Between Truth and Power (New York: Oxford Univ. Press, 2019)

Chapter 3.
The Information Laboratory

"So what I told you was true . . . . from a certain point of view."
Obi-Wan Kenobi in *Star Wars, Episode VI: Return of the Jedi* (1983)

The emergence of the platform as the core organizational logic of the networked information economy and the accompanying proliferation of infrastructures for data harvesting and predictive profiling have profoundly reshaped both patterns of information flow and capabilities for participation in social and commercial life. The changes upend settled ways of understanding the nature and social function of media technologies—and challenge conventional wisdom about the appropriate roles(s) for law in relation to media and information.

For several hundred years, political philosophers and legal theorists have conceptualized media technologies as "technologies of freedom," arguing that access to information and to the means of communication promotes reason, self-determination, and democratic self-government.[1] Some things about that equation have not changed; certainly, access to information, self-determination, and democratic self-government are inescapably interrelated. But aspects of the interrelationship have changed beyond recognition. As communications theorist Mark Andrejevic explains, our most deeply rooted instincts about the role of information in a democratic society "took shape during an era of relative information scarcity," and so many defining political battles "revolve[d] around issues of scarcity and the restriction of access to information."[2] Today's networked digital information infrastructures have different and more complicated affordances. In the contemporary era of *infoglut*—of "an unimaginably unmanageable flow of mediated information . . . available to anyone with Internet access"—new political and epistemological dilemmas flow instead from abundance and algorithmic intermediation.[3] The problem is not scarcity but rather the need for new ways of cutting through the clutter, and the resiting of power within platforms, databases, and algorithms means that meaning is easily manipulated.

As the volume of information available online has mushroomed, the quest for data-intensive surplus extraction described in Chapter 2 has spurred development of a fast-evolving collection of techniques designed to undercut the exercise of informed reason by users of networked information services. Contemporary, platform-based information infrastructures and ecosystems are being optimized to detect behavioral cues and to appeal to motivation and emotion on a subconscious level. That gradual but seemingly inexorable shift has begun to produce object lessons in the law of unintended consequences. Widespread dispersal of personal data has engendered new patterns of

reputational anxiety, manipulation, and insecurity. Algorithmically mediated processes designed to create tight stimulus-response feedback loops have exposed and deepened social divides on a variety of cultural and political issues, reinforced the power of conspiracy theories and junk science, and amplified toxic currents of bigotry, nationalism, and ideological extremism.

Debates about *how law should respond* to the emergence of massively-intermediated media environments have generated more heat than light. Many accomplished and well-meaning observers misread contemporary media ecologies, applying time-tested syllogisms about media freedom, reasoned public discourse, and rational self-determination to situations for which they are no longer well suited. Meanwhile, powerful information-economy actors have mobilized new kinds of arguments about freedom of expression to stave off protective regulation and deflect accountability for both old and new kinds of harm. Those arguments give the traditional First Amendment metaphor of a "marketplace of ideas" a modern and distinctly neoliberalized inflection, positing a virtuous alignment between economic and expressive liberty. They also introduce a powerful new metaphoric frame—that of the information laboratory, a site of beneficial and constitutionally privileged innovation and experimentation that functions as a depoliticized engine of truth production. Meanwhile, a combination of expertly fanned anxiety about censorship and exquisitely calibrated political gamesmanship about what constitutes noninterference with freedom of expression works to foreclose discussion of viable (and speech-regarding) alternative pathways. The result of those efforts is a growing constellation of de jure and de facto legal immunities that predominantly bolsters private economic power, that magnifies the vulnerability of ordinary citizens to manipulation, exploitation, and political disempowerment, and that threatens profound collective harm.

The Emergent Limbic Media System

It is useful to begin by exploring patterns of information flow within the platform-based, massively intermediated information environment. As we saw in Chapter 2, the construct of the biopolitical public domain and its accompanying logic of productive appropriation have both catalyzed and justified large-scale sociotechnical shifts toward datafication, data harvesting, and the construction of powerful new data refineries. But Chapter 2 did not delve deeply into questions about the *kinds* of data that information businesses collect or the *mechanisms* by which algorithmic intermediation operates on the data to produce results. This section takes up those questions. Both to structure the discussion and by way of provocation, I offer the following analogy: The operation of the digital information environment has begun to mimic the operation of the collection of brain structures that mid-twentieth-century neurologists christened the limbic system and that play vital roles in a number of precognitive functions, including emotion, motivation, and habit-formation.[4]

I do not mean to suggest that anything about the configuration or operation of the digital information environment is natural or organically determined. I seek simply to focus the reader's attention on the mismatch between the "technologies of freedom" frame that dominates legal discussions about media law and policy and the kinds of

responses that platform-based, massively intermediated information infrastructures work to produce. By design and as operated, the emergent limbic media system supplies the information laboratory with responsive experimental subjects.

Rather than predominantly stimulating the development and exercise of conscious and deliberate reason, today's networked information flows are optimized to produce what social psychologist Shoshana Zuboff calls instrumentarian power: They employ a radical behaviorist approach to human psychology to mobilize and reinforce patterns of motivation, cognition, and behavior that operate on automatic, near-instinctual levels and that may be manipulated instrumentally.[5] To similar effect, but focusing on the subjects of datafication, legal philosopher Mireille Hildebrandt traces the emergence of a new form of "data-driven agency" that is "mindless," algorithmically mediated, and constituted by "ubiquitous anticipation."[6] The result is an emergent form of collective consciousness that is primed for precognitive activation and manipulation at scale. To an extent, that reflects deliberate design, but experiments in data-driven, algorithmic intermediation also have proved powerful in ways their designers likely did not intend or expect. They portend far-reaching collateral effects on the emerging information society and the subjects who inhabit it.

Prologue: Reputation as Capital and Stigma

An important forerunner of the emergence of data-driven agency was the gradual reinvention of digital reputation as both an explicit locus of self-management and a distributed mechanism for behavior modification. As twentieth-century sociologist Erving Goffman documented, self-presentation is an enduring human concern. Individuals have always devoted time to reputation work of one sort or another, building, cementing, and sometimes undermining their standing in their communities.[7] In the networked information age, however, reputation has become increasingly quantified and datafied, and reputational data and metrics are widely dispersed, flowing through channels far removed from individual control. As those shifts have occurred, the mechanisms for building and maintaining reputational capital and attempting to repair reputational damage have changed almost beyond recognition.[8]

Today's quantified, datafied reputation metrics trace their origins to two mid-twentieth-century developments. The first, discussed in Chapter 2, was the emergence of the consumer reporting industry. The types of socially mediated, inherently local judgments about reputation that historically had guided credit and employment decisions could not perform that function well in an increasingly urbanized, national economy, and so practices of reputation assessment began to evolve to meet changing needs.[9] The earliest consumer reporting entities were simply clearinghouses for collection and exchange of the sorts of information traditionally monitored by local lenders—salary, repayment history, and so on. As the volume of information mushroomed and as technological development produced new methods for storing and processing the information, market actors began to experiment with more efficient ways of formulating and expressing judgments about consumer creditworthiness and reliability. Those efforts led ultimately to metrics for quantified credit scoring.[10]

Consumer reputation scoring was initially the province of a small, specialized group of initiates, but that is no longer the case. To participate in reputation scoring

markets, one needs both computing resources and access to flows of relevant information. The revolution in processing power that began during the late twentieth century, and that continues today with the development of cloud-based data processing services, has put the necessary computing resources within general reach. And, as we saw in Chapter 2, the emergence of networked information architectures and the reconfiguration of those architectures to enable pervasive tracking and data harvesting have made flows of personal data ubiquitous and easy to capture. The relevance of those flows to predictive scoring is both an article of faith and the foundation of a multibillion-dollar industry. Today, consumer reputation metrics include a wide range of correlations, inferences, and predictions generated by data mining and analysis.[11]

Another historical precursor of contemporary quantified, datafied reputation metrics was the ratings systems developed during the mid-twentieth century to demystify markets in consumer goods and services. As mass-marketed goods and services increasingly displaced more local options, and as those goods and services became increasingly more complex and difficult for consumers to evaluate at the point of purchase, ratings systems such as those developed by *Consumer Reports* and *Good Housekeeping* emerged.[12] Those systems, often consisting of simple, 5-point scales for communicating the results of more complicated product testing, are the conceptual antecedents of the customer satisfaction ratings that today are seemingly everywhere. Like credit scoring, however, ratings production is no longer the sole province of trained experts. Many contemporary ratings systems claim a different kind of epistemic authority, located in the personal experiences of consuming subjects. Information businesses—including both general-purpose platforms such as Google, Amazon, and Yelp and specialized sites such as TripAdvisor and Zappos—compete with each other to develop crowd-sourced ratings and present them to consumers as valuable sources of information.

