair information practices in the era of pervasive commercial surveillance. In regulatory proceedings and in the media, the data processing industries have advanced a carefully crafted narrative that links data processing with "innovation" and positions privacy and "innovation" as fundamentally and intractably opposed. That narrative powerfully shapes prevailing perceptions of feasible regulatory options.[63] Data brokers and platform firms proudly tout their "unprecedented," "proprietary," and sometimes "patented" analytic techniques.[64] Claims like these situate ownership of personal data at the heart of the data refinery, vesting it in those who (supposedly) create value where none previously existed. They work to create and perpetuate a narrative of romantic authorship that unfolds in counterpoint to that of the public domain, and that is old and familiar.[65] Meanwhile, commentators concerned to preserve the benefits of so-called "Big Data" worry that a right to withdraw one's data from databases, if widely exercised, would compromise the utility of those databases as resources for pattern identification.[66]

The "raw data" framing, of course, conceals an important misdescription. As we saw in Part I, it is inaccurate to say that the data

---

[62] *See id.* at 494-95.

[63] *See* Julie E. Cohen, *The Surveillance-Innovation Complex: The Irony of the Participatory Turn*, *in* THE PARTICIPATORY CONDITION IN THE DIGITAL AGE 207, 218-22 (2016).

[64] For some examples, see *About*, INTELIUS, http://corp.intelius.com (last visited July 20, 2017) ("proprietary genomic technology"); *About*, SPOKEO, http://www.spokeo.com/about (last visited July 20, 2017) ("proprietary merge technology"); *Company Overview*, ID ANALYTICS, http://www.idanalytics.com/company (last visited July 20, 2017) ("patented analytics"); Amit Finkelstein, *Facebook Analytics Adds Pages Support and Launches Automated Insights*, FACEBOOK FOR DEVELOPERS (Apr. 18, 2017), https://developers.facebook.com/blog/post/2017/04/18/facebook-analytics-new-features-f8 ("advanced machine learning and artificial intelligence," "exciting features," "powerful"); *New Oracle Data Cloud and Data-as-Service Offerings Redefine Data-Driven Enterprise*, ORACLE (July 22, 2014), http://www.oracle.com/us/corporate/pressrelease/data-cloud-and-daas-072214 ("unprecedented intelligence"); Susan Wojcicki, *The Eight Pillars of Innovation*, THINK WITH GOOGLE (July 2011), https://www.thinkwithgoogle.com/marketing-resources/8-pillars-of-innovation ("sophisticated technology," "innovative outcomes," "uncharted territory").

[65] *See generally* JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY (1998); Chander & Sunder, *supra* note 60.

[66] *See, e.g.*, Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 67-68 (2012).

collected for processing just happen to be there; flows of personal data are artifacts of design for datafication. From that perspective, the processes of harvesting and culling "raw" consumer personal data resemble the harvesting of raw materials within an industrial system of agriculture. Just as agriculture on an industrial scale demands grain varieties suited to being grown and harvested industrially, so the collection of personal information on an industrial scale inevitably adopts an active, curatorial stance regarding the items to be gathered.[67] Strains of information are selected and cultivated precisely for their durability and commercial value within a set of information processing operations. The data are both raw and cultivated, both real and highly artificial. The algorithmic processes that manipulate the data function as information-age refineries. In a process comparable to the milling of corn and wheat to generate stable, uniform byproducts optimized for industrial food production, they convert data-based inputs into the forms best suited for exploitation on an industrial scale.[68] They refine and massage consumer personal data to produce virtual representations — data doubles — that work to make human behaviors and preferences calculable, predictable, and profitable *in aggregate* by producing tranches of data doubles with probabilistically determined purchasing and risk profiles.[69] Business of all sorts can use the information to determine the particular prices and feature packages best calibrated for surplus extraction, and to generate preemptive nudges that, when well executed, operate as self-fulfilling prophecies, producing consummated transactions over the offerings already judged to be most likely to appeal to targeted consumers.[70]

---

[67] *See* MICHAEL POLLAN, THE OMNIVORE'S DILEMMA: A NATURAL HISTORY OF FOUR MEALS 30-31, 36-37, 41-42, 45, 58-59 (2007). *See generally* Danah Boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO. COMM. & SOC'Y 662 (2012); LISA GITELMAN, ED., "RAW DATA" IS AN OXYMORON (2013).

[68] *See* POLLAN, *supra* note 67, at 17-19, 85-99.

[69] *See generally* Greg Elmer, *IPO 2.0: The Panopticon Goes Public*, 4 MEDIA TROPES 1, 9-12 (2013); Marion Fourcade & Kieran Healy, *Seeing Like a Market*, 15 SOCIO-ECON. REV. 9 (2017); Zuboff, *supra* note 29.

[70] This terminology combines the concept of the nudge, imported from the context of behavioral economics, see generally RICHARD THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008), and is now widely used by both critics and admirers of data-based analytics, with that of preemption as used by MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW 57-61 (2015), and Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE 65, 68-71 (2013). The preemptive nudge simultaneously suggests and forecloses.

The idea of a public domain of personal information does vital background work in the emerging platform economy, altering the legal status of the inputs to and outputs of personal data processing in ways that are relational and distributive. It both suggests and legitimates a pattern of appropriation by some, with economic and political consequences for others.

C. Speech Markets and Information Laboratories (Immunities from Accountability)

As the networked information environment has redistributed control over reputational development, powerful economic actors have worked to craft narratives that make unaccountability for certain types of information harms seem logical, inevitable, and right. They have relied heavily on the U.S. first amendment tradition, which characterizes the public sphere as a marketplace of ideas — an arena for neutral truth production through deliberate, reasoned exchange, where the goods on offer can be evaluated on their merits, where the volume and quality of information are regulated by the laws of supply and demand, and where those making decisions about the quality of information function as separate, individual nodes of rationality.[71] In that project, they have benefited from preexisting libertarian and neoliberal narratives that already supplied potent recipes for resisting media regulation. As the marketplace metaphor has come to be seen as increasingly inapt for the massively-intermediated, platform-based information environment, however, platforms also have introduced a new metaphoric frame: that of the information laboratory, which functions as a site of depoliticized innovation through continuous, behaviorist experimentation. In Hohfeldian terms, the developments sketched in this section are most aptly characterized as emergent legal immunities and correlative disabilities. Their ongoing construction has proceeded in almost willful disregard of the fact that the affordances of

[71] The metaphor traces its origins to a famous dissent by Justice Holmes. *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas — that the best test of truth is the power of the thought to get itself accepted in the competition of the market . . . ."). For a sampling of perspectives on the metaphor and its significance for free speech jurisprudence, see generally Vincent Blasi, *Holmes and the Marketplace of Ideas*, 2004 SUP. CT. REV. 1; Stanley Ingber, *The Marketplace of Ideas: A Legitimizing Myth*, 33 DUKE L.J. 1 (1984); Robert Post, *Reconciling Theory and Doctrine in First Amendment Jurisprudence*, 88 CALIF. L. REV. 2353 (2000).

the platform-based, massively intermediated information environment strain the idea of neutral truth production past the breaking point.

The legal construction of platform immunity for information harms is in part a constitutional strategy that leverages preexisting trends in first amendment jurisprudence. For some time now, a campaign has been underway to insulate all forms of commercial information processing and direct-to-consumer communication from regulatory oversight on first amendment grounds. For almost two centuries, the first amendment was considered largely irrelevant to regulation of speech advancing commercial activities because such regulation was understood to be directed fundamentally at commerce rather than at public discourse. That began to change in the late twentieth-century, in a line of cases that became known as the Court's commercial speech jurisprudence; according to those cases, regulation of commercial speech that is neither misleading nor related to unlawful activity must advance a substantial government interest and must be appropriately tailored to that interest.[72] Today that doctrine is under sustained assault for being too lenient. Both regulations addressing direct-to-consumer communication and regulations addressing information processing more generally begin with some definition of scope that identifies particular types of content and/or particular actors. Other strands of first amendment jurisprudence label such distinctions as requiring compelling justification and the narrowest possible tailoring. That analytical gap has created a point of entry for an antiregulatory agenda that holds all regulation of information processing to be illegitimate.[73] A notable recent victory for that agenda is *Sorrell v. IMS Health Inc.*, in which a majority of the Court struck down a Vermont statute prohibiting pharmaceutical companies' use of prescriber-identifying information for marketing purposes, applying strict

[72] *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 561-66 (1980). *See generally* Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447 (1978); Bates v. State Bar of Ariz., 433 U.S. 350 (1977); Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748 (1976).

[73] For a discussion of the origins of the neoliberal first amendment as an advocacy movement, see generally Amanda Shanor, *The New* Lochner, 2016 WISC. L. REV. 133. For influential formulations of the first amendment challenge to information privacy regulation, see generally Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Keep Other People from Speaking About You*, 52 STAN. L. REV. 1049 (2000); Solveig Singleton, *Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector*, CATO INST. POL'Y ANALYSIS, Jan. 22, 1998, https://object.cato.org/sites/cato.org/files/pubs/pdf/pa-295.pdf (Policy Analysis No. 295); Adam Thierer & Berin Szoka, *What Unites Advocates of Speech Controls & Privacy Regulation?*, PROGRESS ON POINT, Nov. 2009, at 1, http://www.pff.org/issues-pubs/pops/2009/pop16.19-unites-speech-and-privacy-reg-advocates.pdf.

scrutiny because the restriction was both content- and speaker-based.[74] Characterizing the state's action as an attempt to undermine the persuasive force of pharmaceutical marketers' speech (and thereby harnessing the marketplace metaphor), the majority concluded that the law struck at the core of the zone that the first amendment protects.[75]

Although platforms did not originate the campaign to constitutionalize regulation of commercial information processing activities, they have been willing participants both through their own efforts and via the efforts of trade associations and libertarian think tanks. Advertiser trade associations that count major platform firms Apple, Google, and Microsoft among their members filed a coalition amicus brief on behalf of respondent data brokers in *Sorrell* and regularly participate in other commercial speech litigation.[76] In 2012, Google commissioned an expert white paper on platform free speech rights that has become a cornerstone of the speech-based defense that platforms assert in litigation with private plaintiffs challenging their information processing practices.[77]

In litigation with private parties alleging information-related harms, however, courts typically do not need to reach constitutional defenses because another kind of immunity kicks in. Section 230 of the Communications Decency Act ("CDA"), enacted as part of the Telecommunications Act of 1996, grants broad immunity to online intermediaries for their roles in distributing speech produced by others.[78] In the legislative history and in individual statements,

---

[74] *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 563-70 (2011). *See generally* Reed v. Town of Gilbert, 135 S. Ct. 2218 (2015) (holding that laws either motivated by disagreement with a message or unable to be justified without reference to the content of the regulated speech are content-based and must satisfy strict scrutiny).

[75] *See Sorrell*, 564 U.S. at 577-78.

[76] Brief of Amici Curiae Ass'n of Nat'l Advertisers, Inc. et al. in Support of Respondents, *Sorrell*, 564 U.S. 552 (No. 10-779), 2011 WL 1253920. *But see, e.g.*, Brief of Amici Curiae of Ass'n of Nat'l Advertisers, Inc. et al. in Support of Petitioners, Nike, Inc. v. Kasky, 539 U.S. 654 (2003) (No. 02-575), 2003 WL 835112.

[77] *See* Eugene Volokh & Donald M. Falk, *Google: First Amendment Protection for Search Engine Results*, 8 J.L. ECON. & POL'Y 883 (2012); *see also* e-ventures Worldwide, LLC v. Google, Inc., 188 F. Supp. 3d 1265, 1274 (M.D. Fla. 2016) ("The Court has little quarrel with the cases cited by Google for the proposition that search engine output results are protected by the First Amendment.") (citing Zhang v. Baidu.com Inc., 10 F. Supp. 3d 433, 455 (S.D.N.Y. 2014)), *appeal docketed*, No. 17-11178 (11th Cir. Mar. 16, 2017); Defendants Vill. Voice Media Holdings, LLC; Backpage.com, LLC; and New Times Media, LLC's Motion for Summary Judgment at 9, 17-26, J.S. v. Vill. Voice Media Holdings, LLC, No. 12-2-11362-4 (Wash. Sup. Ct. Mar. 23, 2017).

[78] Communications Decency Act, Pub. L. No. 104-104 § 509, 110 Stat. 56, 138

members of Congress endorsed the marketplace metaphor as the principal justification for section 230's broad grant of immunity, stating their belief that such immunity would foster and preserve the emerging network as a vibrant marketplace of ideas.[79] Both the statutory language and the discourse that surrounded its adoption framed still-emergent networked information architectures as engines for neutral truth production — conduits that would simply reflect and transmit what people wanted to say. In other words, they posited the Internet as a space lacking the sorts of specific affordances that might themselves shape communicative practices and communicative content.[80]

Speech intermediaries and information aggregators have worked strenuously to defend that institutional settlement even as time and technological change have undermined its implicit premises, downplaying or reframing the extent to which what we see online is itself recursively shaped by what information businesses produce. For the most part, courts have uncritically accepted those arguments, concluding both that algorithmic mediation doesn't make an intermediary a publisher of other people's speech and that the same processes of mediation are speech-like in their own right.[81]

As Part I explained, however, market-based narratives about the origins of and justifications for platform immunity are premised on

(1996) (codified as amended at 47 U.S.C. § 230(c)(1) (2012)).

[79] *See* Communications Decency Act of 1996, Pub. L. 104-104, tit. V, 110 Stat. 133 (codified as amended at 47 U.S.C. § 230(a)(3) (1998)) ("The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."); 142 CONG. REC. H1175 (daily ed. Feb. 1, 1996) (statement of Rep. Gilchrest) ("And with the advent of the information age, we need to recognize the need for competition among information media so that the free marketplace of ideas can be communicated through a free marketplace of information outlets. This bill seeks to exploit the market's ability to maximize quality, maximize consumer choice, and minimize prices."); *see also* Senator Ronald Wyden, Speech to the Section 230 Anniversary Conference (Mar. 4, 2011) ("The Internet is becoming a central platform for commerce and a means by which people and societies organize. It is the shipping lane of the 21st century, the marketplace of ideas and a democratic town square inside even the most repressive of nations. It was imperative in 1996 that the nascent Internet be protected from the interests of those that wanted to tax and control it. But now that we have seen the power and importance of the Internet — protecting it is that much more imperative.").

[80] *See* Gillespie, *supra* note 27, at 359. On the persistence and inaccuracy of the myth of cyberspace as empty space, see generally Julie E. Cohen, *Cyberspace and/as Space*, 107 COLUM. L. REV. 210 (2007) [hereinafter Cohen, *Cyberspace*].