Within platform-based information environments, the ratings craze has spread beyond businesses and products to individuals themselves. An early pioneer in this regard was eBay, which developed the first widely publicized system for aggregating user feedback on buyers and sellers. Contemporaneously, news and information sites such as Slashdot began using feedback systems to help users make sense of the rapidly proliferating participatory universe. Slashdot designed its interface both to push more highly rated comments to the top and to identify those users whose postings tended to be rated more highly.[13] Both models spread rapidly to other platform-based commercial and discussion fora, which developed variants suited to their own purposes. Sites as varied as Twitter, Reddit, and Amazon all rely heavily on both crowd-sourced content and data designed to enable participating users to evaluate the value of contributions by other participating users. Meanwhile, computer scientists and legal academics have gravitated to the idea of crowd-sourced, peer-produced ratings as a panacea for a wide variety of social coordination problems ranging from driving to dating.[14]

Both the personal data used for consumer reputation scoring and publicly available reputation metrics are increasingly widely dispersed, and that has made network users vulnerable to new kinds of reputational harm. Crowd-sourced ratings systems and similar participation metrics are expressly designed to enable reputation-at-a-distance and to allow users to dispense with the need for repeat interaction before forming judgments.

For exactly those reasons, though, such systems create new possibilities for abuse ranging from self-interested gaming to targeted sabotage.[15] The consequences of the latter can be especially drastic for individuals and small businesses, which may lack both the resources to counter sabotage campaigns and the reputational security to ignore them. The design and operation of social networking platforms also magnifies reputational vulnerability. Although in recent years social networking platforms such as Facebook have allowed users to indicate their preferences about sharing certain items and about identification and tagging in photos posted by others, it is impossible to prevent information posted to a social network from spreading beyond its point of origin.

Neither the growing importance of datafied reputational constructs nor the new vulnerabilities they generate have been lost on network users. Literatures from marketing to self-help to media studies reflect the emergence of an acutely reputation-inflected sensibility of self-presentation. Social media updates, for example, are less spontaneous and more carefully curated to accentuate the positive and enviable. Younger, "born digital" network users in particular have developed and internalized elaborate rules of self-presentation.[16] Many older users, meanwhile, cultivate techniques of online reputation building that are highly instrumentalized, straightforwardly acknowledging that their point is to craft reputation as a factor of production. In part, that approach reflects the changing nature of production in the dematerialized, platform-based labor markets described in Chapter 1. Self-promotion is an essential survival skill for freelance information workers, and new data-based metrics of reputation—numbers of followers on Twitter or Instagram, number of views on YouTube, and so on—matter for success. It has become common to see self-proclaimed experts on self-management and self-promotion tutoring their readers on the best ways of maximizing and refining their own public exposure.[17]

The paradoxical combination of heightened reputational sensibility and diminished control over reputational development creates and feeds a continual need for reputational maintenance and repair.[18] Predictably, maintenance and repair themselves have become business models. One model, euphemistically titled "search engine optimization" (SEO) has emerged to serve the needs of both individuals and businesses seeking to burnish their public images and improve their visibility. Another, dedicated to credit monitoring and credit repair, responds to the increasing prevalence of credit fraud and identity theft by offering individuals the promise of protection for a small monthly fee.[19]

Although the language of reputation management and self-management is the language of individual choice, the new economies of reputation and reputation modeling distribute reputational authority and vulnerability unevenly. Information about reputation is plentiful, but decoding and effective intervention require specialized expertise. The technologies of curation and repair that offer to return some measure of control also change the nature of that control. Prior to the era of datafied, dispersed reputation, repairing damaged commercial and social reputation demanded sustained relational and communal engagement. The new processes of curation and repair substitute an individualized, commodified vision of reputation management as a market-centered activity pursued by individual neoliberal subjects.

Surveillance as Play and Self-Betterment

Techniques for motivating enrollment and participation in the surveillance economy also have contributed importantly to the emergence of data-driven, instrumentarian power and the formation of data-driven agency. Within commercial surveillance environments, the themes of play, games, and participation are increasingly prominent. The forms of play and gaming are highly organized and strategic and revolve around the idea of gamification, defined in business texts as the application of concepts and techniques from games to drive consumer "engagement" that promotes business objectives in other areas of activity.[20] In gamified commercial surveillance environments, personal data collected from subscribers—both at enrollment and on a continual basis during the course of play—are used both to deliver rewards and to engage in various forms of targeted marketing.

FourSquare, a social networking application used for sharing information about one's whereabouts, is generally credited with popularizing the idea of gamification as a data collection technique. For the first four years of its existence, FourSquare offered subscribers opportunities to compete for rewards, which took the form of badges that might designate a subscriber "Mayor" of her favorite bar (for being a regular visitor) or "Player Please" (for checking into the bar with three or more members of the opposite sex). The success of that initial experiment inspired a broad and durable marketplace shift. For example, discount fashion retailer H&M, in partnership with an online gaming company, has used gamification to bring customers off the street and into its stores, offering those who are playing the game items that can be scanned in the store to generate discounts. Nike+, a personal fitness tool, uses gamification to help its users set fitness goals, monitor their own progress, and track their progress relative to that of other users.

As these examples illustrate, the gamification of commercial surveillance has roots in customer loyalty programs that are decades old, but gamification rewards customer loyalty in ways that generate public, social recognition. The field of crowd-sourced promotion has its cautionary tales. Facebook's ill-fated Beacon service, which automatically coopted its members' social updates as promotion tools, sparked outrage that led to high-profile class action litigation.[21] Contrast, however, the experience of gamified promotion ventures that are shopping-oriented first and foremost. Groupon, a social shopping site, uses gamification—in the form of an anthropomorphic icon named "Clicky" that entices users to pursue access to additional content and exclusive discounts—to incentivize bargain-hunters to visit the site more frequently. Groupon's early success can be traced to its founders' recognition that customers could absorb producer surplus and reveal information about their resources, their patterns of discretionary spending, and their social networks at the same time. After settling the Beacon litigation, Facebook used its newly developed "Like" button to similar (but far more wide-ranging) effect.[22]

The gamification of commercial surveillance environments also has roots in the Quantified Self movement, which was founded in 2007 by a group of technology evangelists seeking better living through data. The initial impetus behind the QS movement was aggressively populist. QS entrepreneurs and communities offered participants the opportunity to shift control of health, diet, and fitness away from impersonal providers offering cookie-cutter recommendations and back toward

individuals, and promised to keep participants' data safe within walled gardens.[23] Predictably, however, commercial providers of QS technologies and applications entered the field, offering services like the Nike+ fitness tracker described previously. As they have done so, the dialogue around QS has shifted, deemphasizing control over data and emphasizing instead the need to provide and share data to gain tools for controlling other aspects of one's life, including health, diet, and fitness, but also work habits, sex life, sleep patterns, and so on. Where the populist QS discourse was earnest and geeky, commercial QS products speak to lifestyle concerns in the language of marketing.[24]

Gamified surveillance environments are not games, but they are like games. They manifest both actions taken by the subject of gamified surveillance to perform the in-world rituals of gameplay—for example, to unlock benefits or "level up" membership—and background machine actions that establish the environment for gameplay—for example, the repetitive background displays of status updates from other users or ticker updates offering a continual stream of discount opportunities. They also establish an external frame of reference for the gameworld—for example, by establishing a process for enrollment, defining tiers of membership and corresponding benefits, and imposing "gamic death" upon logout.[25] But there are also profound differences between games and gamified surveillance environments. The gameworld purports to be the social world, or some segment of it, but its focus is on targeting and nudging patterns of discretionary spending and leisure mobility. Gamification techniques reconfigure their participants as depoliticized subjects who achieve both self-expression and self-realization through the purposive and playful exercise of consumptive freedom.[26]

Gamified surveillance environments therefore also constitute powerful mechanisms for behavioral conditioning. The "token economies" characteristic of gamified surveillance environments have been used as a form of behaviorist therapy for psychiatric patients, preparing them for reintegration into society by giving them sets of situation-specific rituals to perform.[27] In commercial surveillance environments, gamification takes on a similarly ameliorative gloss, inculcating repetitive behavior patterns oriented toward self-betterment. As Jennifer Whitson describes it, "becoming the victorious subject of gamification is a never-ending leveling-up process, guided by a teleology of constant and continual improvement, driven by an unending stream of positive feedback and virtual rewards, and fuelled by the notion that this process is playful."[28]

Like the sublimation of consent, discussed in Chapter 2, gamification is a technique for supply chain management that works to keep the surveillance economy's data harvesting pipelines full and flowing. Its rapid spread reflects the same financialization dynamics that Chapter 1 explored. FourSquare emerged as social networking platforms were migrating into the economic mainstream and seeking sources of financing in capital markets. Its use of rewards as incentives for participants was both a strategy for achieving market penetration and a way of responding to potential investors' demands for a plausible revenue model. Foursquare is also a cautionary tale, because its gamification strategy proved unable to hold subscriber interest over the longer term, and in 2013 it announced that it was abandoning its badge system.[29] Different and more durable examples of gamification within social networking platforms are the unending competition for followers, favorites, and retweets on Twitter and for followers

and likes on Facebook and Instagram. While Foursquare's badge system proved in the end to be a passing fad, on Twitter, Facebook, and Instagram the rewards leverage a more intrinsic motivation for recognition and influence.

Recall from Chapter 2, moreover, that the user interfaces that mediate access to gamified surveillance environments also are designed with behavioral conditioning in mind. Both the dominant platforms that sit atop data harvesting ecologies and lesser designers of app-based services rely on insights gleaned from addiction research to maximize users' "time on device."[30] More time on device means more data, and more data translate into a wider range of potential surplus extraction opportunities.

The Rise of Behavioral Microtargeting

The newest commercial surveillance techniques are designed to bypass individual awareness altogether, detecting behavioral cues and using them to target precisely calibrated flows of promotional, informational, and cultural content. From one perspective, such activities are broadly consistent with marketing's decades-long effort to claim for itself the status of a behavioral science.[31] From another, techniques for behavioral microtargeting represent radical departures from the traditional marketing canon. As Zuboff describes, today's cutting-edge behavioral surveillance techniques trace their origins to two sets of mid-twentieth-century research initiatives: one in experimental social psychology that was predicated on absolute denial of the possibility of free will, and another on the behavior of animal herds that emphasized behavioral "tuning" to modulate group behavior in desired ways.[32] As applied to human beings, such techniques eschew persuasion in favor of direct behavioral conditioning, and they target not only consumptive preferences but also cultural, political, and religious affiliations and even basic frames for scientific, historical, and journalistic understanding.

From the perspective of purveyors of goods and services, behavioral microtargeting responds to the dilemma of abundance that characterizes the contemporary era of infoglut. Strategies for capturing market share using branding and gamification have become both more powerful and more demonstrably incomplete. As we saw in Chapter 1, branding has assumed ever-increasing economic and legal importance in the informational economy. Modern branding is memetic and compelling, exploiting compact, graphically intensive signifiers and catchy slogans and soundbites carefully designed to take root in consumers' subconscious minds.[33] Platform-based media environments enable brands to become even further detached from the goods and services to which they notionally refer and to take on expressive lives of their own. The modern corporation does not simply advertise its wares. It develops a "social media presence" on platforms such as Facebook and Twitter, streaming updates to its followers about developments that might implicate its market or enhance its brand cachet, and uses social media to recruit certain types of consumers as brand evangelists. And, as we have just seen, it uses gamification strategies in an attempt to capture and hold consumers' attention.

Ultimately, however, brand-related strategies for consumer surplus extraction confront inherent limitations. First, consumers are not simply passive recipients of brand-related messaging. Some simply resist brand-related messaging, while others appropriate and remix logos, jingles, and other promotional material to subvert such messaging in

powerful and creative ways.[34] The same platform-based media infrastructures that enable businesses to reach consumers also enable consumers to assign new meanings to brands and advertising copy and distribute their own messages widely. Second, even highly effective brand-related messaging must contend with the condition of infoglut, which makes even those messages that (some) consumers want to receive difficult to distinguish from the millions of other pieces of information competing for their attention. As David Murakami Wood and Kirstie Ball have explained, even the more certain access to consumer preferences that databases combining demographic information with information about buying behavior appeared to promise is in important respects a mirage; like other techniques of governance, the constructed "brandscapes" informed by such databases remain "messy, contingent, and subject to failure."[35]

Techniques for behavioral surveillance and microtargeting promise solutions to these problems. Chapter 2 traced the emergence of the sensing net as a distributed assemblage for harvesting vast quantities of behavioral data for industrial-scale refinement, analysis, and deployment. From a behaviorist standpoint, unmediated behavioral data—data that are not self-reported or otherwise subject to conscious manipulation by data subjects—are the holy grail, promising previously unequaled accuracy in predictive forecasting and commensurate levels of profit. That logic dictates continuous experimentation with methods for sensing, measuring, and modeling consumer interests, affinities, and aversions.

Like gamification, behavioral microtargeting is not the exclusive province of platform firms and data brokers. As Joseph Turow has described, supermarkets in particular have been pioneers in the use of techniques for tracking consumers' progress through physical stores and correlating patterns of movement and browsing with coupons and personalized discount offers.[36] The siren song of behavioral microtargeting also has attracted a wide and varied assortment of academic researchers focused on improving the state of the art. Burgeoning literatures in marketing, psychology, and data science describe new research programs designed to test the efficacy of existing microtargeting techniques and develop new ones.[37]

Within platform-based, massively intermediated environments, however, techniques for behavioral surveillance and microtargeting have opened vast new horizons of opportunity, furthering the intertwined platform strategies of intermediation and legibility that Chapter 1 described. Both dominant platform firms like Amazon, Facebook, and Google and smaller, more specialized entities are continually experimenting with techniques designed to detect and record the minutest of pauses on a pageview or news item or the movements of a cursor hovering over a link, creating detailed simulacra of attention patterns and inferred personality traits that can be folded into existing systems for algorithmic intermediation.[38] Other new microtargeting initiatives deployed within platform-based environments attempt to detect users' mental and emotional states and personalize promotional messages accordingly. Facebook in particular has acknowledged conducting various experiments involving use of linguistic analysis to detect users' emotional states.[39]

Meanwhile, providers of online content have pursued methods of competing for attention and mindshare that harness both the insights of behavioral psychology and the properties of network organization. The reigning method of content optimization for user

engagement, pioneered by the founders of sites such as BuzzFeed and UpWorthy, involves a technique colloquially known as clickbait—"a style of headline that explicitly tease[s] readers, withholding just enough information to titillate them into reading further."[40] According to behavioral psychologists, clickbait exploits a nearly universal human dislike of being uninformed about something that everyone else already knows. Users will engage with the content by clicking through the headline in order not to be left out of the loop, and they will share what they find with their networks as a way of signaling inclusion to others.[41]

Like so much else in the online environment, the emphasis on content optimization for engagement reflects the importance of digital advertising revenues. Page views and clicks generate revenues, and when users share an item with others in their social networks, it may begin to spread virally, eliciting more page views and more clicks. In the wake of platform-driven cycles of consolidation and retrenchment in the print media industry, even long-established outlets for news and commentary now rely on services such as Chartbeat, a platform for tracking clicks, likes, and retweets, to help them refine their abilities to drive Web traffic. One result is that media outlets of all types increasingly rush to cover the same topics, lean heavily on techniques for manufacturing instant outrage, and frame their appeals for attention in the same breathless, you-won't-believe-what-happened-next tone.[42]

Platform-based providers of search, content aggregation, and social networking services operate at the intersection of behavioral microtargeting and content optimization for engagement. So, for example, Google's search engine uses behavioral cues together with its accumulated wealth of data about users to anticipate the type of content users want to find and adjust both autocomplete recommendations and search results accordingly.[43] Its content aggregation platform YouTube uses similar information to target video content; social networking providers such as Facebook and microblogging platforms such as Twitter function as de facto aggregators for a wide range of content and deliver feeds optimized to everything that is known or inferred about particular users' opinions and beliefs. By design, all of those algorithms incorporate feedback effects, and so their operation both reflects and continually reinforces the powerful economic motivation to pursue viral spread. That is where the law of unintended consequences kicks in. Within platform-based, massively-intermediated environments, the digital unconscious becomes a device for manipulating and activating subjectivity at scale. Platform-based intermediation alters collective behavior in ways that have begun to produce large-scale societal effects.[44]

Amplifying Collective Unreason

Some of the most transformative effects of networked, platform-based media infrastructures concern the ways that they alter and amplify the capabilities and behaviors of groups. Networked, platform-based architectures enhance the ability to form groups and share information among members, to harness the wisdom and creativity of crowds, and to coalesce in passionate, powerful mobs. They also, however, magnify the dark side of each of those forms of affiliation, collective meaning-making, and collective action. In particular, the spread of behavioral surveillance techniques into the domains of search and content distribution has produced powerful affordances for volatility, polarization, and public unreason.