[81] *See generally* James Grimmelmann, *Speech Engines*, 98 MINN. L. REV. 868 (2014).

assumptions about the affordances of media infrastructures that no longer hold. Platform-based, massively-intermediated processes of search and social networking are inherently processes of market manipulation. Networked environments configured to optimize data harvesting and surplus extraction operate — and are systematically designed to operate — in ways that preclude even the most perceptive and reasonable consumer from evaluating the goods or services on offer. Predictive profiling seeks to minimize the need to persuade by targeting directly those potential customers most strongly predisposed to buy and appealing to everything that is known about those customers' habits and predilections. And, as we saw in Part I, the deliberate design of platform-based, massively-intermediated media infrastructures for data harvesting and commercial surveillance has produced other, less deliberate affordances that amplify the role of unreason in online interaction, and that matter enormously.

Most recently, platform businesses have begun to acknowledge more directly their pervasive manipulations of the information environment in the service of profit extraction, and to recast those manipulations as inherently directed toward discovering scientific truths about human behavior. Platform-based media infrastructures, they argue, are information laboratories, in which providers of information services experiment to see which types of information are most useful and most responsive to consumers' needs and innovate by providing that information. So, for example, Google's chief economist has explained that at any given time Google and competing search engines are running millions of experiments on their users, designed to determine how we respond to information so that search results can be optimized.[82] Facebook, which through its news feed competes with search engines to structure users' access to the wider information environment, also experiments on its users. In 2014, a paper coauthored by a Facebook data scientist and published in the *Proceedings of the National Academy of Sciences* described a massive experiment in which Facebook varied items in users' newsfeeds and then used automated discourse analysis tools on those users' own subsequent posts to gauge the effects of the newsfeeds on their emotional states.[83] When critics decried Facebook's failure to give

[82] *See generally* Hal R. Varian, *Beyond Big Data*, 49 BUS. ECON. 27 (2014).

[83] *See* Adam D. I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L ACAD. SCI. 8788 (2014).

users prior notice of the experiment, Facebook's defenders pointed out that marketing is inherently a science of experimentation.[84]

Within the emerging narrative of the information laboratory as an engine of behaviorist truth-discovery and depoliticized innovation, the fact that online information intermediaries manipulate meaning in ways and for purposes that they do not disclose ceases to be an inconvenient truth to be carefully downplayed and becomes banal and unremarkable reality. From that perspective, the recent troubling demonstrations that platform-based, massively-intermediated media infrastructures have played pivotal roles in fostering deeply entrenched political polarization — polarization that extends all the way down to bedrock narratives about reality and scientific fact — are mere glitches in systems that are still being perfected through sober and responsible experimentation. So framed, they are not problems requiring resolution in the domain of media regulation, competition regulation, or some other domain, but rather matters best left to the benevolent and disinterested experts in the white lab coats to sort out.[85]

That too is a mistake on the most basic, descriptive level. Affordances for polarization and volatility are not fixed and invariant; they are constructed and can be amplified or dampened by deliberate choices made in the course of a platform's design. At minimum, the platform business model, which is so heavily reliant on predictive profiling and target marketing and on the information cascades and sensationalism that draw eyeballs and generate ad revenues, is causally implicated in the current dysfunctions of the online information environment even though that was not its creators' intent. Arguably, platform businesses that resist serious, open exploration of those causal dynamics are complicit in fostering the dysfunctions. More

[84] For critiques, see, for example, Michael Hiltzik, *Facebook's User Manipulation Study: Why You Should Be Very Afraid*, L.A. TIMES (June 30, 2014, 2:02 PM), http://www.latimes.com/business/hiltzik/la-fi-mh-facebooks-user-20140630-column.html; Letter from James Grimmelmann & Leslie Meltzer Henry, Professors of Law, Francis King Carey Sch. of Law, to Inder M. Verma, Editor-in-Chief, Proceedings of the Nat'l Acad. of Sci. (July 17, 2014), http://james.grimmelmann.net/files/legal/facebook/PNAS.pdf. For defenses, see, for example, Dan Diamond, *The Outrage over Facebook's 'Creepy' Experiment Is out-of-Bounds — and This Study Proves It*, FORBES (July 1, 2014, 2:34 PM), http://www.forbes.com/sites/dandiamond/2014/07/01/the-outrage-over-facebooks-creepy-experiment-is-out-of-bounds-and-this-study-proves-it; Duncan J. Watts, *Stop Complaining About the Facebook Study. It's a Golden Age for Research*, GUARDIAN (July 7, 2014, 7:45 AM), http://www.theguardian.com/commentisfree/2014/jul/07/facebook-study-science-experiment-research.

[85] For an especially fulsome statement of this view, see Mark Zuckerberg, *Building Global Community*, FACEBOOK (Feb. 16, 2017), https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634.

troubling still, some platforms have been silent partners in fostering the hate and harassment that they officially disclaim.[86] If ever the time were ripe for rethinking the frames and presumptions that conventionally have structured discussions of media regulation in U.S. law and policy, that time surely is now.

The *logic of expressive immunity*, however, requires that attempts to focus judicial and legislative attention on these issues be met with carefully tended hysteria about censorship and injured protestations of first amendment virtue. Those strategies too build upon traditions within first amendment doctrine and rhetoric. Both the arguments for first amendment immunity and the strident defenses of intermediary immunity by information businesses and their apologists express a long-established and distinctively neoliberal ideology of public discourse, within which profit-motivated private enterprises are appropriate and morally virtuous guarantors of expressive liberty.[87] From one perspective, they represent the latest step in a decades-long campaign to equate all forms of media regulation with censorship; from another, they have produced a new and powerful antiregulatory force field that insulates information businesses from accountability for both new and old information harms. An analytical framework that begins by assuming the problem of mediated unreason away disables courts and policymakers from crafting appropriate (and appropriately speech-regarding) forms of regulatory oversight.

---

[86] *See, e.g.*, Madison Malone Kircher, *Are Tech Companies Lazy, Incompetent, or Greedy?*, N.Y. MAG. (Sept. 15, 2017, 5:40 PM), http://nymag.com/selectall/2017/09/google-facebook-and-twitter-sell-hate-speech-targeted-ads.html; Keegan Hankes, *Cloudflare Optimizing Content Delivery for at Least 48 Hate Sites Across Europe*, SOUTHERN POVERTY L. CTR. (Mar. 7, 2017), https://www.splcenter.org/hatewatch/2017/03/07/cloudflare-optimizing-content-delivery-least-48-hate-sites-across-europe; Ken Schwencke, *How One Major Internet Company Helps Serve up Hate on the Internet*, PROPUBLICA (May 4, 2017, 8:00 AM), http://propublica.org/article/how-cloudflare-helps-serve-up-hate-on-the-web?utm_campaign=weekly-newsletter&utm_source=pardot&utm_medium=email. As of this writing, increased attention to this issue is beginning to prompt changes in platform policies, but the changes are controversial and contested. *See* Timothy B. Lee, *Tech Companies Declare War on Hate Speech—And Conservatives Are Worried*, ARS TECHNICA (Aug. 31, 2017, 7:05 PM), https://arstechnica.com/tech-policy/2017/08/tech-companies-are-cracking-down-on-hate-speech/.

[87] *See generally* Julie E. Cohen, *The Zombie First Amendment*, 56 WM. & MARY L. REV. 1119 (2015) [hereinafter Cohen, *The Zombie First Amendment*]; Timothy K. Kuhner, Citizens United *as Neoliberal Jurisprudence: The Resurgence of Economic Theory*, 18 VA. J. SOC. POL'Y & L. 395 (2011).

D. Conduits vs. Content (Powers of Interdiction)

Platforms are not the only powerful entities with interests in shaping flows of information, and logics of intermediation are not the only kinds of logics that networked, platform-based infrastructures enable. Networked media infrastructures also offer new possibilities for interrupting and blocking information flows, and those capabilities can be deployed to serve a variety of interests. In particular, nation states and intellectual property owners have pushed both to code interdiction capabilities into the network's underlying logical and hardware layers and to impose interdiction obligations on network intermediaries, including platforms. In Hohfeldian terms, such arrangements are most aptly classified as powers to alter the legal obligations of others and to impose liability for noncompliance. Platforms, meanwhile, have resisted those efforts, seeking arrangements that better serve their own interests. In terms of law on the books, those struggles have produced a still-shifting patchwork of regulatory obligations and political stalemates. The apparent disarray, however, masks two more durable shifts. In many contexts, platform-based and algorithmically-mediated "self-regulation" has emerged as the path of least resistance. At the same time, *logics of fiat interdiction* have become progressively normalized within legal and policy discourse.

State actors have always sought to control information flows, and all states permit some such controls. For example, in democratic countries that traditionally have recognized broad protection for freedoms of speech and association, there is broad consensus that neither child pornography nor step-by-step instructions for producing weapons-grade plutonium should circulate freely. In mid-1990s, however, amid dawning realization that decentralized digital networks facilitated the uncontrolled and sometimes viral spread of all kinds of information, long-stable areas of consensus about state control of information flows began to destabilize and shift. Some countries began to mandate backbone-level filtering for certain kinds of content and/or to enlist Internet access and search providers in such filtering.[88] Others began to confront new kinds of disputes about prohibited information flow.

In the United States, one recurring topic of dispute has been the extent of the government's ability to conduct secret surveillance

[88] *See generally* MACKINNON, *supra* note 39, at 34-66; A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE 129 (Brian Kahin & Charles Nesson eds., 1997).

programs that rely on the cooperation of private communications providers and use practices of "deep secrecy" to shield such programs from public oversight.[89] By the turn of the twenty-first century, a diverse collection of scholars, tech industry observers, and legal advocates had become worried that networked digital communications infrastructures were enabling vast, secret expansions in government surveillance activities. Bits of evidence gleaned from public investigations following the terrorist attacks of 9/11, inadvertent leaks, and isolated acts of whistleblowing were beginning to add up to the outline of something much larger. The courts, however, rebuffed an early attempt to litigate the chilling effects of dragnet surveillance, reasoning that the plaintiffs had not alleged cognizable injury because they could not prove they or their clients had been targeted or that any of their communications had been collected and read.[90] After disclosure of a long-term, secret, government surveillance operation inside AT&T's San Francisco Bay Area operations center prompted class action litigation, Congress hastily amended the Foreign Intelligence Surveillance Act to retroactively authorize certain warrantless demands for interception and also granted retroactive immunity to intermediaries that had complied with such demands.[91] Then, in June 2013, the world learned that former National Security Agency contractor Edward Snowden had copied and disclosed to the media voluminous files documenting the NSA's extralegal surveillance of communications worldwide, including many programs conducted with the essential involvement of platform firms. In the wave of lawsuits that followed the Snowden disclosures, courts have become willing to concede that the government conducted some level of dragnet communications surveillance but then have cited other justifications either for dismissal or for allowing only limited "jurisdictional discovery" that feature logics of fiat interdiction at their core, including both the need to defer to the executive branch in national security matters and the imperative of protecting state secrets.[92]

---

[89] *See generally* David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257 (2010).

[90] *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1140-41 (2013).

[91] *See* FISA Amendments Act, Pub. L. No. 110-261, 122 Stat. 2436, 2448-67 (2008) (codified as amended at 50 U.S.C. §§ 1881a, 1885a(a)(4) (2015)); *In re* Nat'l Sec. Agency Telecomms. Records Litig., 633 F. Supp. 2d 949 (N.D. Cal. 2009) (dismissing class action claims), *aff'd in relevant part*, 671 F.3d 881 (9th Cir. 2011), *cert. denied*, 568 U.S. 958 (2012).

[92] *See, e.g.*, Wikimedia Found. v. NSA, 857 F.3d 193, 209-11, 213-15 (4th Cir. 2017) (recognizing standing for large media organization engaged in trillions of communications but holding that other plaintiffs lacked standing because they could

Another recurring topic of dispute has been the extent to which the government can require platforms to preserve lines of access into users' private communications. In 1994, Congress enacted legislation requiring telecommunications providers to design and maintain wiretap capability, but efforts to legislate similar "back door" capabilities for digital microprocessors were defeated after strong opposition from both the computer industry and academic computer scientists.[93] The resulting equilibrium was only temporary, however. The statutory framework has become increasingly obsolete in an era in which communications by voice, text, and email all travel over digital networks and in which capabilities for strong communications encryption are increasingly widespread. In the wake of the 2015 terrorist attack in San Bernardino, California, after which investigators acquired but could not readily access one terrorist's iPhone, law enforcement and national security officials mounted an aggressive campaign, still continuing as of this writing, to convince both Congress and the courts to impose decryption mandates on communications firms that provide strong encryption capabilities to their users.[94]

not show that NSA's upstream surveillance program intercepted "substantially all" communications); Schuchardt v. President, 839 F.3d 336, 349-54 (3d Cir. 2016) (accepted allegation that NSA's upstream surveillance program intercepted substantially all communications for purposes of ruling on motion to dismiss but cautioning that plaintiff should be allowed only limited "jurisdictional discovery" because of secrecy concerns surrounding national security operations); Obama v. Klayman, 800 F.3d 559, 563-64 (D.C. Cir. 2015) (Brown, J., concurring) (same); ACLU v. Clapper, 959 F. Supp. 2d 724, 751-56 (S.D.N.Y. 2013) (dismissed constitutional claims but noting that, even if those claims could proceed, preliminary injunction would be inappropriate given the urgently compelling nature of the government's need to combat terrorism), *rev'd on other grounds*, 785 F.3d 787 (2d Cir. 2015); Jewel v. NSA, No. C 08-04373 JSW, 2015 WL 545925, at *5 (N.D. Cal. Feb. 10, 2015) (granting summary judgment for government on plaintiffs' constitutional claims because, even if plaintiffs could establish standing, state secrets doctrine would prevent full litigation of the issues), *appeal dismissed*, 810 F.3d 622, 625 (9th Cir. 2015) (holding that certification for interlocutory appeal was not warranted).

[93] *See* Communications Assistance for Law Enforcement Act, Pub. L. 103-414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C. §§ 1001-1010 (2012)); DANIELLE KEHL ET AL., DOOMED TO REPEAT HISTORY? LESSONS FROM THE CRYPTO WARS OF THE 1990S 1, 5-11 (2015), http://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf; Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES MAG. (June 12, 1994), http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all.