Platform-based digital infrastructures' affordances for collective meaning-making are widely recognized. Just as networked digital 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, their political affiliations, their identity perspectives, their affiliations with real-world communities (such as neighborhood or parent-teacher associations), and so on. Like their counterparts in real space, online affinity groups provide friendship, intellectual and emotional affirmation, and shared organizational capacity. Unlike their real space counterparts, online affinity groups can extend over great distances and also can bridge other kinds of divides, connecting many who otherwise would not have met. The internet era has witnessed the emergence of a vast, diverse, and eclectic range of peer-based 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.[45] Search engines and crowd sourcing sites exploit the "wisdom of crowds," basing judgments about relevance and importance on the searching, linking, and upvoting behavior of millions of users.[46]

Platform-based digital infrastructures also both facilitate collective action and enable new forms of collective action. The landscape of networked collective action encompasses everything from spontaneous flash mobs to social action campaigns coordinated via Facebook pages, Twitter hashtags, and reddits to digital infrastructures for facilitating both traditional charitable giving and new types of "pay-it-forward" generosity. Networked information and communication technologies also have enabled rapid organization of mass protests, such as those mobilized by the Occupy Wall Street and Black Lives Matter movements and by pro-democracy activists during the political uprisings of the Arab Spring.[47]

The dominant cultural narratives about these cultural and political effects of platform-based interconnection have been celebratory, but other implications of the platform-based digital environment's affordances for collective meaning-making and collective action are less rosy. Distributed communities of peers have created and sustained thriving exchanges for malware and stolen personal information, as well as robust and seemingly impermeable alternate realities rooted in misinformation, junk science, and virulent forms of ideological extremism. Crowd-based judgments about the relevance, credibility, and urgency of online information can create cascades that lend sensationalized, false, and harmful online material extraordinary staying power, and those cascades can engender behaviors that cause both private and social harms.[48]

Platform-based, massively intermediated environments both expose and intensify political and ideological polarization around multiple, assertedly equivalent truths. Cultural and ideological polarization themselves are not new phenomena; in fact, social scientists who study political polarization have found that the percentages of Americans holding sharply opposing views on major political and cultural issues have remained fairly constant over the decades. What has changed is that percentages of respondents reporting strongly negative feelings about those with opposing views have skyrocketed.[49] That result stands in jarring contradiction to the utopianism of the early internet pioneers, who assumed that expanded access to information online would usher in a new era of cosmopolitanism and enlightened tolerance. Platform-based intermediation promotes

cosmopolitanism only to those users already inclined in that direction; to other users, it promotes other values.

A wealth of social science research shows that more homogenous groups—whether online or off—more readily become polarized in both their beliefs and their perceptions of reality. Algorithmic mediation of information flows intended to target controversial material to receptive audiences intensifies in-group effects, reinforcing existing biases, inculcating resistance to facts that contradict preferred narratives, and encouraging demonization and abuse of those who hold opposite beliefs and political goals. People do encounter other perspectives online, but exposure to opposing views is more likely to trigger automatic, instinctual rejection and anger than it is to promote reasoned engagement.[50] And platform affordances for volatility, engagement around sensationalized content, and ideological polarization have fueled the emergence of a vast alternative media ecosystem organized around conspiracist theorizing and hyperpartisan political outrage.[51]

Relatedly, platform-based information feeds flatten communicative hierarchies in a way that underscores the relative unimportance of claims to objective and/or empirical authority. A Facebook or Twitter feed, for example, presents the reader with a continuous stream of content within which all sources appear to be equivalent. That diminishes the privileged position once held by the three major broadcast networks and by national newspapers of record and invites both relativization and rejection of the possibility of objectivity; "all so-called experts are biased, any account partial, all conclusions the result of an arbitrary and premature closure of the debate."[52] Relativization fortifies alternate realities such as climate change denialism and anti-vaccination narratives and the echo chambers that support them. Relativization and infoglut also generate new types of power asymmetries that revolve around differential access to data and to the ability to capture, store, and process it on a massive scale. Under such conditions, techniques of critique and deconstruction increasingly become tools of powerful interests seeking to advance their own agendas.[53]

Platform affordances for cascade-based diffusion, polarization, and relativization are easily manipulated and weaponized. 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, some distributors had no particular political axe to grind, but instead were simply circulating content carefully designed to earn the clicks, views, shares, and retweets that generate advertising revenue. Other stories were sponsored by hostile state actors, and still others were sponsored by wealthy and highly motivated domestic interests seeking to reinforce and widen existing partisan divides. As they had hoped, groups predisposed to believe the worst of Clinton and her team shared, up-voted, and retweeted the stories.[54] Experts in election law and digital voting, watching carefully for signs of fraudulent tampering with digital voting machines, were unprepared for new kinds of digital disinformation and misinformation that took aim directly at voters' minds. Arguably, however, no-one should have been

surprised; the weeks leading up to both the earlier "Brexit" vote in the United Kingdom and the 2014 Russian incursions into Ukraine had followed similar patterns.[55]

Platform affordances also have fueled upsurges in ethnic nationalism, ideological extremism, identity-based harassment, and mob aggression. Affordances for networked collective action enable the rapid, ad hoc formation of angry, vengeful mobs, eager to shame real or apparent transgressors. Pioneering work by Danielle Citron in law and by Whitney Phillips in media studies explores the ways that networked, massively intermediated spaces reinforce and magnify the power of crowds to target selected individuals and groups. Women and members of racial, religious, and sexual minorities are especially frequent targets of crowd-sourced hate and intimidation.[56] More generally, investigations by multiple teams of researchers have explored the ways that platform-based, massively intermediated environments amplify bigotry and hate, intensify narratives about threats to national, racial, and religious purity, and propel coded memes into the limelight.[57] As a result of its increasing ubiquity and its algorithmically-mediated normalization, nativist and white supremacist hate-mongering bleeds inexorably into political discourse and public life. The pro-Brexit vote was influenced in part by narratives about the cultural and economic consequences of uncontrolled migration, and similar themes continue to shape elections and political debates across Europe and the United States. Activists affiliated with extremist movements have adopted cutting-edge content targeting techniques and sophisticated and ironic modes of outreach, and those efforts have gradually but inexorably shifted the tenor of public discourse, gaining in strength as outraged responses generate new information cascades and bringing bigotry and xenophobia into the mainstream.[58]

The increasingly unreasoning and often vicious 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. 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 networked information technologies have assumed within the political economy of informational capitalism also make them sites of extraordinary divisiveness and 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.

Can't Touch This: The Unbearable Lightness of Intermediation

As the platform-based, massively-intermediated information environment has evolved toward ever-greater efficiency as a tool for behavioral and cognitive conditioning, powerful information-economy actors have worked to craft narratives that make unaccountability for certain types of information harms seem logical, inevitable, and right. One important narrative mobilizes the idea of innovation to clothe commercial

information processing operations in a presumption of virtue. The discourse of information processing as innovation signals an important shift in the political economy of surveillance: the emergence of a *surveillance-innovation complex* within which advances in information processing are privileged for their own sake and regulatory oversight is systematically marginalized.

Two other important narratives mobilize the idea of freedom of expression to imbue information processing and data-driven, algorithmic intermediation with constitutional privilege. During the closing decades of the twentieth century, businesses of all sorts began to appropriate and repurpose the strand of the U.S. first amendment tradition that characterizes the public sphere as a *marketplace of ideas* to support robust anti-regulatory narratives that encompass a wide range of information-related activities. Information businesses have continued and expanded upon those efforts, and they also have begun to develop a new metaphoric frame that positions the networked information and communications environment as a depoliticized, self-regulating apparatus for truth production—an *information laboratory* that is, and should be, untouchable by protective regulation. Those efforts have proceeded in almost willful disregard of the fact that the networked digital information environment is neither neutral nor self-regulating, and they have catalyzed tectonic shifts in relations of accountability.

Within the Hohfeldian framework of entitlements and disentitlements with which this Part is concerned, the developments chronicled here are most aptly characterized as emergent legal immunities and correlative disabilities. Legal scholars exploring the meaning of the immunity-disability dyad have tended to focus on questions about the accountability of government actors.[59] In the networked information economy, at least, that approach is too hasty. Law entrenches informational immunity and correlative disability not only when it constrains or empowers the state, but also when it alters the legal relationships between private parties. We will see in this section that the intertwined *logics of innovative and expressive immunity* underwrite broad regimes of de jure and de facto insulation from accountability for internet intermediaries and other information businesses. They also deeply infuse the ongoing dialogues among policymakers and academics about the appropriate extent of accountability for information harms.

Innovation Jumps the Shark

Our story begins with a concerted effort by information businesses to recast discourses about information processing and its potential benefits and harms as discourses about innovation and the type of regulatory environment that it requires. In government proceedings and in the popular press, the information processing industries have worked to position innovation and protective regulation as intractably opposed. That strategy has produced a discursive process that infuses "innovation" with a particular, contingent meaning linked to economic liberty and the absence of government oversight.

Over the past decade or so, in proceedings convened by the Federal Trade Commission, the Department of Commerce, and the White House, in the debates that preceded the replacement of the European Data Protection Directive with the General Data Protection Regulation, and in ongoing discussions about the prospects for new U.S. legislation, members of the information processing industries—including platform firms, data brokers, and others—have advanced a carefully crafted narrative organized around

the themes of innovation and deregulation. Urging that "data-driven innovation can only occur if laws encourage use and reuse of data,"[60] they have argued that "industry self-regulation is flexible and can adapt to rapid changes in technology and consumer expectations, whereas legislation and government regulation can stifle innovation."[61] The rhetoric of freely flowing innovation as the lifeblood of the economy, and of regulation as its enemy, has been taken up by the libertarian think tanks and technology blogs, whose contributors work to offset what they view as alarmist narratives about the extent of commercial surveillance.[62] Meanwhile, commentators concerned to preserve the full range of potential benefits from future information processing—whatever those may be—worry that rights to withdraw one's data from databases or curtail uses of one's data, if widely exercised, would compromise the utility of those databases as resources for pattern identification.[63]

Implicit in rhetoric linking innovation with deregulation is a conception of innovation as an autonomous and inevitably beneficial process that is the natural result of human liberty. Importantly, that conception is relatively invulnerable to the standard science studies critique of public debates about technology policy, for it does not depend on deterministic assumptions about the inevitable, linear nature of scientific and technical progress. In the early twenty-first century, the idea of technological development as autonomous has been thoroughly debunked. Instead, both industry leaders and policy makers speak the language of diffusion studies, which emphasizes all of the contingent factors that can affect the market uptake of technological developments.[64] The understanding of diffusion studies that is current in business and regulatory circles, however, is a specifically market-centered one, and it puts a different kind of autonomy in play, which resides in the market itself. According to that understanding, invention may be historically and technologically contingent, but innovation is not. Innovations rise to the top of the pack as a result of the choices of self-interested actors, catalyzing a continual and inherently depoliticized process of social and economic betterment. And if innovation is autonomous, then what is produced is what should be produced. Regulators can only get in the way, and when they do we are all worse off, so they should not meddle.

Regulators, for their part, have responded to the rhetoric of autonomous, market-centered innovation by embracing the concept of a balance between two opposing goods. While rejecting the premise that regulation should simply defer to innovation in the digital era, they have accepted the more general proposition that privacy and innovation are in tension, and have turned back to conceptions of choice and consent as offering a way out of the resulting dilemma. In a series of reports expressly framing the privacy-innovation relationship as one of conflict, they have argued that a predictable legal framework for privacy protection is necessary to create user trust and foster the right climate for market acceptance.[65] U.S. regulators and diplomats have worked to soften the European Commission's regulatory stance on data protection, articulating justifications in which the theme of innovation is uppermost.[66]

The view of innovation as both inevitable and riskless is all the more remarkable because it is an anomaly. In the domains of environmental regulation and food and drug regulation, regulatory regimes have long endorsed the precautionary principle, which dictates caution in the face of as-yet-unknown and potentially significant risks.

Importantly, rather than stifling "innovation," the precautionary approach is widely recognized as creating incentive effects of its own, encouraging research and development in areas such as clean manufacturing and energy production, safe drug delivery, and the like.[67]

We will return to the problem of how to conduct precautionary regulation of information processing activities in Chapter 6; for now, I simply want to underscore that the understanding of information and information processing as definitionally exempt from precautionary regulation has persisted even as it has become increasingly difficult to maintain. Information processing has jumped the shark, running far ahead of the twentieth-century logic that animates our current, largely hands-off regulatory philosophy. There is mounting evidence about a wide variety of systemic threats created by digital infrastructures optimized for commercial surveillance: threats to the security of data transmission protocols anddata reservoirs, predatory pricing and discrimination in markets for financial services and consumer goods, large-scale manipulation of electoral processes, and amplification of junk science, organized hate, and virulent nationalism, and a more basic and pervasive corruption of public discourse.[68] As we saw in Chapter 1, the financial transactions that produced the economic bubble of the 2000's and the ensuing global financial collapse were triumphs of complex information processing. Before and after the crash, both financial leaders seeking to avoid regulation and the government officials charged with oversight responsibility invoked "innovation" to justify regulatory restraint.[69]

The rhetoric of information processing as innovation has been particularly powerful in the United States because it both derives from and mobilizes a distinctively American ideology about the power and promise of technology. Scholars such as Vincent Mosco and David Nye have documented the American inclination to believe that technology will subdue unruly nature and usher in an age of transcendent reason. For information industry thought leaders, faith in the "technological sublime" is a powerful motivator, reinforcing virtuous narratives about automated, data-driven surveillance and, for some, informing the confident expectation of a "singularity" waiting in our soon-to-be-realized future.[70] For economists and business scholars, it justifies confidence in a process that Austrian economist Joseph Schumpeter termed creative destruction: the sudden emergence of new forms of economic activity that both displace existing incumbents and disrupt the structure of existing markets.[71] For both groups, the way forward is clear: innovate first and clean up the mess (if any) later. (Or, put differently, move fast and break things, and then consider damage control strategies.).

The equation of innovation with economic liberty is not solely an American phenomenon, however. That framing of innovation has won adherents in some of the world's most important developing economies. As we saw in Chapter 2, India is embroiled in a bitter struggle over the future of data harvesting facilitated by the Aadhaar biometric identification system, and proponents of opening the "India Stack" to private innovation have included both multinational corporations and Indian entrepreneurs.[72] As Chapters 7 and 8 will discuss, the global platform firms Tencent and Alibaba are leading exponents of an emerging Chinese brand of informational capitalism characterized by closer and more openly acknowledged public-private partnerships in surveillance and control of information flow. For its part, the European technology sector has produced

few firms that can rival their U.S.- and China-based counterparts, and some scholars and policymakers on both sides of the Atlantic have concluded that the European data protection regime is at least partly to blame.[73]

Scholars who study surveillance have worked to draw attention to a surveillance-industrial complex in Western political economy: a symbiotic relationship between state surveillance and private-sector producers of surveillance technologies.[74] The surveillance-industrial complex encompasses a set of essential production relations: for surveillance technologies to be available, they must be produced, and for a market to exist, the technologies must be lawful and sought-after. Politically, however, the idea of a mutually beneficial relation between the state and producers of surveillance technologies has always been problematic, underscoring the degree to which systematic, focused observation of individual activities can threaten fundamental civil liberties. In the era of the "war on terror," support for government information gathering has become widespread, but the view that supervision and transparency are essential to minimizing surveillance abuses is also widely shared across the political spectrum.