[94] *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 344 (E.D.N.Y. 2016); *In re* The Search of an Apple Iphone Seized During the Execution of a Search Warrant on a

The major copyright industries and software producing firms also have worked to alter the legal status of providers of networked information services in ways that would require them to prevent flows of unauthorized content or face potentially ruinous liability. The political power of the copyright industries predates that of platform firms. Over the course of the twentieth century, the publishing, music, television, and motion picture industries coalesced into a politically savvy interest group that exerted powerful influence over the shape of copyright legislation. By the 1990s, the software industry also had emerged as a force to be reckoned with in copyright legislative debates. As the uncontrolled viral spread of information via digital networks began to command the attention of lawmakers and policymakers, both old and new copyright industries worked to spread alarm about the growing amount of online infringement and file-sharing. In a blizzard of press releases and media interviews, and in a variety of more formal interventions ranging from conference remarks to congressional testimony, they equated online copyright infringement with theft, piracy, communism, plague, pandemic, and, notably, with terrorism.[95] They lobbied strenuously for the enactment of new legislative protections and also filed high-profile lawsuits against third-party service and equipment providers that they viewed as culpable facilitators.

Generally speaking, the copyright industries have pursued two primary strategies that implicate the legal status of platform firms. One revolves around takedowns of infringing content using a streamlined process triggered by notice without prior judicial review; formally, the process is optional, but platforms that implement it receive safe harbor from infringement liability.[96] Although the notice-and-takedown system regularly elicits significant numbers of meritless or legally

Black Lexus IS300, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016); *The Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 14-15 (2016) (statement of James Comey, Director, FBI); Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What it Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599, 621-26 (2016); *All Writs Act Orders for Assistance from Tech Companies*, AM. C.L. UNION, http://www.aclu.org/map/all-writs-act-orders-assistance-tech-companies (last visited July 20, 2017).

[95] *See generally* Julie E. Cohen, *Pervasively Distributed Copyright Enforcement*, 95 GEO. L.J. 1, 24-25 (2006); John Logie, *A Copyright Cold War? The Polarized Rhetoric of the Peer-to-Peer Debates*, FIRST MONDAY (July 7, 2003), http://firstmonday.org/article/view/1064/984.

[96] *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, § 202, 112 Stat. 2860, 2879-80, 2885 (1998) (codified as amended at 17 U.S.C. § 512(c)-(d), (j)(1) (2012)).

questionable takedown notices (many generated by automated processes for detecting infringement), it has been implemented around the world as a result of pressure exerted by U.S. trade negotiators.[97] The second strategy relies on prohibitions against circumvention of technical access protections and trafficking in circumvention technologies.[98] The anti-trafficking provisions in particular were the cornerstone of a litigation campaign designed to ensure that manufacturers of equipment for rendering media content sought appropriate licenses. As a result of those efforts and parallel campaigns to develop new technical-protection formats and standards, the major commercially available systems for delivering and playing audiovisual content now incorporate functionality designed to defeat copying and prevent retransmissions to unauthorized platforms and devices.[99]

The emergence of dominant platform firms, however, has shifted the balances of power in debates about both government surveillance and online copyright enforcement. Platform and copyright interests have clashed repeatedly both in the courts and in Congress, and platform interests often have gotten the upper hand. From the beginning, new platform-based technologies for storing, finding, and sharing information seemed to frustrate efforts to block unauthorized flows of infringing content. In litigation, the copyright industries argued that the platform business model fell outside the scope of legislated safe harbors for online service providers that complied with the notice and takedown process; in Congress, they pressed their case for the imposition of affirmative filtering obligations and other new mandates.[100] Both efforts failed repeatedly. The push for new mandates

[97] *See* Markham C. Erickson & Sarah K. Leggin, *Exporting Internet Law Through International Trade Agreements: Recalibrating U.S. Trade Policy in the Digital Age*, 24 CATH. U. J.L. & TECH. 317, 343-49 (2016). *See generally* Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171 (2010); Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621 (2006).

[98] *See* Digital Millennium Copyright Act §§ 1201-1204.

[99] *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 158-60, 179-81 (2012); TARLETON GILLESPIE, WIRED SHUT: COPYRIGHT AND THE SHAPE OF DIGITAL CULTURE (2007).

[100] *See, e.g.*, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1021-23 (9th Cir. 2013); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 34-35 (2d Cir. 2012); Audio Broadcast Flag Licensing Act of 2006, H.R. 4861, 109th Cong. (2006); Digital Transition Content Security Act of 2005, H.R. 4569, 109th Cong. (2005); Consumer Broadband and Digital Television Promotion Act of 2002, S. 2048, 107th Cong. (2002); *see also* Am. Library Ass'n v. FCC, 406 F.3d 689, 691-92 (D.C. Cir. 2005) (invalidating a broadcast content protection rule issued by the FCC on

culminated in 2011, when proposed legislation establishing new procedures for blocking access to domains offering infringing content and isolating them from their payment providers began to move rapidly through Congress and was widely expected to pass. Instead, platform firms flexed their newfound political muscle in a novel way, repurposing their access protocols to coordinate a massive mobilization of the online community that effectively shut down many of the Internet's most popular sites.[101] Congress tabled the legislation soon afterward and has not revived it.

Platform firms also have visibly resisted some government initiatives for surveillance and deep secrecy. In 2008, after several widely-publicized capitulations by platform firms to authoritarian regimes' demands for censorship of certain content, a coalition of platform firms, academics, and nongovernmental organizations formed the Global Network Initiative, an organization dedicated to helping communications intermediaries advocate for their users' freedom of speech, privacy, and other civil liberties worldwide.[102] After the Snowden revelations, platform giant Apple Computer spearheaded a movement to make strong encryption the marketplace default for both voice and text communications.[103] As law enforcement officials seeking access to encrypted communications and devices have urged Congress to respond by imposing decryption mandates, platform firms

jurisdictional grounds). *But see* Commercial Availability of Navigation Devices and Compatibility Between Cable Systems and Consumer Electronics Equipment, 68 Fed. Reg. 66,728 (Nov. 28, 2003) (to be codified at 47 C.F.R. pt. 15, 76) (incorporating copy-protection requirement into cable plug-and-play standard).

101 *See, e.g.*, Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (2011); Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA), S. 968, 112th Cong. (as amended, May 26, 2011); *SOPA/PIPA: Internet Blacklist Legislation*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/coica-internet-censorship-and-copyright-bill (last visited Mar. 20, 2015).

102 GLOB. NETWORK INITIATIVE, GNI PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY 1-2 (2008), http://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy_0.pdf; *see* MACKINNON, *supra* note 39, at 138-39, 179-82; Jeffrey Rosen, *Google's Gatekeepers*, N.Y. TIMES MAG. (Nov. 28, 2008), http://www.nytimes.com/2008/11/30/magazine/30google-t.html; Jane Spencer & Kevin J. Delaney, *YouTube Unplugged*, WALL ST. J. (Mar. 21, 2008, 11:59 PM), https://www.wsj.com/articles/SB120605651500353307.

103 Kevin Poulsen, *Apple's iPhone Encryption Is a Godsend, Even if Cops Hate It*, WIRED (Oct. 8, 2014, 6:30 AM), http://www.wired.com/2014/10/golden-key; *see* Joseph Cox, *Encryption Is Going Mainstream, but Will People Actually Use It?*, VICE: MOTHERBOARD (Aug. 21, 2014, 8:05 AM), https://motherboard.vice.com/en_us/article/8qx5zp/encryption-is-going-mainstream-but-will-people-use-it; David Meyer, *Why WhatsApp's Encryption Embrace Is a Landmark Event*, FORTUNE (Apr. 5, 2016), http://fortune.com/2016/04/06/whatsapp-encryption-embrace.

have pushed back, arguing that mandatory decryption "back doors" will make the network less secure for everyone.[104] Platforms also have fought for the ability to make public certain basic kinds of information about the many requests that they receive to provide communications data for national security investigations.[105]

At the same time, though, platforms also have engaged in increasing amounts of filtering and interdiction, both for their own purposes and as a strategy for defusing public controversy and forestalling direct regulation. Every major Internet company that hosts user-provided content uses automated filtering technology to prevent the posting of infringing content, and the major payment providers have begun entering agreements with the major copyright trade associations that obligate them to restrict access by entities and sites identified as infringing.[106] Similarly, following its successful campaign against legislated domain-blocking requirements, Google announced that it would begin demoting or removing entirely from search results sites that generate repeated takedown notices.[107] Dominant platform firms also filter and remove a wide variety of other content, including some terrorist-related content, and are always-already poised to expand those initiatives as external events seem to require.[108] Notably,

[104] *See generally* Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. CYBERSECURITY 69 (2015); Bruce Schneier, Opinion, *How to Design — and Defend Against — the Perfect Security Backdoor*, WIRED (Oct. 16, 2013, 9:25 AM), http://www.wired.com/2013/10/how-to-design-and-defend-against-the-perfect-backdoor; Sara Sorcher, *The Battle Between Washington and Silicon Valley Over Encryption*, CHRISTIAN SCI. MONITOR: PASSCODE (July 7, 2015), http://projects.csmonitor.com/cryptowars.

[105] *See generally* Hannah Bloch-Webha, *Process without Procedure: National Security Letters and First Amendment Rights*, 49 SUFFOLK U. L. REV. 367, 376-81 (2016); Rebecca Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, 124 YALE L.J.F. 158 (2014).

[106] *See generally* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81 (2010); Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523 (2015).

[107] *See An Update to Our Search Algorithms*, GOOGLE: INSIDE SEARCH (Aug. 10, 2012), https://search.googleblog.com/2012/08/an-update-to-our-search-algorithms.html; *see also Continued Progress on Fighting Piracy*, GOOGLE: PUB. POL'Y BLOG (Oct. 17, 2014), https://publicpolicy.googleblog.com/2014/10/continued-progress-on-fighting-piracy.html; Adi Robertson, *Google Rolling Out New Search Update to Downrank 'Most Notorious' Pirate Sites*, VERGE (Oct. 17, 2014, 11:55 AM), http://www.theverge.com/2014/10/17/6994249/google-rolling-out-pirate-search-update-report; James Titcomb, *Google and Microsoft Agree Crackdown on Illegal Downloads*, TELEGRAPH (Feb. 20, 2017, 7:29 AM), http://telegraph.co.uk/technology/2017/02/20/google-microsoft-agree-anti-piracy-code-crackdown-illegal-downloads.

[108] *See, e.g.*, Timothy B. Lee, *Facebook Revamps Political-Ad Rules After Discovering*

although the major platforms widely publicize information about the takedown notices they receive from copyright owners and, to the extent permitted, about government production requests, they provide no comparable public transparency about the details of their own automatic filtering and manipulation.

Commentators attempting to evaluate the complex landscape of platform behavior have disagreed about whether to count platforms as civil libertarians, obstructors of justice, or privatized extensions of the surveillance state.[109] I will return to the puzzle of how to connect platform behavior with platform motivation in Part III.D, below; here, my point is more basic and concerns the division of authority to intercept and block information flows. Although the balance of power remains contested and is still evolving, two points seem certain: First, failures on the part of copyright interests and law enforcement to achieve their goals via legislation or litigation most often simply shift struggles over interdiction and control into less visible channels. Second, compromises that involve voluntary filtering shift much day-to-day authority over interdiction of information flows to platforms and at the same time make interdiction decisions more difficult to contest. The "new normal" in the platform economy is a condition in which privatized, fiat-based prohibitions on information flow are both increasingly routine and increasingly opaque.

III. PLATFORMS AND REGULATORY INSTITUTIONS

Many lawyers are familiar with recent high-profile debates over the applicability of existing regulatory obligations to platform companies

Russian Ad Buys, ARS TECHNICA (Sept. 21, 2017, 1:38 PM), https://arstechnica.com/tech-policy/2017/09/facebook-revamps-political-ad-rules-after-discovering-russian-ad-buys; Sam Levin, *Tech Giants Team Up to Fight Extremism Following Cries that They Allow Terrorism*, GUARDIAN (June 26, 2017, 3:24 PM), https://www.theguardian.com/technology/2017/jun/26/google-facebook-counter-terrorism-online-extremism; *How Facebook Guides Moderators on Terrorist Content*, GUARDIAN (May 24, 2017, 1:00 PM), https://www.theguardian.com/news/gallery/2017/may/24/how-facebook-guides-moderators-on-terrorist-content. *See generally* Tarleton Gillespie, *Governance of and by Platforms*, *in* SAGE HANDBOOK OF SOCIAL MEDIA (Jean Burgess et al. eds., forthcoming 2017).

[109] *See, e.g.*, Danielle Keats Citron, *Extremist Speech and Compelled Conformity*, 93 NOTRE DAME L. REV. (forthcoming 2017) (privatized extensions); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. (forthcoming 2017) (civil libertarians); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. (forthcoming 2018) (obstructors). *See generally* ELEC. FRONTIER FOUND., WHO HAS YOUR BACK? PROTECTING YOUR DATA FROM GOVERNMENT REQUEST: SHARING ECONOMY EDITION 3-4 (2016), https://www.eff.org/files/2016/05/04/who-has-your-back-2016.pdf.

— for example, whether Uber is a taxi company, whether and how Amazon.com transactions should be taxed, whether Google or Facebook should be required to remove privacy-invasive or harassing material that is brought to its attention, and so on. Orly Lobel's important work on the regulation of platforms has parsed many of the complexities of these disputes, arguing that the answers to questions about both classification and institutional competence depend importantly on context.[110]

Those debates are important, but participants in them tend to take preexisting institutional features of the legal system for granted, and my project here is different. Platform companies are encountering legal systems worldwide at a time of crisis. Court systems are overburdened, regulatory bureaucracies seem to be forever racing to respond to fast-moving technological and business developments, and new institutions for resolving trade disputes and setting network standards route nimbly around other features of the legal landscape — ranging from conflicting national laws to international human rights mandates and goals — as though they were mere speed bumps. Platform companies did not create any of these situations, but they have proved adept at exploiting them. Their interventions matter precisely because the contours of our regulatory institutions — including not only agencies but also courts and institutional structures for recognizing and vindicating fundamental rights — are not timeless and unchanging.

Powerful economic interests have always sought to reshape jurisdictional, procedural, and methodological rules to their advantage. Legal scholars who study judicial and regulatory processes have shown that institutional design responds over time to the interventions of powerful actors who, in Marc Galanter's framing, are repeat players and can play for rules in addition to results.[111] Well-resourced repeat players also work to craft compelling narratives about the structure of legal institutions, pursuing a species of "deep" capture that operates at the level of ideology.[112] Both projects become easier when the ground is shifting. In their encounters with judicial and

110 *See* Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 117-66 (2016).

111 *See generally* PREVENTING REGULATORY CAPTURE: SPECIAL INTEREST INFLUENCE AND HOW TO LIMIT IT (Daniel Carpenter & David A. Moss eds., 2014); Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 LAW & SOC'Y REV. 95 (1974).

112 *See generally* Jon Hanson & David Yosifon, *The Situation: An Introduction to the Situational Character, Critical Realism, Power Economics, and Deep Capture*, 152 U. PA. L. REV. 129 (2003).

regulatory institutions in the United States and around the world, platform firms and their advocates have labored to minimize their accountability and maximize their scope for self-determination and self-governance. Their interventions have both accelerated and altered the trajectories of institutional evolution.

Processes of institutional realignment also respond to preexisting settlements regarding the distribution of rights, privileges, and other entitlements. As Morton Horwitz demonstrated in his classic study of the evolution of private and commercial law prior to the constitutional battles of the *Lochner* era, such distributive baselines produce deep structuring effects, shaping the framing of disputes about a variety of other matters.[113] So too with informational entitlements and disentitlements. In contests over the legal obligations of platforms, the logics of performative enclosure, appropriative privilege, expressive immunity, and fiat interdiction generate powerful normative force fields, defining some options as the paths of least resistance and foreclosing others entirely.

A. Catch Me If You Can: Platforms in Court

Platforms have developed a suite of powerful strategies for evading accountability in litigation.[114] To some extent, they have benefited from processes of retrenchment that were already underway. Never an ideal vehicle for advancement of mass justice claims, the court system today is overtaxed logistically and under siege ideologically. As consumer products and services and related theories of personal and economic harm have become more complex, numbers of lawsuits and litigants have mushroomed. At the same time, a well-funded movement for "tort reform" has contested attempts to shift liability for complex, highly informationalized harms to the industries whose products and activities are implicated in those harms.[115] Against a backdrop of growing institutional dysfunction, platforms have leveraged the logics of performative enclosure, appropriative privilege,

---

[113] *See* MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW, 1780-1860, at 47-54, 78-97, 116-26, 186-210, 218-26 (1977).

[114] The discussion in this section is adapted from Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535 (2017) [hereinafter Cohen, *Information Privacy Litigation*].

[115] For some different perspectives on what to do about the resulting dysfunctions, see generally GILLIAN K. HADFIELD, RULES FOR A FLAT WORLD: WHY HUMANS INVENTED LAW AND HOW TO REINVENT IT FOR A COMPLEX GLOBAL ECONOMY (2016); Richard A. Nagareda, *Turning from Tort to Administration*, 94 MICH. L. REV. 899 (1996); Judith Resnik, *Managerial Judges*, 96 HARV. L. REV. 374, 421-22 (1982).

and expressive immunity to keep many disputes out of the court system entirely, to ensure that others are soon dismissed, and to minimize the operational impact of the few that proceed to judgment.

Many lawsuits against platform firms allege information privacy harms. Such lawsuits are part of a more general trend in the contemporary litigation landscape. New class complaints alleging information privacy and data security violations are filed seemingly every few weeks and have become enormously controversial. Large information businesses and defense counsel bemoan the purported threats to corporate bottom lines and to processes of information-based "innovation" more generally.[116]

At least in the case of lawsuits against platform firms, however, those worries are largely unfounded. A constellation of rules covering everything from waiver of judicial process to standing to the proper approaches to structuring class claims and remedies works systematically to blunt their impact. Those results flow partly from more general changes in the class action litigation landscape. Like contemporary mass tort claims, most information privacy claims against large information businesses are funneled into procedurally opaque multidistrict litigation proceedings, and most suits settle while still in the preliminary stages, so that even a certification decision is made in the context of a motion to certify a settlement class.[117] Platforms, however, have begun to seem uniquely untouchable.

---

[116] *See, e.g.*, Brief of the Coal. for Sensible Pub. Records Access et al. as Amici Curiae in Support of Petitioner at 1-2, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339) ("As a result [of the decision below], amici's members — some of whom supply lending, insurance or transactional information, or facilitate residential real estate purchases — face increased costs of doing business and are significantly less willing to bear risk and to innovate, to the ultimate detriment of all consumers and the economy."); Brief for Amici Curiae Ebay Inc. et al. in Support of Petitioner at 23-24, *Spokeo*, 136 S. Ct. 1540 (No. 13-1339) ("Perversely, the primary consequences of the expensive litigation and resulting *in terrorem* settlements of these no-injury controversies are the diversion of resources away from technology companies' efforts to develop and provide increasingly innovative services and products to the users who often comprise the putative classes in these cases."); Brief of Trans Union LLC as Amicus Curiae in Support of Petitioner at 2, *Spokeo*, 136 S. Ct. 1540 (No. 13-1339) ("If this Court does not grant the petition for certiorari and correct the Ninth Circuit's error, then the immediate result will be more 'bet the company' litigation filed under the [Fair Credit Reporting] Act," inevitably reducing innovation in new data services and diminishing "the scope of predictive information available to credit grantors to manage risk"); *see also* Larry Downes, *A Rational Response to the Privacy "Crisis,"* CATO INST. POL'Y ANALYSIS, Jan. 7, 2013, at 1-2, 16, https://object.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf.

[117] *See, e.g.*, *In re* LinkedIn User Privacy Litig., 309 F.R.D. 573, 584 (N.D. Cal. 2015); *In re* Google Referrer Header Privacy Litig., No. 5:10-cv-04809 EJD, 2014 WL

To begin with, platform firms enjoy an especially privileged position from which to exploit the relational turn in litigation avoidance. In a wide variety of contexts ranging from employment contracts to service contracts to one-off consumer transactions, courts have become more and more willing to require enforcement of boilerplate clauses requiring arbitration of disputes and waiver of the right to bring class claims — and, as a result of that stance, the use of such clauses is becoming increasingly widespread.[118] Platform firms have taken full advantage of this trend, incorporating litigation avoidance provisions into their terms of service and thus — via the logic of performative enclosure — into the core of the access-for-data bargain.[119] As platforms intermediate users' networked lives more and more completely, such provisions have become both unavoidable and far-reaching.

A second avenue for disposing of information privacy litigation against platform firms involves standing to sue. Plaintiffs asserting intangible harms often have difficulty establishing the requisite injury.[120] The logic of appropriative privilege gives platforms a leg up

1266091, at *2-4 (N.D. Cal. Mar. 26, 2014); *In re* Netflix Privacy Litig., No. 5:11-CV-00379 EJD, 2012 WL 2598819, at *2-4 (N.D. Cal. July 5, 2012). *See generally* Elizabeth Chamblee Burch, *Judging Multidistrict Litigation*, 90 N.Y.U. L. REV. 71 (2015); J. Maria Glover, *Mass Litigation Governance in the Post-Class Action Era: The Problems and Promise of Non-Removable State Actions in Multi-District Litigation*, 5 J. TORT L. 1 (2014).

[118] *See, e.g.*, DIRECTV, Inc. v. Imburgia, 136 S. Ct. 463, 469-71 (2015); Am. Express Co. v. Italian Colors Rest., 133 S. Ct. 2304, 2309 (2013); Nitro-Lift Techs., L.L.C. v. Howard, 568 U.S. 17, 20-21 (2012); Marmet Health Care Ctr., Inc. v. Brown, 565 U.S. 530, 532-34 (2012); CompuCredit Corp. v. Greenwood, 565 U.S. 95, 102 (2012); AT&T Mobility LLC v. Concepcion, 563 U.S. 333, 352 (2011); *see also* Myriam Gilles, *The Day Doctrine Died: Private Arbitration and the End of Law*, 2016 U. ILL. L. REV. 371, 400-09 (2016); Jean R. Sternlight, *Disarming Employees: How American Employers Are Using Mandatory Arbitration to Deprive Workers of Legal Protection*, 80 BROOK. L. REV. 1309, 1310 n.9, 1344-45 (2015). *See generally* J. Maria Glover, *Disappearing Claims and the Erosion of Substantive Law*, 124 YALE L.J. 3052 (2015).

[119] *See* Amy J. Schmitz, *Consumer Redress in the United States*, *in* THE NEW REGULATORY FRAMEWORK FOR CONSUMER DISPUTE RESOLUTION 325, 327-30, 336-38 (Pablo Cortés ed., 2016); Myriam Gilles, *Killing Them with Kindness: Examining "Consumer-Friendly" Arbitration Clauses After* AT&T Mobility v. Concepcion, 88 NOTRE DAME L. REV. 825, 850-61 (2012); *The Gig Economy: Using Mandatory Arbitration Agreements with Class Action Waivers*, FISHER PHILLIPS (May 1, 2017), https://www.fisherphillips.com/pp/publication-the-gig-economy-using-mandatory-arbitration-agreements.pdf; *see also* Stephanie Strom, *When 'Liking' a Brand Online Voids the Right to Sue*, N.Y. TIMES (Apr. 16, 2014), https://nyti.ms/1l9uZ5R (discussing corporations' attempts to require mandatory arbitration through platforms).

[120] *See generally* Cohen, *Information Privacy Litigation*, *supra* note 114; Seth F.

in disputes about injuries allegedly flowing from their collection and use of personal information. Within the Hohfeldian framework, the correlative of an entitlement that takes the form of a privilege is no right to object to the conduct that the privilege protects. Defendants in information privacy litigation understand that relationship well and have labored tirelessly to convince courts of its inevitability, framing acts of information collection and use as routine background conditions that create no cognizable injury.[121] Information privacy claims, they argue, are really no more than generalized claims about the perceived unfairness of economic and technological processes that people have not yet learned to accept. The argument reliably gets results; many information privacy claims are dismissed quickly on standing grounds and the Supreme Court has signaled its implicit support for that approach.[122]

Other lawsuits against platform firms allege harms suffered as a result of information initially furnished by third parties but made more salient through the involvement of platform-based intermediation. In these suits, platforms benefit from the logic of expressive immunity described in Part II.C above. In contexts involving alleged defamation and similar harms, courts have

Kreimer, *"Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745 (2016).

[121] *See, e.g.*, Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995) ("[A] single, random cardholder's name has little or no intrinsic value to defendants (or a merchant). Rather, an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names."); Brief for Experian Info. Sols., Inc., as Amicus Curiae Supporting Petitioners at 1-2, First Am. Fin. Corp. v. Edwards, 567 U.S. 756 (2012) (No. 10-708) ("Such suits are possible because the [Fair Credit Reporting] Act permits plaintiffs to sue for . . . what may be a wholly technical violation. Indeed, it is not uncommon in these cases for significant numbers of class members to have actually *benefited* from the alleged violations."); Brief of Trans Union LLC as Amicus Curiae in Support of Petitioner at 19, Spokeo v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339) ("It is rare for a single item, inaccurate in a small detail, to actually result in a denial of credit."); James C. Cooper, *Opinion: Why the Supreme Court Should Side with Data Brokers*, CHRISTIAN SCI. MONITOR (Nov. 2, 2015), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1102/Opinion-Why-the-Supreme-Court-should-side-with-data-brokers.

[122] *See Spokeo*, 136 S. Ct. at 1548 (ruling in the context of a class action for statutory damages for violation of the Fair Credit Reporting Act that even when Congress has defined a cause of action and provided a remedy, an individual plaintiff still must show adverse consequences that are sufficiently concrete); *see also* Michael Wolgin, *"Concrete" Disparities in Article III Case Law After* Spokeo, CLASS ACTIONS & DERIVATIVE SUITS, Winter 2017, at 4 (providing overview of post-*Spokeo* split among lower courts on what must be shown to establish concreteness).

interpreted the statutory immunity for online intermediaries broadly, eliminating not only traditional publisher liability but also distributor liability for intermediaries possessing knowledge of ongoing harm.[123] In addition, because the statutory language sweeps well beyond defamation in ways that implicate many other types of expressive conduct, it has supplied defenses in many — though not all — lawsuits alleging a wide variety of other harms ranging from discrimination to market manipulation.[124] Although some commentators have questioned whether Congress really intended to grant such broad insulation to a business model whose shape was still unknown, others have criticized the current regime because it does not yield dismissals quickly enough.[125]

Of the handful of lawsuits that survive these initial obstacles — often claims for violation of sector-specific privacy statutes that prescribe particular procedures and provide statutory damages for noncompliance — many confront additional hurdles flowing from the opaque, technically arcane character of platform-based intermediation and from the logic of performative enclosure, which operates to shelter the technical details from discovery. Interactions involving

[123] *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 330-34 (4th Cir. 1997) (barring a defamation claim against AOL.com for its delay in removing defamatory posts about the plaintiff on an AOL bulletin board); Murawski v. Pataki, 514 F. Supp. 2d 577, 591 (S.D.N.Y. 2007) (barring a libel claim against Ask.com for displaying a website with allegedly defamatory statements about plaintiff in its search results); Parker v. Google, Inc., 422 F. Supp. 2d 492, 500-01 (E.D. Pa. 2006) (barring a defamation claim against Google for archiving websites containing defamatory statements about the plaintiff in its cache). For comparison with the traditional formulation of defamation liability, see RESTATEMENT (SECOND) OF TORTS § 558 (AM. LAW INST. 1977) (imposing liability on anyone who negligently or intentionally publishes defamatory information about another); *id.* § 577 (defining publication broadly as intentional or negligent communication of defamatory material to any third party, and imposing liability on those who "intentionally and unreasonably" fail to remove defamatory statements from their land or chattels); *id.* § 578 (holding re-publishers liable to the same degree as the original publisher); *id.* § 581 (imposing liability on a distributor of a defamatory statement only if the distributor "knows or has reason to know of its defamatory character," but treating television and radio broadcasters as though they were original publishers).

[124] For reviews of the case law, see generally David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373 (2010) (finding that roughly one-third of litigated cases survived the assertion of CDA 230 defenses); Jeff Kosseff, *The Gradual Erosion of the Law that Shaped the Internet: Section 230's Evolution over Two Decades*, 18 COLUM. SCI. & TECH. L. REV. 1 (2016) (describing a suite of emerging, judicially-developed limitations on the scope of CDA 230 immunity).

[125] *See, e.g.*, Jane R. Bambauer & Derek E. Bambauer, *Vanished*, 18 VA. J.L. & TECH. 137, 141-43 (2013).

consumers' personally identifying information often are embedded deeply within the operating protocols of a mobile phone platforms or web browser, and may involve complex commercial relationships among multiple players in platforms' cross-licensing ecologies. That complexity and opacity enable platform firms to argue that the methods proposed for ascertaining classes of affected consumers are too imprecise.[126] Courts reject some of these ascertainability challenges, but they also routinely decline requests to certify classes consisting of all consumers affected by the challenged activity.[127] They also have been reluctant to craft discovery orders broad enough to enable plaintiffs' counsel to understand the challenged patterns of information flow.[128]

Even the rare lawsuits against platform firms that yield seven-figure class payouts have relatively little effect on platform information processing practices. Consider two examples: In 2010, Facebook agreed to pay $9.5 million to settle class claims resulting from its Beacon service, which had automatically repurposed user posts intended only for limited circulation as advertising for the products and services that users happened to mention; in 2011, Google paid $8.5 million to settle claims arising from the rollout of its Google Buzz social networking service, which used users' Gmail contacts to populate their publicly visible profiles.[129] Both awards received

[126] In most circuits, a putative class plaintiff must prove that a proposed class is both sufficiently numerous to warrant class-based adjudication and sufficiently definite that its membership is ascertainable. *See* FED. R. CIV. P. 23(a)(1)-(3); Marcus v. BMW of North Am., LLC, 687 F.3d 583, 592-93 (3d Cir. 2012). *But see* Mullins v. Direct Dig., LLC, 795 F.3d 654, 657-58 (7th Cir. 2015) ("Nothing in Rule 23 mentions or implies this heightened requirement under Rule 23(b)(3), which has the effect of skewing the balance that district courts must strike when deciding whether to certify classes.")