The emerging *surveillance-innovation complex* represents a new, politically opportunistic phase of the symbiosis between surveillance and political economy, one that casts surveillance in an unambiguously progressive light and repositions it as a modality of economic growth. The surveillance-innovation complex is far more than a set of production relations. It is also a discursive formation that has as its purpose and effect not simply to legitimate surveillance but more fundamentally to give it sex appeal. Within the surveillance-industrial complex, surveillance is a necessary evil; within the surveillance-innovation complex, it is a force for unalloyed good. The resulting model of surveillance is light, politically nimble, and relatively impervious to regulatory constraint.

From Persuasion to Experimentation

A second strand of the ongoing legal and policy discussion about accountability for information harms involves attempts to constitutionalize data harvesting and processing activities. In recent decades a campaign has been underway to insulate all forms of commercial information processing from regulatory oversight by invoking the First Amendment's protection for freedom of speech. It has mobilized two powerful metaphoric frames: the familiar conception of the public sphere as a *marketplace of ideas*—a site where the laws of supply and demand produce high-quality information—and a newer conception of the platform-based, massively-intermediated public sphere as an *information laboratory*—a site where beneficial experimentation yields new forms of datafied and depoliticized truth.

Historically speaking, a striking aspect of the campaign to constitutionalize all information-related regulation is the relative novelty—even for the U.S.—of the theory of expressive liberty that it seeks to enshrine. As has been ably chronicled elsewhere, corporate attainment of constitutional personhood did not follow inevitably from constitutional text or history but rather was the fruit of a long and carefully strategized legal and public relations campaign.[75] Even so, 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.

In the late twentieth century, an anti-regulatory agenda refined in law review articles and strategy sessions at libertarian and neoliberal think tanks began to produce a steady stream of First Amendment challenges to regulatory activity.[76] The initial cases challenged regulations targeting various types of complex corporate and professional messaging. They produced what became known as the commercial speech doctrine—a type of intermediate constitutional scrutiny that attempted to strike a balance between protecting speech interests and preserving room for the protective regulation necessary in complex, increasingly informationalized markets.[77] Meanwhile, the various internal information processing activities that firms had begun to undertake—activities afforded by new technologies for computing and data storage—were not on constitutional litigators' radar screens at all. Today, both parts of that equation have changed. The test developed by the courts for evaluating the legitimacy of regulations targeting corporate communications is under sustained assault for being too lenient, and information processing is in the spotlight.

The contemporary First Amendment anti-regulatory agenda blends rigid doctrinal logic and entrepreneurial, expansionist expressions of neoliberal governmentality together in a potent cocktail. According to the most widely held definition, "commercial speech" includes only direct-to-consumer communications—communications that "propose a commercial transaction." When other types of corporate information processing activities were not considered speech at all, a narrow definition of commercial speech simply would have excluded them from the First Amendment landscape. If those other activities do count as speech, however, the fact that they are not "commercial speech" bolsters arguments for stricter scrutiny of regulations that burden them. In particular, regimes of economic regulation generally begin with scope limitations identifying particular types of content and/or particular actors. Other strands of First Amendment jurisprudence, however, label such distinctions as requiring compelling justification and the narrowest possible tailoring, and that doctrinal structure has enabled arguments for regulatory minimization to find easy points of entry.

The contemporary First Amendment anti-regulatory agenda also relies on a particular, distinctively neoliberal reading of the marketplace-of-ideas metaphor. As originally elaborated by judges and commentators conversant with liberal political theory, the metaphor connoted an arena for deliberate, reasoned exchange, where the ideas on offer could be evaluated on their merits. The neoliberal anti-regulatory reading is more literal: the marketplace of ideas is an arena where the volume and quality of information are—and should be—regulated only by the laws of supply and demand, and where those making decisions about the quality of information function as separate, individual nodes of rationality.[78] So, for example, businesses challenging mandatory disclosure and labeling requirements argue that the government is simply interposing its own opinions about what information consumers ought to want before making marketplace decisions, and businesses challenging regulations on other kinds of information processing argue that the regulations distort the natural and normal operation of the marketplace.

In a notable recent victory for both the campaign to constitutionalize information processing and the neoliberal reading of the marketplace metaphor, a majority of the Supreme Court ruled that a Vermont statute prohibiting pharmaceutical companies' use

of prescriber-identifying information for marketing purposes—a practice known as "detailing"—must survive strict scrutiny because the restriction was both content- and speaker-based.[79] The state legislature had enacted the law because it feared that allowing detailers to conduct data mining operations in the state's prescription drug database and use the information to market more costly proprietary drugs would drive up the cost of its Medicaid prescription drug program. The majority, however, saw the state's action as an attempt to undermine the persuasive force of pharmaceutical marketers' speech.[80]

Sorrell, however, also suggests the marketplace metaphor's logical limits. The detailing activities in *Sorrell* targeted physicians rather than their patients, so the issue was not squarely joined, but data-driven targeting is different from persuasion along a critical dimension that has to do with transparency and manipulation. As we saw in Chapter 2, the operative principle behind predictive data processing is the preemptive nudge rather than the reasoned comparison among alternatives, and its point is surplus extraction, pure and simple. Its goal is to minimize the need to persuade by targeting those potential customers most strongly predisposed to buy and crafting appeals based on their habits and predilections. Constitutional challenges to mandatory labeling and disclosure requirements similarly ignore that direct-to-consumer information is pervasively manipulated. Today, even basic consumer products increasingly come with a bewildering amount of information attached—consider, for example, nutrition-related marketing claims and the conflicting recommendations that they engender. In markets for information-related goods and services, and in online marketplaces for goods and services of all sorts, consumer awareness is even easier to manipulate because the purchase interaction can be designed in ways that lead consumers to overlook or minimize crucial terms of the deal.[81]

Platform-based, massively-intermediated processes of search, content aggregation, and social networking strain the marketplace metaphor past the breaking point. As this chapter has explained, platform-based environments optimized for behavioral surveillance and microtargeting operate—and are systematically designed to operate—in ways that preclude even the most perceptive and reasonable consumer from evaluating the goods, services, and information on offer. Advertisers use platforms' services precisely to ensure that different users see different offers. Techniques for behavioral microtargeting and content optimization attempt to bypass reason and persuasion altogether—and, as we have also seen, those techniques produce other harmful effects that manifest at scale. At minimum, information businesses are complicit in fostering the information cascades that draw eyeballs and generate ad revenues—and some have been silent partners in fostering the conspiracy theories, extremism, and violence that they officially disclaim.[82]

Unfazed by mounting scrutiny on these issues, platform businesses have worked to recast their pervasive manipulations of the information environment in the service of profit extraction as scientific truth-discovery processes. Platform-based media infrastructures, they argue, are laboratories in which providers of information services experiment to see which types of information are most useful and most responsive to consumers' needs.[83] 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.[84] A 2014 paper coauthored by a Facebook data scientist described varying items in users' newsfeeds and then using automated discourse analysis tools on those users' own subsequent posts to gauge the effects of the newsfeeds on their emotional states. When critics decried Facebook's failure to give users prior notice of the experiment, Facebook's defenders pointed out that marketing is inherently a science of experimentation. In a stark demonstration of its own power to influence political processes, Facebook also has acknowledged, and has seemed to expect public approbation for, experimenting with ways of delivering "get out and vote" messages.[85]

The metaphoric frame of the information laboratory appropriates and repurposes the neoliberalized, innovation-centered trope of the surveillance-innovation complex as a constitutional trump. It solidifies the positioning of surveillance as an activity that is virtuous, productive, and therefore rightly exempted from legal and social control. Within the frame of the information laboratory, the fact that online information intermediaries manipulate meaning in ways and for purposes that they do not disclose is of little moment. Similarly, the recent troubling demonstrations that platform-based, massively-intermediated media infrastructures have played pivotal roles in fostering and amplifying deeply entrenched political polarization that extends all the way down to bedrock narratives about reality and scientific fact becomes a matter best left to the experts in the white lab coats to sort out.

In short, the information laboratory is a First Amendment metaphor optimized for what platforms do. From Google's description of its mission to "organize the world's information and make it universally accessible and useful" to Mark Zuckerberg's insistence that Facebook represents a space for people to build community and resolve their differences, platform firms' self-descriptions imagine a public sphere continually structured and restructured for optimal utility by enlightened stewards.[86] They position the information laboratory as supplying the public sphere's essential infrastructure. In those formulations, the platform is the solution to all of the world's information needs, and if it is the solution, it cannot possibly be the problem.