[127] *See, e.g.*, Opperman v. Path, Inc., No. 13-cv-00453-JST, 2016 U.S. Dist. LEXIS 92403, at *8 (N.D. Cal. July 15, 2016) (declining to certify class of all users of the invasive versions of Path's software and instead limiting class to those registered as users during four-month period in which the software downloaded iDevice Contacts from all users); *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016) (limiting class to those consumers who had already paid for credit monitoring or stated that they had expended personal time on credit monitoring); *In re* Hulu Privacy Litig., No. C 11–03764 LB, 2014 WL 2758598, at *14 (N.D. Cal. June 17, 2014) (denying without prejudice motion to certify class of "users of both Facebook and Hulu during the class period" and suggesting possible methods of defining subclasses based on variables such as whether users remained logged in and whether and how they cleared cookies).

[128] *See* Campbell v. Facebook Inc., No. 13-CV-05996-PJH, 2016 WL 7888026, at *1-2 (N.D. Cal. Oct. 14, 2016).

[129] *See* Damon Darlin, *Google Settles Suit over Buzz and Privacy*, N.Y. TIMES (Nov. 3,

widespread media coverage and seemed large in absolute terms, but they were minimal relative to the number of individuals affected and more minimal still when measured against the profits resulting from the challenged activity.[130] Both awards, moreover, accompanied agreements in which the platform firms promised to do more to educate consumers about their practices and to redesign their procedures for obtaining consent, but not to halt the challenged practices entirely. Settlements such as these are widely regarded as having produced almost no meaningful change in business practices relating to the collection, processing, and exchange of consumer personal information. Suits against information platforms under other kinds of statutes — for example, class actions by Uber passengers alleging deceptive safety-related marketing and by Uber drivers alleging that they are employees entitled to reimbursement for fuel and maintenance expenses — have begun to follow similar patterns.[131]

Copyright infringement lawsuits are a partial exception to these stories of displacement, deflection, and minimization of claims of platform-related injury. Platforms have won many of the reported cases, but those victories have not come quickly or easily. Instead, litigation over such matters as the adequacy of takedown procedures, the triggers for indirect infringement liability, and the interplay between indirect infringement theories and the statutory safe harbors has required courts to explore and evaluate platform operations in detail.[132] In light of the discussion in Part II.D, above, that should

2010, 12:19 AM), https://nyti.ms/2sOTSNJ; Miguel Helft, *Critics Say Google Invades Privacy with New Service*, N.Y. TIMES (Feb. 12, 2010), https://nyti.ms/2k8g2Gg; David Kravets, *Judge Approves $9.5 Million Facebook 'Beacon' Award*, WIRED (Mar. 17, 2010, 2:18 PM), https://www.wired.com/2010/03/facebook-beacon-2; Ryan Singel, *Facebook Beacon Tracking Program Draws Privacy Lawsuit*, WIRED (Aug. 14, 2008, 1:48 PM), https://www.wired.com/2008/08/facebook-beacon.

130 For discussion of this point and detailed analysis of several recent settlements, see generally Marc Rotenberg & David Jacobs, *Enforcing Privacy Rights: Class Action Litigation and the Challenge of* Cy Pres, *in* ENFORCING PRIVACY (David Wright & Paul De Hert eds., 2015). To similar effect, remedial orders resolving class claims for injunctive or declaratory relief tend to be very narrowly drawn. *See, e.g.*, *In re* Yahoo Mail Litig., 308 F.R.D. 577, 601 (N.D. Cal. 2015); David Kravets, *The Most Absurd Internet Privacy Class-Action Settlement Ever*, ARS TECHNICA (Aug. 30, 2016, 11:55 AM), https://arstechnica.com/tech-policy/2016/08/the-most-absurd-internet-privacy-class-action-settlement-ever.

131 *See* Sam Levin, *Uber Lawsuits Timeline: Company Ordered to Pay Out $161.9m Since 2009*, GUARDIAN (Apr. 13, 2016, 7:00 AM), https://www.theguardian.com/technology/2016/apr/13/uber-lawsuits-619-million-ride-hailing-app; *Uber Lawsuit Settlement*, CLASSACTION.COM, https://www.classaction.com/uber/settlement/#uber-settlements (last visited June 7, 2017).

132 *See, e.g.*, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913

come as no particular surprise; the balance of power between platform firms and the major copyright industries is still evolving. Even here, however, the trajectory has begun to bend away from the courts. Copyright litigation between the major industry players can be prolonged and expensive — litigation between Viacom and Google over infringing videos on YouTube dragged on for seven years — and both sides face considerable downside risk.[133] And so it also should come as no particular surprise that major litigation between platforms and copyright interests has become much rarer and compromises based on platform self-regulation more common.

B. Now You See Me, Now You Don't: Platforms and the Administrative State

Platforms have developed equally powerful strategies for avoiding regulatory accountability. Like the courts, the administrative state — still comprised principally of models and constructs developed in the context of the industrial economy — is poorly equipped to address the challenges now confronting it.[134] Platforms have proved adept both at practicing regulatory arbitrage and at resisting or coopting attempts to extend new kinds of regulatory oversight to their core information processing operations. As before, they have leveraged the logics of performative enclosure, productive appropriation, and expressive immunity and the distributive baselines suggested by those logics to ensure that their operations have remained largely invisible to regulatory oversight.

Some of the most visible and heated disputes about platforms and the administrative state are the least complicated. For example, regimes regulating labor and transportation employ definitional gateways — e.g., "employer" and "employee" or "taxi" and "limousine" — to determine which entities are subject to their

(2005); UMG Recordings, Inc. v. Shelter Capital Partners, LLC, 718 F.3d 1006 (9th Cir. 2013); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012); Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788 (9th Cir. 2007); CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544 (4th Cir. 2004); Field v. Google, 412 F. Supp. 2d 1106 (D. Nev. 2006); Hendrickson v. Amazon.com, Inc., 298 F. Supp. 2d 914 (C.D. Cal. 2003).

133 *See* Joe Silver, *Viacom and Google Settle $1 Billion YouTube Lawsuit*, ARS TECHNICA (Mar. 18, 2014, 8:54 AM), https://arstechnica.com/tech-policy/2014/03/viacom-and-google-reach-settlement-in-long-running-youtube-lawsuit.

134 The discussion in this section is adapted from Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRES L. 369, 371 (2016).

requirements.[135] High-profile, platform-based "disruptors" of existing work arrangements — including labor-matching sites like Mechanical Turk and TaskRabbit and transportation-matching sites like Uber and Lyft — argue that such regimes do not apply to them. Calling themselves information businesses rather than, for example, temporary employment agencies or transportation businesses, they insist that, except for the people they hire to write their code and conduct their government relations operations, they do not actually employ anyone. Their true business, they argue, is innovation; they are simply bringing surplus production capacity online and into a new, freelancer-driven economy that is nimbler, more cost-effective, and less impersonal.[136] In some ways, that characterization is accurate; platforms recruit user-workers into arrangements that are styled as licenses to access the platform's resources. As critics have detailed, however, provisions in those licenses cover matters more commonly addressed in employment agreements.[137] And platforms' self-interested description of their operations is incomplete; they are also structures for converting the labor of user-workers and their customers into flows of monetizable data and finance capital. The logics of performative enclosure, productive appropriation, and expressive immunity work to make these functions seem both less salient and less important from a regulatory standpoint.

Platforms also benefit from other kinds of regulatory arbitrage that are potentially far more intractable, because they involve divisions of authority that are baked into the structure of the modern administrative state. The point is most usefully illustrated with an extended example involving the ongoing dispute over whether to impose a mandate of "net neutrality" — the obligation to "treat all content, sites, and platforms equally"[138] — on broadband Internet access providers. Regulatory authority over the group of actors whose actions shape the neutrality or non-neutrality of networked

---

135 *See, e.g.*, Fair Labor Standards Act of 1938, 29 U.S.C. § 203 (2012) ("employer" and "employee"); D.C. Mun. Regs. tit. 31, § 9901 (2017) ("taxicab" and "black car"); N.Y.C., N.Y., Admin. Code § 19-502 (2014) ("taxi" and "black car").

136 *See, e.g.*, Lobel, *supra* note 110, at 96-101; Steven Hill, *Uber and Lyft's Big New Lie: Their Excuse for Avoiding Regulation Is Finally Falling Apart*, SALON (Jan. 16, 2016, 12:59 PM), http://www.salon.com/2016/01/16/uber_and_lyfts_big_new_lie_their_excuse_for_avoiding_regulation_is_finally_falling_apart.

137 *See* Valerio De Stefano, *The Rise of the "Just-in-Time" Workforce: On-Demand Work, Crowdwork, and Labor Protection in the "Gig-Economy*," 37 COMP. LAB. L. & POL'Y J. 471, 485-89 (2016).

138 Tim Wu, *Network Neutrality FAQ*, TIMWU.ORG, http://www.timwu.org/network_neutrality.html (last visited Oct. 26, 2015).

information environments is both hobbled by outdated legislative framing and fragmented by obsolete institutional design.

Important aspects of the net neutrality dispute are artifacts of outdated statutory grants of authority. The last set of major amendments to the statutory framework granting the Federal Communications Commission ("FCC") authority to regulate "telecommunications" dates from 1996, a year in which Internet services were still-emergent and not yet understood as central components of modern communications architecture and policy.[139] Initially, the FCC classified cable broadband services as information services under the statute, but after the D.C. Circuit ruled that the statute did not permit imposition of nondiscrimination obligations on such services and invalidated an initial set of net neutrality rules, it recharacterized broadband Internet access providers as common carriers subject to regulation under a different title of the statute and then issued new rules.[140] The parts of the statute that regulate designated common carriers, however, were designed for basic telephone service; common carriers must route all calls to their destinations without blocking or playing favorites.[141] The telephone-based communications paradigm is too narrow to encompass all of the service-related questions that digital networked communications raise. Internet access providers routinely engage in traffic management for a diverse set of purposes ranging from network optimization to spam control to network security, and some network uses require higher bandwidth than others. Commercial Internet access providers typically have defined tiers of pricing based on network speed and data usage rather than on the services consumers plan to use, but also have experimented by selectively slowing or prioritizing traffic in ways that serve their own narrower interests.[142] Net neutrality regulation takes

[139] *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified as amended in scattered sections of 18 U.S.C. & 47 U.S.C.).

[140] *See* Verizon v. FCC, 740 F.3d 623, 628 (D.C. Cir. 2014) (invalidating the antiblocking and nondiscrimination rules in *In re* Preserving the Open Internet, 25 F.C.C.R. 17905 (2010)); Protecting and Promoting the Open Internet, 80 Fed. Reg. 19,738, 19,738 (Apr. 13, 2015) (to be codified at 47 C.F.R. pt. 1, 8, & 20). As of this writing, the Trump-era FCC is poised to reverse the 2015 rules if it can.

[141] *See* 47 U.S.C. §§ 201(a), 202(a) (2012).

[142] *See, e.g.*, Ingrid Burrington, *How Mobile Carriers Skirt Net-Neutrality Rules*, ATLANTIC (Dec. 18, 2015), https://www.theatlantic.com/technology/archive/2015/12/not-everyone-can-use-the-cloud-equally/421209; Adam Liptak, *Verizon Blocks Messages of Abortion Rights Group*, N.Y. TIMES (Sept. 27, 2007), https://nyti.ms/2nDEKE4; John D. McKinnon & Thomas Gryta, *YouTube Says T-Mobile Is Throttling Its Video Traffic*, WALL ST. J. (Dec. 22, 2015, 5:02 PM), https://www.wsj.com/articles/youtube-says-t-mobile-is-throttling-its-

aim at the latter sort of conduct, but needs to say something about the former sort and to provide guidelines for distinguishing between the two. The statute provides no help, and the complexity of the project multiplies opportunities for rent-seeking.

The topic of net neutrality also intersects with questions about both justifiable price discrimination and required public provision of essential services in ways that allow the logics of performative enclosure and productive appropriation to find points of entry. From the Internet access provider's perspective, the ability to discriminate among different types of network traffic facilitates efforts to assert control over the collection and use of personally identifying information about subscribers and their online activities. The logics of performative enclosure and productive appropriation reinforce arguments framing such discrimination as a business necessity. With regard to essential services, the FCC has long overseen a program to offer "lifeline" telephone service to the poorest consumers, and more recently oversaw development of a parallel "essentials" program for basic broadband Internet access.[143] At least some wireless Internet providers, however, would prefer to handle the essential-services problem via the practice of zero rating, in which usage of a designated suite of applications is not counted for billing purposes. Such arrangements — which, from the provider perspective, represent a permutation of the access-for-data bargain — are more affordable, but they are not neutral.[144] The telephone-based communications

video-traffic-1450821730; Kevin J. O'Brien, *Putting the Brakes on Web-Surfing Speeds*, N.Y. TIMES (Nov. 13, 2011), https://nyti.ms/2sOOvyb; Shalini Ramachandran, *Netflix to Pay Comcast for Smoother Streaming*, WALL ST. J. (Feb. 23, 2014, 7:47 PM), https://www.wsj.com/articles/netflix-agrees-to-pay-comcast-to-improve-its-streaming-1393175346; Peter Svensson, *Comcast Blocks Some Internet Traffic*, WASH. POST (Oct. 19, 2007, 6:32 PM), http://www.washingtonpost.com/wp-dyn/content/article/2007/10/19/AR2007101900842.html; *Why Free Can Be a Problem on the Internet*, N.Y. TIMES (Nov. 14, 2015), https://nyti.ms/1kVnEw4; Edward Wyatt, *AT&T Accused of Deceiving Smartphone Customers with Unlimited Data Plans*, N.Y. TIMES (Oct. 28, 2014), https://nyti.ms/ZYXrSz.