The Most Important Law

Debates about whether and when platform providers and other information intermediaries should be accountable to private plaintiffs for information-related harms are pervasively structured by the logics of innovative and expressive immunity. In the United States, efforts to insulate information intermediaries from liability bore early fruit in section 230 of the Communications Decency Act (CDA), which was enacted as part of the Telecommunications Act of 1996 and granted broad immunity to providers of "interactive computer services" for their roles in distributing speech produced by others. A broad coalition of information businesses and digital civil liberties advocates has worked strenuously to defend that institutional settlement, mobilizing the interlocking frames of the surveillance-innovation complex, the marketplace of ideas, and the information laboratory and downplaying the extent to which intermediaries shape both the content that users see and the contexts within which that content is offered.

After early court decisions in defamation cases against internet access providers suggested a risk of significant liability for an emerging industry that promised to create unprecedented opportunities for both expression and commercial development, early

internet intermediaries and their supporters pushed Congress to establish clear rules precluding liability for those merely furnishing conduits or platforms for speech by third parties. Invoking the familiar idea of media technologies as technologies of freedom, they prophesied that a broad grant of immunity would promote the spread of online commerce and the flowering of public discourse. Sympathetic members of Congress obliged by inserting into a comprehensive telecommunications reform bill language that not only granted information intermediaries immunity for defamatory speech published by others but also extended that immunity well beyond the bounds of existing defamation law to encompass an open-ended group of information-related harms.[87]

The language and legislative history of the CDA showcase both the marketplace and laboratory frames that now dominate debates about information and communications policy—and illustrate their uneasy juxtaposition. The language of section 230—titled "protection for private blocking and screening of offensive material"—expressed the hope that internet access providers, acting as "Good Samaritans," would develop and make available to consumers tools for filtering out undesirable content. (As Chapter 4 will discuss, the new law also included an ill-fated attempt to establish broad liability for those directly providing indecent content online.) At the same time, both in the legislative history and in individual statements, members of Congress endorsed the marketplace metaphor as a principal justification for section 230's broad grant of immunity, stating their belief that immunity for infrastructure providers would foster and preserve the emerging network as a vibrant marketplace of ideas.[88] That language framed still-emergent networked information architectures as neutral speech engines that would simply reflect and transmit what people wanted to say. In other words, it implicitly posited the internet as a neutral space lacking the sorts of specific affordances that might themselves shape communicative practices and communicative content, even as the good Samaritan language both invited manipulation and invested it with innovative virtue.

The impact of section 230 on the litigation landscape has been stark. Courts have interpreted the statutory language as eliminating not only traditional publisher liability for defamation but also distributor liability for intermediaries possessing knowledge of falsity and ongoing harm. Today, defamation lawsuits against information platform providers are routinely found to be preempted by the statute, as are many other kinds of claims involving actionable falsity—for example, business tort claims alleging an intermediary's participation in false advertising or unfair competition. 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 lawsuits alleging a wide variety of other harms ranging from discrimination to market manipulation.[89] 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.[90]

Two features of the contemporary debate about intermediary immunity are especially striking. One is the widespread refusal by judges, policymakers, and legal scholars to pay careful attention to what platform-based online intermediaries do. Views about the unassailable rightness of intermediary immunity have solidified even as time and technological change have undermined the presumptions of truth production and technological neutrality that section 230's proponents emphasized. As we saw earlier in

this chapter, today's platform-based, massively intermediated information environment has attributes that Congress in 1996 could not have imagined; it is continually manipulated by techniques for detecting and predicting predilections, calibrating commercial and affective appeal, and structuring information feeds accordingly.

Attempts to focus judicial attention on these issues are rapidly hijacked by injured protestations of innocence and expressive virtue. As James Grimmelmann has painstakingly demonstrated, search engines have become adept at insisting on their neutrality for purposes of section 230 even while claiming that their search results are their own constitutionally protected speech.[91] For the most part, courts have uncritically accepted both sets of arguments, concluding both that algorithmic intermediation doesn't make an intermediary a publisher of other people's speech and that the same processes of intermediation are speech-like in their own right. Digital civil liberties organizations, meanwhile, have christened section 230 the internet era's "most important law" and have argued that altering the terms of the balance struck in 1996—near-complete immunity in exchange for voluntary self-oversight—would spell disaster for both freedom of expression and the internet economy. That proposition has commanded broad consensus even among commentators otherwise inclined to be critical of platforms, the speech environments they provide, and their approaches to self-governance.[92]

The second striking feature of the contemporary debate about intermediary immunity concerns the widespread consensus about what intermediary companies are not: they are not "media companies."[93] Intermediaries' continued insistence on that distinction may seem increasingly disingenuous, but it is carefully crafted to maintain a strategic distance between the activities of content provision and data-driven, algorithmic intermediation.

From one perspective, the attempted distinction between a content provider such as Disney, HBO, Fox News, or the *New York Times* and a giant platform provider such as Facebook or Google's YouTube is powerfully anachronistic. Despite the Supreme Court's relatively recent pronouncement that "television networks and major newspapers" are "the most important means of mass communications in modern times," internet platforms play an increasingly important and multifaceted role in structuring the universe of information that people see.[94] For some people, online services long ago eclipsed television networks and major newspapers as information sources. Both the continuing collapse of the print newspaper industry and the continuing dramatic increases in mobile device ownership suggest that the proportion of the population that relies on television and print newspapers for current events coverage will continue to decline.[95] There is also a pervasive interplay between web-based content and mainstream media content that attempts to distinguish between the two typically overlook. Many people who rely on traditional news sources also rely on giant platform businesses to serve as news aggregators. Traditional media cover topics that are trending online and use techniques for maximizing user engagement once that coverage migrates back online, and political interest groups seeking to influence mainstream media coverage of particular topics exploit that dynamic for their own purposes.[96]

From another perspective, maintaining a bright-line distinction between content providers and online intermediaries is essential to avoiding closer scrutiny of the ways that data-driven, algorithmic intermediation shapes content. Within the U.S.

constitutional tradition, media companies are paradigmatic speakers, and Supreme Court decisions in cases challenging both media and election regulation have positioned ownership of the means of communication as the ultimate touchstone of expressive freedom.[97] Consistent with that orientation, the dominant approach to media regulation holds that technological distribution bottlenecks are the principal obstacles to market entry by new media owners. As the concentrated broadcast markets of the middle twentieth century gave way to more complex infrastructures for cable and satellite distribution, that approach became a recipe for deregulation, and the deregulatory consensus has endured even as consolidation in both local and nationwide media markets has become increasingly pronounced.[98] That might change, however, if public and legislative attention were to focus on intermediated news feeds and the distributed sociotechnical systems that enable giant platform firms to control and manipulate them. As things stand, media law and policy in the United States have almost nothing to say about the activities of online intermediaries, and platform firms would like to keep it that way.

So read, the internal contradictions in intermediaries' descriptions of what they are and are not have a very particular purpose. They work to define a new category of information-related activity that consists of non-content-based expression—that is simultaneously in between users and content (and therefore not content) and useful to users who want content (and therefore expressive). Because its purveyors are not providing content, they are both definitionally exempt from legacy regimes of media regulation and beneath the radar of enterprising regulators who might be seeking to update those regimes. Because what they provide gives the torrent of online information a more definite structure, it can be described as advancing the information laboratory's experimental mission, and it can be named in a way that comports with that mission—as providing both utility and *moderation*.[99] The language of moderation simultaneously proclaims intermediaries' virtue—signaling that they have become the good Samaritans that Congress envisioned—and diverts attention from questions about why flows of online information are *im*moderate to begin with. It therefore represents a significant narrative triumph.

European legal regimes have demanded more from information businesses, but those demands also have presented the opportunity for more intensive and opaque self-regulation of information flows in networked spaces. The evolution of the so-called "right to be forgotten" for data subjects is illustrative. Led by Google, which lost a key decision in the European Court of Justice on delinking of old, potentially damaging information, information businesses bitterly criticized the initial articulations of the right by European jurists and officials. Relying heavily on the frame of the information laboratory as depoliticized truth engine, they characterized takedown requests as efforts to subtract information from the historical record, making the remaining information less authentic and complete. In the media, they also pursued a strategy of widely publicizing the inevitable outrageous requests while barely acknowledging the many legitimate ones.[100] Reading the headlines, one would not understand that both the European Court of Justice and the Commission had clearly articulated the need to consider public interests in freedom of speech and access to information and had carefully distinguished between linking and indexing by search engines and online archiving by originating sites.[101] When the dust settled, though, Google itself had put in place takedown procedures that

performed the very same role it had claimed was both impossible and unwise.[102] As Chapter 4 will discuss in more detail, European debates about platforms' roles in the circulation of terrorist and hate speech have begun to follow a similar path.