143 *See* 47 C.F.R. §§ 54.101-54.1310 (2016); FED. COMMC'N COMM'N, LIFELINE AND LINK UP REFORM AND MODERNIZATION 2-4 (2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-38A1.pdf. *But see* Press Release, Ajit Pai, FCC Chairman, On the Future of Broadband in the Lifeline Program (Mar. 29, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DOC-344129A1.pdf (asserting that states have principal responsibility for designating providers).

144 *See In re* Wireless Telecomms. Bureau Policy Report, 32 FCC Rcd. 1093 (2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0203/DA-17-127A1.pdf; FED. COMMC'N COMM'N, WIRELESS TELECOMMS. BUREAU, POLICY REVIEW OF MOBILE BROADBAND OPERATORS' SPONSORED DATA OFFERINGS FOR ZERO RATED CONTENT AND SERVICES (2017), https://www.fcc.gov/document/release-report-policy-review-mobile-zero-rating-practices; Klint Finley, *The FCC OK's Streaming for Free — but Net Neutrality Will Pay*,

paradigm also does not easily encompass these types of questions. An ideal enabling statute for the modern FCC would acknowledge the full range of considerations that attend the provision of Internet access and provide guidance on how to weigh them.

More fundamentally still, the current regulatory structure does not permit any regulator to consider the full group of actors whose activities determine the neutrality or nonneutrality of access to networked digital communications capabilities. The FCC-issued rules applied straightforwardly to broadband and wireless Internet providers, with some exceptions for certain voice-over-Internet services, and not at all to platforms like Facebook and Twitter that do not provide Internet access.[145] If the question is whether an entity provides telecommunications services of the general sort contemplated by Congress in the most recent iteration of the statute, those distinctions may make sense; if the question is whether platforms' self-interested mediation of the networked information environment ought to be subject to some basic nondiscrimination obligations, they seem both arbitrary and laughable. Platforms and their government relations firms have exploited the apparent unfairness; for example, Google has adopted the posture of a supplicant seeking nondiscriminatory access to connection points for its Google Fiber initiative, even though it and other dominant platform firms "already benefit from what are essentially internet fast lanes, and this has been the case for years."[146] Proposals to create a regulatory authority empowered to impose comparable neutrality obligations on search providers, meanwhile,

WIRED (Feb. 3, 2017), https://www.wired.com/2017/02/fcc-oks-streaming-free-net-neutrality-will-pay. *See generally* Arturo J. Carrillo, *Having Your Cake and Eating It Too? Zero-Rating, Net Neutrality, and International Law*, 19 STAN. TECH. L. REV. 364 (2016).

[145] *See* 47 C.F.R. §§ 8.2-8.11 (2016); *see also* Protecting and Promoting the Open Internet, 80 Fed. Reg. 19,738, 19,741-42 (Apr. 13, 2015) (to be codified at 47 C.F.R. pt. 1, 8, & 20) ("The open Internet rules described above apply to both fixed and mobile broadband Internet access service . . . . This Order [also] recognizes that some data services — like facilities-based VoIP offerings, heart monitors, or energy consumption sensors — may be offered by a broadband provider but . . . are not broadband Internet access service.").

[146] Robert McMillan, *What Everyone Gets Wrong in the Debate over Net Neutrality*, WIRED (June 23, 2014), https://www.wired.com/2014/06/net_neutrality_missing; *see* Alistair Barr, *Google Strikes an Upbeat Note with FCC on Title II*, WALL ST. J. (Dec. 31, 2014, 4:12 PM), https://blogs.wsj.com/digits/2014/12/31/google-strikes-an-upbeat-note-with-fcc-on-title-ii. *See generally* Letter from Austin C. Schlick, Dir. of Commc'ns Law, Google, to Marlene H. Dortch, Sec'y, FCC (Dec. 30, 2014), https://ecfsapi.fcc.gov/file/100319291940/2016-10-03%20Google%20Letter%20(WC%2016-106).pdf; Ryan Singel, *Now That It's in the Broadband Game, Google Flip-Flops on Network Neutrality*, WIRED (July 30, 2013), https://www.wired.com/2013/07/google-neutrality.

have drawn criticism from commentators all along the political spectrum.[147]

A final group of problems involves platform conduct that is simply intractable using conventional regulatory methodologies. Debates about the need for antitrust oversight of platform-based environments are one example. As we saw in Part I, the economics of two-sided markets differ in important ways from those of traditional, one-sided markets. Because platforms can define terms for each user group separately, pricing is not a reliable sign of market power in two-sided markets, and secondary heuristics such as the competition regulator's basic distinction between horizontal and vertical integration strategies also do not translate well to the platform-based environment. The complexity and opacity of platform-based, massively-intermediated exchange structures have stymied courts and policymakers used to working with more traditional economic models.[148] Competition regulators in the European Union, who have tangled more aggressively with the dominant platform firms, have made more progress toward developing new methodologies for determining when platform-related advantages ripen into market harms.[149]

---

[147] *See generally* Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008); Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697 (2010); James Grimmelmann, *Don't Censor Search*, 117 YALE L.J. POCKET PART 48 (2007), http://www.yalelawjournal.org/forum/dont-censor-search (arguing against the regulation of search providers); Berin Szoka, *First Amendment Protection of Search Algorithms as Editorial Discretion*, TECH. LIBERATION FRONT (June 4, 2009), https://techliberation.com/2009/06/04/first-amendment-protection-of-search-algorithms-as-editorial-discretion (arguing that because search providers are public companies they should be subject to public regulations). *But see* Frank Pasquale, *Dominant Search Engines: An Essential Cultural & Political Facility*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 401, 401-02 (Berin Szoka & Adam Marcus eds., 2010) ("I now see that [our article,] *Federal Search Commission*, like many other parts of the search engine accountability literature, tried too hard to shoehorn a wide variety of social concerns about search engines into the economic language of antitrust policy. It is now time for scholars and activists to move beyond the crabbed vocabulary of competition law to develop a richer normative critique of search engine dominance.").

[148] For discussions of the difficulties that attend antitrust modeling of two- and multi-sided markets and reviews of the literature, see generally Evans & Schmalensee, *supra* note 32; Khan, *supra* note 33; Rochet & Tirole, *supra* note 32.

[149] *See, e.g.*, Press Release, European Comm'n, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 27, 2017), http://europa.eu/rapid/press-release_IP-17-1784_en.htm; Daniel Boffey, *Google Fined Record €2.4bn by EU over Search Results*, GUARDIAN (June 27, 2017), https://www.nytimes.com/2017/06/23/technology/gmail-ads.html?mcubz=3. *See generally* Martens, *supra* note 35.

An even thornier example of methodological intractability involves rules intended to ensure that flows of information about the goods, services, and capabilities on offer are accurate and unbiased — for example, rules for consumer protection and investor protection and rules prohibiting invidious discrimination in employment, finance, and housing markets. Such rules are premised on the assumptions that information is scarce and costly to obtain and convey, and that regulatory mandates therefore can produce meaningful changes in the nature and quality of information available to or about market participants. The platform-based environment, however, is characterized by both information abundance and endemic information asymmetry. Those conditions make information-forcing rules easy to manipulate and information-blocking rules easy to evade. For example, to enforce existing antidiscrimination laws effectively, the various agencies with enforcement authority need the ability to detect and prove discrimination, yet that task is increasingly difficult when decisions about lending, employment, and housing are made via complex algorithms used to detect patterns in masses of data and the data itself reflects preexisting patterns of inequality.[150] Consumer protection regulators typically seek both to require disclosure of material information and to prevent marketing practices that are unfair or deceptive, but within platform environments, consumer awareness is easy to manipulate more directly, and many goods and services are amenable to versioning using price discrimination frameworks designed to appeal to what is known or inferred about consumer preferences.[151]

These are genuinely difficult problems; the existing regulatory toolkit is poorly adapted for scrutinizing algorithmic models and methods, and the techniques for machine learning and artificial intelligence on which platforms increasingly rely are even less amenable to explanation and oversight.[152] But encounters between

[150] *See generally* Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016).

[151] *See generally* Hal R. Varian, *Versioning Information Goods*, *in* INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL INFORMATION AND INTELLECTUAL PROPERTY 190 (Brian Kahin & Hal R. Varian eds., 2000); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Andrew D. Gershoff, Ran Kivetz & Anat Keinan, *Consumer Response to Versioning: How Brands' Production Methods Affect Perceptions of Unfairness*, 39 J. CONSUMER RES. 382 (2012); Lauren Willis, *Performance-Based Consumer Regulation*, 82 U. CHI. L. REV. 1309, 1321-26 (2015) (summarizing research on consumer manipulation).

[152] *See generally* Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669 (2010); Danielle Keats Citron & Frank

platforms and regulators also have been profoundly shaped by tacit understandings of the baseline entitlements that platforms enjoy. According to the logic of productive appropriation, it makes sense that unfettered information processing should be the default and restrictions the exception. According to the logics of performative enclosure and expressive immunity, the idea of accountability for modern "information laboratories" is easy to frame as unjust and its advocates as petulant whiners.[153] These now-habitual ways of framing regulatory discussion militate in favor of governance according to voluntary, "best practice" standards and diminish the incentive to develop new and appropriately rigorous methods of public oversight.[154]

C. Your Laws Have No Meaning Here: Platforms and Fundamental Rights

For some commentators on the emerging platform economy, the prospect of continued and ever more severe regulatory destabilization is a joyous one — a necessary period of disruption en route to a more perfectly free (and substantially deregulated) digital future. Although many digital entrepreneurs and pundits self-identify as iconoclasts, that view of the digital networked world has become their own version of conventional and unquestioned wisdom. Writing at the dawn of the digital era, self-appointed cyber-philosopher John Perry Barlow proclaimed cyberspace to be a new domain of pure freedom. Addressing the nations of the world, he proclaimed: "Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."[155] In the era of the platform, that statement has proved

Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014); Cary Coglianese & Jennifer Nash, *The Law of the Test: Performance-Based Regulation and Diesel Emissions Control*, 34 YALE J. ON REG. 33 (2017); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017).

153 *See, e.g.*, Larry Downes, *A Rational Response to the Privacy "Crisis,"* CATO INST. POL'Y ANALYSIS, Jan. 7, 2013, at 1, http://www.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf; Berin Szoka & Adam Thierer, *Targeted Online Advertising: What's the Harm and Where Are We Heading?*, PROGRESS ON POINT, June 2009, at 1, http://www.pff.org/issues-pubs/pops/2009/pop16.2targetonlinead.pdf.

154 *See generally* Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543 (2000); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342 (2004); David Zaring, *Best Practices*, 81 N.Y.U. L. REV. 294 (2006).

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

prescient in a way that Barlow perhaps did not intend. The "legal concepts" that increasingly have no meaning in online environments include the guarantees that supposedly protect the fundamental rights of Internet users, including the expressive and associational freedoms whose supremacy Barlow asserted.

Within domestic and international discourses about fundamental rights, the paradigmatic legal guarantees are those that bind sovereign states in their dealings with their own citizens. State-centered conceptions of protection and enforceability sit uneasily alongside a reality in which flows of information to, from, and about network users are intermediated by privately owned and operated information platforms, and in which those flows as a practical matter define those individuals' expressive, associational, and commercial experiences and opportunities.

Concern about the unaccountability of private economic power is a longstanding theme within human rights scholarship and activism. In 2008, the United Nations Secretary-General appointed a Special Representative to supervise the development of a framework and a set of guiding principles intended to nudge multinational corporations toward behavior more consistent with existing human rights norms.[156] The United Nations also has sponsored a series of special reports dealing with the power of information intermediaries and the threats that counterterrorism efforts pose to fundamental rights and liberties.[157] Guiding principles and special reports have no independent legal force, however, and the reports have served only to

[156] *See generally* John Ruggie (Special Representative of the Secretary-General), Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011).

[157] *See generally, e.g.*, Ben Emmerson, General Assembly, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, U.N. Doc. A/70/371 (Sept. 18, 2015); David Kaye, Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/29/32 (May 22, 2015); Ben Emmerson, General Assembly, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, U.N. Doc. A/69/397 (Sept. 23, 2014); Frank La Rue, Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013); Frank La Rue, Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/17/27 (May 16, 2011); Martin Scheinin, Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009).

underscore the extent of the disconnect. Within U.S. constitutional discourse, matters are even more complicated because platform firms also are conceptualized as rights-bearing entities, sheltered from the full weight of accountability for their users' rights by the logic of expressive immunity described in Part II.C.[158]

In the wake of the Snowden revelations about the U.S.-driven cooptation of privately operated networked communication infrastructures for mass surveillance, the power of information platforms has become a topic of broader concern. As noted in Part II.D, above, a coalition of platform firms, academics, and human rights NGOs, had earlier founded the Global Network Initiative in an attempt both to counter censorship demands made by certain countries and to respond to criticisms levied at platforms for acceding to such demands. The initiative's website proudly proclaims: "Privacy is a human right and guarantor of human dignity. Privacy is important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age."[159] The documents leaked by Snowden, however, revealed both traditional telecommunications providers and platform firms to be essential participants in ongoing and seemingly lawless government surveillance operations.

Post-Snowden, platform firms have worked hard to restore and burnish their civil libertarian public personae, filing lawsuits to challenge government production requests and developing a "warrant canary" system to circumvent the gag orders that customarily accompany such requests.[160] Unquestionably, that resistance sometimes has helped to frame questions about the legality of such operations for judicial and legislative review. Some academic commentators now argue that communications platforms —

[158] For a more detailed discussion of the disconnects involved in viewing platforms as both speakers and speech facilitators, see generally Cohen, *The Zombie First Amendment*, *supra* note 87, at 1122-28; Grimmelmann, *supra* note 147.

[159] GLOB. NETWORK INITIATIVE, GNI PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY 3 (2011), http://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy_0.pdf.

[160] *See, e.g.*, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016); *In re* Search of Info. Associated with [Redacted] @gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757 (GMH), 2017 WL 2480752 (D.D.C. June 2, 2017); *In re* Info. Associated with One Yahoo Email Address That Is Stored at Premises Controlled by Yahoo, No. 17–M–1234, No. 17–M–1235, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017); *see also* Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105, 149 (2016); Naomi Gilens, *The NSA Has Not Been Here: Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures*, 28 HARV. J.L. & TECH. 525, 529-30 (2015).

"surveillance intermediaries," to borrow Alan Rozenshtein's terminology — fulfill an important separation of powers function without which the potential for surveillance abuses by the state would be far greater.[161] Others, more skeptical, observe that platforms challenge only a very small number of the orders they receive.[162]

Even as the idea of "surveillance intermediaries" surfaces one set of important dynamics surrounding the conduct of surveillance operations, moreover, it persistently obscures others. Platform firms are intermediaries for government surveillance, but they are also surveillance principals in their own right. So, for example, Google has led the industry campaign against government information collection via secret national security letters, but also has continued to amass a formidable database linking Gmail users to their Internet activities and Android users to their geographic movements and mobile device usage patterns, and it has pursued a series of ventures in artificial intelligence — ranging from digital assistants to smart thermostats to portable virtual reality headsets — designed to extend its reach into other areas of users' lives.[163] Its decision to stop scanning the contents of emails sent and received within Gmail — initially in response to demands by paying corporate "G Suite" clients seeking better security for their own secrets — leaves its other surveillance initiatives in place.[164] Facebook offers securely encrypted chat via its WhatsApp

[161] Rozenshtein, *supra* note 109; *see also* Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 662-64 (2016).

[162] *See generally* Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441 (2015).

[163] *See* Laurie Beaver, *Google Assistant Is Coming to Audi, Volvo*, BUS. INSIDER (May 16, 2017, 12:46 PM), http://www.businessinsider.com/google-assistant-is-coming-to-audi-volvo-2017-5; Jayson DeMers, *Is 'Google Now' the Future of Mobile Search?*, FORBES (Oct. 6, 2014, 11:30 AM), https://www.forbes.com/sites/jaysondemers/2014/10/06/is-google-now-the-future-of-mobile-search; Samuel Gibbs, *Google Introduces the Biggest Algorithm Change in Three Years*, GUARDIAN (Sept. 27, 2013, 7:33 AM), https://www.theguardian.com/technology/2013/sep/27/google-biggest-algorithm-change-hummingbird; Mark Gurman & Mark Bergen, *Google to Push AI Smarts to iPhone, New Photo Books Service*, BLOOMBERG TECH. (May 16, 2017, 3:30 AM), https://www.bloomberg.com/news/articles/2017-05-16/google-to-push-ai-smarts-to-iphone-new-photo-books-service; Tess Townsend, *Google I/O 2017: Everything Important That Google Announced Today*, RECODE (May 17, 2017, 3:52 PM), https://www.recode.net/2017/5/17/15654076/google-io-biggest-announcements-keynote-highlights-2017; Tess Townsend, *Google I/O 2017: Expect a Clearer Understanding of Google's 'AI First' Future*, RECODE (May 16, 2017, 6:05 PM), https://www.recode.net/2017/5/16/15648392/google-io-2017-developers-conference-sundar-pichai-home-assistant-tensorflow-vr; Kim Zetter, *Google Takes on Rare Fight Against National Security Letters*, WIRED (Apr. 4, 2013, 1:02 PM), https://www.wired.com/2013/04/google-fights-nsl.

[164] *See* Daisuke Wakabayashi, *Google Will No Longer Scan Email for Ad Targeting*, N.Y. TIMES (June 23, 2017), https://www.nytimes.com/2017/06/23/technology/gmail-

service but also has repurposed user "likes" as product and event advertising, provided facial recognition technology to help users tag friends and acquaintances in photos uploaded by others, and manipulated its news feed to study and monetize users' emotional responses.[165] As described in Part I.E, above, the massive advertising ecosystems constructed by Google and Facebook, with their capacity for automated, personalized targeting and their corresponding amenability to gaming and manipulation, have contributed importantly to the contemporary climate of political polarization and distrust. Apple has offered secure end-to-end encryption for text messages sent via its iMessage service and for users' emails, photos, and contact lists, but collects a wide range of other information about iPhone users and about users of its MacOS operating system, and it has implemented technology to enable push notifications to iPhone owners from merchants whose establishments they happen to be passing.[166] Amazon's natural language-based digital assistant, Alexa, offers users comprehensive management of their online searches, transactions, and entertainment experiences.[167]

ads.html.

[165] *See* Robert Booth, *Facebook Reveals News Feed Experiment to Control Emotions*, GUARDIAN (June 29, 2014, 7:57 PM), https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds; Andy Greenberg, *WhatsApp Just Switched On End-to-End Encryption for Hundreds of Millions of Users*, WIRED (Nov. 18, 2014, 10:54 AM), https://www.wired.com/2014/11/whatsapp-encrypted-messaging; Drew Guarini, *Facebook Finally Axes Controversial 'Sponsored Stories' Ads*, HUFFINGTON POST (Jan. 10, 2014, 9:50 AM), http://www.huffingtonpost.com/2014/01/10/facebook-sponsored-storie_n_4574644.html; Jessica Guynn, *Privacy Implications of Facial Recognition Back in the Spotlight*, L.A. TIMES (Dec. 3, 2013, 11:06 AM), http://www.latimes.com/business/technology/la-fi-tn-privacy-implications-of-facial-recognition-back-in-the-spotlight-20131203-story.html; Sam Levin, *Facebook Told Advertisers It Can Identify Teens Feeling 'Insecure' and 'Worthless*,' GUARDIAN (May 1, 2017, 3:01 PM), https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

[166] *See* David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES (Sept. 27, 2014), https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html; Ashkan Soltani & Craig Timberg, *Apple's Mac Computers Can Automatically Collect Your Location Information*, WASH. POST (Oct. 20, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/10/20/apples-mac-computers-can-automatically-collect-your-location-information; Kyle Van Hemert, *4 Reasons Why Apple's iBeacon Is About to Disrupt Interaction Design*, WIRED (Dec. 11, 2013, 9:30 AM), https://www.wired.com/2013/12/4-use-cases-for-ibeacon-the-most-exciting-tech-you-havent-heard-of.

[167] *See* Grant Clauser, *What Is Alexa? What Is the Amazon Echo, and Should You Get One?*, WIRECUTTER, http://thewirecutter.com/reviews/what-is-alexa-what-is-the-amazon-echo-and-should-you-get-one (last updated Sept. 5, 2017); *Echo & Alexa Devices*, AMAZON, https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b/ref=sv_devicesubnav_0?ie=UTF8&node=9818047011 (last visited Sept. 18, 2017).

At no point have these and other platform companies publicly acknowledged the extent to which their own commercial interests and behaviors make them complicit in the construction of the surveillance society in which their customers now find themselves enmeshed. To the contrary, when policymakers and commentators attempt to direct attention to the ways that the platform business model undermines user rights and amplifies organized hate and political dysfunction, platforms are quick to invoke the logics of appropriative privilege and expressive immunity. In the United States, those logics now dominate regulatory and policy discussions about online privacy and freedom of expression. In European legal and policy debates, where those logics are more actively contested, platform firms have worked hard to shift the dominant frameworks in their favor. So, for example, Google bitterly criticized the initial articulations of the "right to be forgotten" by jurists and officials. Relying heavily on the trope of the information laboratory as an engine of neutral truth production, it characterized takedown requests as efforts to subtract information from the historical record, making the remaining information less authentic and complete.[168] In the media, it also pursued a strategy of widely publicizing the inevitable outrageous requests while barely acknowledging the many legitimate ones.[169] Reading the headlines, one would not understand that both the European Court of Justice and the European Commission had clearly articulated the need to consider public interests in freedom of speech and access to

[168] *See* Peter Fleischer, *Reflecting on the Right to Be Forgotten*, GOOGLE: GOOGLE EUR. (Dec. 9, 2016), https://blog.google/topics/google-europe/reflecting-right-be-forgotten; Lila Tretikov, *European Court Decision Punches Holes in Free Knowledge*, WIKIMEDIA BLOG (Aug. 6, 2014), https://blog.wikimedia.org/2014/08/06/european-court-decision-punches-holes-in-free-knowledge.

[169] *See* Natasha Lomas, *Google Super Successful at Spinning Europe's Right To Be Forgotten Ruling as Farce*, TECHCRUNCH (July 4, 2014), http://techcrunch.com/2014/07/04/digital-theatre; Natasha Lomas, *Wikimedia Attacks Europe's Right To Be Forgotten Ruling as Threat to Its Mission*, TECHCRUNCH (Aug. 6, 2014), http://techcrunch.com/2014/08/06/wikimedia-rtbf; Rose Powell, *'Right to Be Forgotten': BBC, The Guardian, Daily Mail Push Back on Google*, SYDNEY MORNING HERALD (July 3, 2014), http://www.smh.com.au/technology/technology-news/right-to-be-forgotten-bbc-the-guardian-daily-mail-push-back-on-google-20140703-zsu9a.html; James Vincent, *Google Chief Eric Schmidt Says 'Right To Be Forgotten' Ruling Has Got the Balance 'Wrong,'* INDEPENDENT (May 15, 2014, 12:07 PM), http://www.independent.co.uk/life-style/gadgets-and-tech/google-chief-eric-schmidt-says-right-to-be-forgotten-ruling-has-got-the-balance-wrong-9377231.html; Kent Walker, *A Principle That Should Not Be Forgotten*, GOOGLE: GOOGLE EUR. (May 19, 2016), http://googlepolicyeurope.blogspot.co.uk/2016/05/a-principle-that-should-not-be-forgotten.html.

information, and also had carefully distinguished between linking and indexing by search engines and archiving by originating sites.[170]

While resisting greater formal control by courts and legislatures, platform companies also have invoked the logics of performative enclosure and fiat interdiction to justify their own restructuring of information flows. By the time the first wave of debates about delinking and erasure began to fade, Google itself had put in place proprietary takedown procedures that performed the very same role it had claimed was both impossible and unwise.[171] Emerging public relations and governance strategies being developed by Facebook and Google for responding to the spread of "fake news," organized hate, malicious manipulations of the online advertising ecosystem, and terrorist content seem poised to follow a similar path.[172]

To similar effect, two of the principal strategies that have been deployed to check national security surveillance simply shift the balance of surveillance power in favor of privately operated communications platforms. This first strategy involves control over data retention. Post-Snowden, Congress enacted legislation narrowing the government's authority to request production of telecommunications metadata, requiring such requests to be

---

[170] *See* Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos (AEPD), ECLI:EU:C:2014:317 ¶ 81, 85-86 (2014); ARTICLE 29 DATA PROT. WORKING PARTY, GUIDELINES ON THE IMPLEMENTATION OF THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT ON 'GOOGLE SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLES' C-131/12 2 (2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), ¶¶ 65-66 & arts. 17, 19, 85, 88, 2016 O.J. (L 119) 1.

[171] *See* Julia Powles & Enrique Chaparro, *How Google Determined Our Right to Be Forgotten*, GUARDIAN (Feb. 18, 2015, 2:30 AM), https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search.

[172] *See* Lee, *supra* note 108; Levin, *supra* note 108; Davey Alba, *Google Goes After Bad Ads and Bad Sites That Profit from Them*, WIRED (Jan. 25, 2017, 9:00 AM), http://www.wired.com/2017/01/google-goes-bad-ads-bad-sites-profit; Monika Bickert & Brian Fishman, *Hard Questions: How We Counter Terrorism*, FACEBOOK: NEWSROOM (June 15, 2017), http://newsroom.fb.com/news/2017/06/how-we-counter-terrorism; Amber Jamieson & Olivia Solon, *Facebook to Begin Flagging Fake News in Response to Mounting Criticism*, GUARDIAN (Feb. 21, 2017, 12:07 PM), http://www.theguardian.com/technology/2016/dec/15/facebook-flag-fake-news-fact-check; Adam Mosseri, *News Feed FYI: Addressing Hoaxes and Fake News*, FACEBOOK: NEWSROOM (Dec. 15, 2016), http://newsroom.fb.com/news/2016/12/news-feed-fyi-addressing-hoaxes-and-fake-news; *YouTube Introduces New Measures To Curb Extremist Video Online*, GUARDIAN (June 19, 2017, 4:38 AM), http://www.theguardian.com/technology/2017/jun/18/more-must-be-done-about-extremist-content-online-says-google.

structured by appropriately defined selectors and effectively banning bulk collection.[173] Self-evidently, the amendments do not limit communications providers' power to collect and retain data for their own purposes, but rather depend on their continuing to do exactly that. The year beforehand, the Court of Justice of the European Union had invalidated a European Union directive mandating data retention by telecommunications providers, ruling that the mandate imposed a disproportionate burden on citizens' fundamental rights.[174] That ruling, however, did not speak directly to purportedly consensual platform activities that result in equally comprehensive collection and retention of data about users.

A very different strategy for safeguarding individual rights against abusive communications surveillance by state actors involves platform provision of strong communications encryption. Notably, strong encryption is an increasingly toothless safeguard for individual rights against *commercial* surveillance, so even a complete shift to encrypted communications would not disrupt the platform business model much, if at all. As we have already seen, that model revolves around the application of machine learning techniques to the digital traces of people's activities in real and virtual spaces. Communications data provide useful inputs to that process, but those inputs are neither the only nor the most important kinds of information on which the platform business model relies. To the contrary, within the behaviorist framework that animates platform logics, what people say to each other matters far less than what they do. Even with strong communications encryption, digital traces of what people do remain available to the platform provider — location-based information collected from mobile devices, sensor-based techniques for tracking interest in physical and virtual stimuli, click-through information for items in news feeds and social network status updates, DNS level information for tracking web browsing, and so on. And network architectures constructed for widespread, sensor-based data harvesting in turn have affordances that facilitate opportunistic data grabs by state actors.

In sum, networked, platform-based communications architectures optimized for data harvesting and predictive modulation of information flows leave network users simultaneously exposed to pervasive surveillance and cut off from the institutional structures for

[173] USA Freedom Act of 2015, Pub. L. No. 114-23, § 101, 129 Stat. 269 (codified as amended at 50 U.S.C. § 1861 (2015)).

[174] Case C-293/12, Case C-594/12, Dig. Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res., ECLI:EU:C:2014:238 (2014).

vindicating the constitutional and human rights that pervasive surveillance threatens. Those architectures also entail continuing vulnerability to state surveillance. Platform responses to demands for surveillance reform have produced meaningful shifts in the balance of power, but often have seemed calibrated first and foremost to preserve their own authority vis-à-vis threatened intrusions by government actors. These developments are combining to constitute the space of networked digital communications as a space devoid of protections for vital human freedoms, even as the activities conducted in that space become more and more fundamental to the exercise of those freedoms.

D. Resistance Is Futile?: Platforms as Emergent Transnational Sovereigns

The broad scope of the authority that platforms exercise over their users and their increasingly robust capacity to resist government demands and evade protections for fundamental rights also raise a different set of questions, which have to do with the dividing line between power and sovereignty. Dominant platforms' role in the international legal order increasingly resembles that of sovereign states. And even as they evade the obligations of domestic legal regimes, platform firms are actively participating in the ongoing construction of new transnational institutions and relationships that are more hospitable to their interests.

It is useful to begin with definitions. Within the Westphalian international legal order, a sovereign state is, most minimally, an entity with a defined territory and a permanent population, the authority to govern its territory, and the capacity to enter into relations with other states.[175] Within that framework, the power of transnational corporations to resist state control has become an increasingly thorny problem.[176] Although such corporations are nominally headquartered in particular countries and have physical assets in many other countries that are amenable to control in varying degrees, their great economic power translates into correspondingly powerful capacity for regulatory arbitrage.

---

[175] *See* Convention on Rights and Duties of States art. 1, Dec. 26, 1933, 49 Stat. 3907, T.S. No. 881; Winston P. Nagan & Craig Hammer, *The Changing Character of Sovereignty in International Law and International Relations*, 43 COLUM. J. TRANSNAT'L L. 141, 149-50 (2002).

[176] *See* Claudio Grossman & Daniel D. Bradlow, *Are We Being Propelled Towards a People-Centered Transnational Legal Order?*, 9 AM. U. J. INT'L L. & POL'Y 1, 8 (1993); *see also* Beth Stephens, *The Amorality of Profit: Transnational Corporations and Human Rights*, 20 BERKELEY J. INT'L L. 45, 57 (2002).

Dominant platform firms fit within the narrative of the transnational corporation as both constrained by and resistant to the international legal order, but they also rewrite that narrative in important ways. To begin with, platforms have both territories and populations. Platform territories are not contiguous physical spaces but rather are defined using protocols, data flows, and algorithms. Both technically and experientially, however, they are clearly demarcated spaces with virtual borders that platforms guard vigilantly.[177] The benefits of those spaces accrue most visibly and predictably to users who maintain permanent and consistent membership. Dominant platforms like Facebook, Google, and Apple have user populations that number in the billions, vastly eclipsing the populations of all but the largest nation states.[178]

As to governance authority, the sovereignty of platforms is emergent and performative. As we have just seen, platform firms acting in their capacity as surveillance intermediaries actively and theatrically resist certain kinds of incursions by nation states on their own governance authority. In court systems around the world, platforms have simultaneously defended against production requests for data stored overseas and resisted attempts by governments where that data is stored to exert control in the interests of data protection.[179] In regulatory fora, they have engaged in protracted negotiation with competition regulators,[180] transportation and labor regulators,[181] data

[177] On networked spaces as experienced spaces, see generally Cohen, *Cyberspace*, *supra* note 80, at 226-49.

[178] *See* Anupam Chander, *Facebookistan*, 90 N.C. L. REV. 1807, 1808 (2012); *Apple Inc. (AAPL.OQ) Company Update*, CREDIT SUISSE (Apr. 4, 2016), http://research-doc.credit-suisse.com (estimated 588 million users as of April 2016); Xavier Harding, *Google Has 7 Products with 1 Billion Users*, POPULAR SCI. (Feb. 1, 2016), http://popsci.com/google-has-7-products-with-1-billion-users (1 billion users as of February 1, 2016); *Stats*, FACEBOOK: NEWSROOM, http://newsroom.fb.com/company-info (last visited June 20, 2017) (1.94 billion monthly active users as of March 2017). Chander dismisses the territory argument out-of-hand on the ground that virtual territories do not count and argues that the staggering user numbers are irrelevant because one can leave Facebook and because the average user has only a few hundred "friends." Chander, *supra*, at 1817-18. But leaving Facebook is increasingly difficult, and even users who do not know one another are nonetheless bound to obey the rules of the platform just as citizens are bound to obey the laws of the state.

[179] *See generally* Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. (forthcoming 2018).

[180] *See, e.g.*, James Kanter, *European Regulators Fine Microsoft, Then Promise to Do Better*, N.Y. TIMES (Mar. 6, 2013), https://www.nytimes.com/2013/03/07/technology/eu-fines-microsoft-over-browser.html; Rowland Manthorpe, *Google Could Be Fined $1bn by the European Commission as Its Antitrust Case Comes to an End*, WIRED (June 16, 2017), http://www.wired.co.uk/article/timeline-googles-marathon-anti-trust-case-

protection authorities,[182] and tax authorities.[183] Although many of these controversies also implicate users' rights of privacy, expression, and association, platforms more often seem to be principally concerned with establishing their own regulatory independence. Speaking at a recent network security conference, Microsoft's president crystallized that ambition, sketching a future in which platform firms function as "a trusted and neutral digital Switzerland."[184] Several months later, chastising the NSA after a powerful hacking exploit that it had developed was stolen and then used by cybercriminals, he characterized "nation-state action and organized criminal action" as "the two most serious forms of cybersecurity threats in the world today."[185] Statements like these, which position platforms as conscientious, neutral stewards of the global digital infrastructure, set a lofty tone that elevates the more self-interested processes of strategic positioning operating continually in the background.

At the same time, platforms are unmatched by other transnational corporations in the extent of the authority they wield over the day-to-day experiences and activities of their users. Platforms govern their

with-the-eu; Mark Scott, *E.U. Fines Facebook $122 Million over Disclosures in WhatsApp Deal*, N.Y. TIMES (May 18, 2017), https://www.nytimes.com/2017/05/18/technology/facebook-european-union-fine-whatsapp.html.

181 *See, e.g.*, Daniel Fisher, *Uber Fights Seattle's Push to Make It Bargain With the Teamsters*, FORBES (Mar. 16, 2017, 5:23 PM), https://www.forbes.com/sites/danielfisher/2017/03/16/uber-asks-can-seattle-really-make-us-bargain-with-the-teamsters; Mark Scott, *Uber Suffers Bloody Nose in Its Fight to Conquer Europe*, N.Y. TIMES (May 11, 2017), https://www.nytimes.com/2017/05/11/technology/uber-ecj-europe.html; Adam Vaccaro, *Uber Doesn't Want Massachusetts to Limit Driver Hours*, BOSTON GLOBE (May 12, 2017), https://www.bostonglobe.com/business/2017/05/11/uber-doesn-want-massachusetts-limit-driver-hours/wXI4yuUVRNBQZZRpog1rIL/story.html.

182 For a detailed exploration of Facebook's dealings with U.S. and Irish regulatory authorities, see generally William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959 (2016).

183 *See* James Kantner & Mark Scott, *Apple Owes $14.5 Billion in Back Taxes to Ireland, E.U. Says*, N.Y. TIMES (Aug. 30, 2016), https://www.nytimes.com/2016/08/31/technology/apple-tax-eu-ireland.html; Sam Schechner, *Apple Hits Back over EU Irish-Tax Decision*, WALL ST. J. (Dec. 19, 2016, 3:12 PM), http://www.wsj.com/articles/eu-raises-pressure-on-apples-tax-deal-in-ireland-1482162608.

184 Kate Conger, *Microsoft Calls for Establishment of a Digital Geneva Convention*, TECHCRUNCH (Feb. 14, 2017), https://techcrunch.com/2017/02/14/microsoft-calls-for-establishment-of-a-digital-geneva-convention. *See generally* Kristen Eichensehr, Digital Switzerlands (Aug. 28, 2017) (unpublished manuscript) (on file with author).

185 Bill Chappell, *WannaCry Ransomware: Microsoft Calls Out NSA for Stockpiling Vulnerabilities*, NPR: TWO-WAY (May 15, 2017, 8:58 AM), http://www.npr.org/sections/thetwo-way/2017/05/15/528439968/wannacry-ransomware-microsoft-calls-out-nsa-for-stockpiling-vulnerabilities.

domains with a quiet tenacity, imposing their own regulatory structures on permitted conduct — e.g., sponsored search results, Facebook "likes" and "tags," Twitter retweets — and their own internal sanctions on disfavored conduct. They have begun to develop more regularized internal codes for handling the latter. As Tarleton Gillespie describes, most general purpose platforms ban or limit pornography, representations of extreme violence, harassment, hate speech, representations of self-harm, and promotion of drug use.[186] In processes that resemble coordinated lawmaking, they develop and share policy guidelines and construct regulatory institutions and practices to regularize the processes of content flagging and removal.[187]

Platforms also increasingly practice diplomacy in the manner of sovereign actors. Facebook's privacy team travels the world meeting with government officials to determine how best to satisfy their concerns while continuing to advance Facebook's own interests, much as a secretary of state and his or her staff might do.[188] Such efforts recently bore unprecedented fruit when Denmark announced the appointment of a digital ambassador whose portfolio focuses on relations with the giant platform companies. That decision in turn may inform discussions now underway in various other European settings about the desirability of appointing new government "digital ministers."[189]

Last and notably, platforms speak with increasingly independent voices in new transnational governance settings that play increasingly

---

186 *See* Gillespie, *supra* note 108.

187 *See id.*; Klonick, *supra* note 109.

188 *See, e.g.*, Gwen Ackerman, *Facebook and Israel Agree to Tackle Terrorist Media Together*, BLOOMBERG (Sept. 12, 2016, 11:18 AM), https://www.bloomberg.com/news/articles/2016-09-12/facebook-and-israel-agree-to-tackle-terrorist-media-together; My Pham, *Vietnam Says Facebook Commits to Preventing Offensive Content*, REUTERS (Apr. 27, 2017, 7:46 PM), http://uk.reuters.com/article/us-facebook-vietnam/vietnam-says-facebook-commits-to-preventing-offensive-content-idUKKBN17T0A0; Mike Swift, *Facebook to Assemble Global Team of 'Diplomats,'* MERCURY NEWS (May 20, 2011, 12:25 PM), http://www.mercurynews.com/2011/05/20/facebook-to-assemble-global-team-of-diplomats.

189 *See* Zoë Henry, *European Nations Appoint 'Digital Ministers,' Recognizing the Clout of Tech Titans*, INC. (Feb. 6, 2017), https://www.inc.com/zoe-henry/denmark-appoints-first-ever-digital-minister-recognizing-political-influence-of-tech.html; Adam Taylor, *Denmark Is Naming an Ambassador Who Will Just Deal with Increasingly Powerful Tech Companies*, WASH. POST (Feb. 4, 2017), https://www.washingtonpost.com/news/worldviews/wp/2017/02/04/denmark-is-naming-an-ambassador-who-will-just-deal-with-increasingly-powerful-tech-companies; *cf.* Youkyung Lee, *Taiwan's "Hacker Minister" Reshaping Digital Democracy*, SEATTLE TIMES (Apr. 23, 2017, 10:47 PM), http://www.seattletimes.com/business/taiwans-hacker-minister-reshaping-digital-democracy-2.

important roles in the emergent global legal order. Those settings, which include world trade negotiations and proceedings conducted by Internet standard-setting bodies, are themselves harbingers of institutional change.[190] In such settings, therefore, the role of platforms in the emergent global legal order is doubly under construction.

CONCLUSION: FUTURE-PROOFING LAW DOES NOT MEAN WHAT YOU THINK IT MEANS

In his closing remarks at the symposium that gave rise to the articles in this volume, Professor Anupam Chander used an analogy to the process of "baby-proofing" a home to raise an important question about the meaning of the term "future-proofing": Do the stairway gates, table bumpers, electric socket covers, and so on protect the baby from the house or the house from the baby? Does the idea of "future-proofing" law refer to a need to protect the (bright, shiny) future from the (presumptively obsolete) legal system? Or, does it refer to a need to protect the (precious and now-jeopardized) rule of law from the (rapacious, continually-accelerating) future?

In both cases, neither answer is quite right. The process of baby-proofing a home changes the lived experience of the baby, the family, and ultimately of society. It engenders new industrial production practices, new markets, and new cross-border trade flows organized around producing and distributing an ever-growing array of essential-until-disposable plastic products, which accumulate in landfills and in the farthest reaches of the ocean. It calls forth tot-sized car seats bulked up like mini Sherman tanks and demands ever larger vehicles that can accommodate multiple units in the back seat(s). It replaces vigilance with architecture — and engenders different kinds and patterns of risk-taking. A technology studies scholar would say that practices of baby-proofing produce new actor-networks — new

[190] *See, e.g.*, KONSTANTINOS KOMAITIS, THE CURRENT STATE OF DOMAIN NAME REGULATION: DOMAIN NAMES AS SECOND-CLASS CITIZENS IN A MARK-DOMINATED WORLD 149-66 (2010); Ingrid Lunden, *How Tech Giants Like Amazon and Google Are Playing the ICANN Domain Game*, TECHCRUNCH (June 13, 2012), https://techcrunch.com/2012/06/13/how-tech-giants-are-playing-the-icann-domain-game; Nicole Sagener, *Report: Lobbyists Heavily Influencing TiSA Negotiations*, EURACTIV (Dec. 13, 2016), https://www.euractiv.com/section/public-affairs/news/report-lobbyists-heavily-influencing-tisa-negotiations; Maira Sutton, *Newly Released Emails Reveal Cozy Relationship Between U.S. Trade Officials and Industry Reps over Secret TiSA Deal*, ELEC. FRONTIER FOUND. (Aug. 26, 2015), https://www.eff.org/deeplinks/2015/08/new-foia-released-emails-reveal-cozy-relations-between-us-trade-officials-and. *See generally* LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 33-85 (2014).

sociotechnical formations that subtly rearrange the relationships among their participants, with ramifications that extend more broadly and deeply than we might assume.[191]

So too for law in the platform-based economy. The uncoordinated patterns of self-interested, strategic intervention by platform firms are producing new legal-institutional formations optimized to their various projects and goals. In broadest brush, this is as it should be; legal institutions should change to meet the demands of the times, and so it is only logical that the ascendancy of platforms should produce new legal relationships and new institutional settlements. But the details matter — and even details that seem small or not worth remarking can engender profound systemic effects.

The full account of law's accommodation to the informational economy is yet to be written, and the Polanyian analogy suggests an important stage still to come. As Polanyi detailed, the human costs of the shift to industrialism ultimately elicited a protective "countermovement" in the form of regulatory constraints on market processes.[192] Whether the shift to an informational, platform-based economy will elicit a comparable protective countermovement is yet to be seen; it is clear, however, that the platform has become a principal vector of institutional destabilization and that some important human costs are beginning to materialize.

The questions now on the table concern the best paths for institutional evolution — and the extent to which legal institutions should bend to the service of emergent economic power. Those questions matter urgently. Law for the platform economy is being written all around us; it is time to pay attention.

---

[191] *See generally* BRUNO LATOUR, REASSEMBLING THE SOCIAL: AN INTRODUCTION TO ACTOR-NETWORK-THEORY (2005); Michel Callon, *Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay*, *in* POWER, ACTION, AND BELIEF: A NEW SOCIOLOGY OF KNOWLEDGE? 196-223 (John Law ed., 1986); Bruno Latour, *Technology Is Society Made Durable*, *in* A SOCIOLOGY OF MONSTERS 103-32 (1984).

[192] *See* POLANYI, *supra* note 2, at 130-31.