Identity and Authentication in the Cloud

A final set of emergent informational immunities is de facto rather than de jure, and is more broadly distributed. As an increasing amount of commercial and government activity moves onto the network, providers of networked information services—including information platform businesses but also financial institutions, healthcare providers, retailers, and government agencies—have become custodians of valuable and sensitive personal information. Nearly everyone, whether knowingly or not, is a user of networked services, and poor security for confidential personal information magnifies users' vulnerability to fraud and identity theft. Custodians of sensitive personal information share a common need to protect against both malicious actors and accidental leaks—and common interests in shifting the risks of losses onto consumers and each other. As they have labored to minimize their exposure to direct regulatory oversight, they have developed a common playbook that involves mobilizing the logic of innovative immunity to justify private governance of data risk.

According to both marketers and policymakers, the future of paperless transactions and networked, remotely controlled devices is rosy. Ad campaigns entice consumers to do their banking by phone, to control their home security systems and personal health records remotely, and to rely on networked medical devices to keep their hearts pumping or their insulin at appropriate levels. They promise convenient and fail-safe storage of personal documents and data in the cloud and offer cloud-based computing services as cheap and powerful substitutes for local computing power. In the very near future, we are told, driverless cars will ferry us to our destinations, leaving even more time for productive intangible labor, while driverless trucks and drones will ensure the just-in-time delivery of those physical goods that we still require.[103]

The sunny optimism of ads and policy discussions about the future of the networked informational economy belies a seemingly continuous stream of major data breaches and epidemic levels of fraud and identity theft. For any particular user, vulnerability is a given, and eventual loss seems only a matter of time.[104] Distributed information architectures protect against localized data losses but at the same time create new and unprecedented systemic and personal vulnerabilities. Large data reservoirs make enticing targets, and widespread norms of promiscuous data harvesting and processing undercut incentives to minimize collection and maximize security at the front end.

Information businesses do not dispute the large and growing threats to the security of personal information; they just do not seem to think the law can or should provide much help. Invoking the narrative of the surveillance-innovation complex, they stress the "burdensome" nature of formal legal obligations, insisting that security should be left in the domain of private best practices.[105] A second and related strand in the campaign against legal accountability invokes the concept of acceptable losses; tighter security practices, they argue, would be "wasteful," though the baseline for that determination is left unspecified.[106] A third strand invokes the language of fault and moral responsibility; blameless information providers, we are told, should not be called to account for the

criminal acts of third parties.[107] Last, and in ironic tension with the marketplace-of-ideas frame, business interests argue that disclosures about data breaches and system vulnerabilities would be "confusing" to consumers.[108]

Among policymakers and academics, there has been a long-running debate over whether the de facto standard of care for entities holding consumer or citizen personal information can be raised simply by enacting so-called data breach notification laws mandating disclosure of incidents. Proponents of the notification approach maintain that disclosure will enable the market to penalize vendors with poor security practices. Opponents object that that prediction lacks foundation in reality. Consumers' abilities to police the terms of online transactions are extremely limited. Data security in particular is a highly complex dimension of transactions that people enter for other reasons, and security levels are not subject to a la carte variation, so it's hard to imagine that greater disclosure would lead to greater consumer empowerment.[109] Put differently, although information businesses' sudden upsurge of concern about consumer confusion is deeply disingenuous, there is more than a grain of truth to it.

Whether data breach notification laws will "work," however, does not really seem to be the point of debates about whether to enact them. Instead, debates about the power of information in an idealized marketplace of custodial services for personal data distract lawmakers from questions about whether and how to impose more substantive security obligations. Perhaps unsurprisingly, most of the laws that have been enacted are weak. Of the 47 U.S. states that have enacted data breach notification laws, about one-third have afforded consumers a private right of action, but the right of action covers only failure to notify. (Additionally, as we will see in Chapter 5, consumer suits alleging privacy harms face many other hurdles.) Provisions authorizing enforcement by state attorneys general similarly focus narrowly on the problem of adequate notification; none defines substantive security-related obligations that data custodians must meet.[110] Congress so far has not acted at all. In contrast, the European Union's new General Data Protection Regulation adopts both data breach notification requirements and substantive data security obligations, although the content of the latter remains to be determined.[111]

In the United States, the Federal Trade Commission has stepped into the breach, asserting authority to police data security practices as an offshoot of its more general jurisdiction over unfair and deceptive acts and practices in commerce. The FTC's Consumer Protection Division has sought and won a series of high-profile consent decrees establishing commitments to meet industry standard best practices. The National Institute of Standards and Technology has endorsed a data security standard reflecting a composite of industry best practices, and that standard now informs FTC enforcement activity. We will consider those efforts more closely in Chapter 6. Some affected industries, however, have resisted even that relatively relaxed level of oversight, mounting court challenges asserting that the FTC lacks jurisdiction to oversee data security at all.[112]

Financial institutions also have sought to hold retailers to higher standards, but the baseline presumptions of private ordering and private governance of security standards have powerfully shaped the discourse around the kinds of obligations that information businesses reasonably can be expected to assume. New payment provider rules incentivize brick-and-mortar retailers to adopt microchip-based credit card readers by

shifting liability to merchants who do not use the technology. As Adam Levitin explains, however, the various interests involved in existing and emerging payment systems markets have principally sought to shape rules about risk allocation in ways that enhance their own competitive position vis-à-vis one another.[113] And financial institutions acting as plaintiffs are poorly placed to vindicate the more significant harms flowing from pervasive insecurity, which concern the loss of control over personal identifiers that are difficult or impossible to change.

The result for consumers is utter powerlessness. Anyone who has ever received a data breach notification and thought about the extent of his or her ability to respond knows that there is very little to be done. The recommended strategy—to double down on the personal information economy by handing over one's personal financial information to a credit monitoring service that will be happy to charge a monthly fee for monitoring accounts and trolling online black markets—does not inspire confidence. Ultimately, the business lobbies are right that debates about security standards are about acceptable losses, but the losses have names and faces. The logics of innovative and expressive immunity dictate a high baseline level of tolerance for human vulnerability in the interest of unfettered commerce.

The Culture of Capture

The interlocking frames of the surveillance-innovation complex, the marketplace of ideas, and the information laboratory express a distinctively neoliberal ideology within which profit-motivated private enterprises are appropriate and morally virtuous guarantors of social progress, expressive liberty, and robust debate about matters of public importance. Over time, that ideology has produced a powerful anti-regulatory force field that affords information businesses an extra layer of insulation against efforts to create new forms of legal accountability. A helpful framework for understanding that force field is the idea of "deep capture," or capture on the level of ideology.[114] The intertwined frames of the information marketplace and the information laboratory have attained the status of ground truths, and the mainstream of thought about optimal public policy has come to reflect their unquestioned rightness.

Scholars who study the relationships between regulators and regulated entities have recognized for some time that morality tales in which regulatory capture proceeds via naked assertions of economic power are far too simple. Generally speaking, regulators understand themselves as acting in the public interest and care about underlying legal and policy narratives of right and obligation. Powerful actors also use their resources to reshape those narratives, however, supplying a range of inputs that include legal arguments, economic models, empirical studies, opinion polls testing public responses to carefully crafted questions, and compelling rhetorical and metaphoric devices for framing descriptions and arguments. Those inputs function as information subsidies, supplying policymakers who have limited resources of their own with ready access to a trove of facts, anecdotes, theories, and narrative frameworks from which to draw.[115] Information-economy actors are no different.

Platform-based information infrastructures have provided unprecedented opportunities for advocacy groups to communicate their visions for a future unencumbered by regulatory meddling directly and simultaneously to policymakers,

journalists, and the public. The landscape is busy and complex, characterized by a dense and interlocking network of ties between and among for-profit firms, wealthy individuals, industry trade associations, and ostensibly nonprofit entities with grand- and objective-sounding names.[116] A flood of research output, carefully burnished with a shiny patina of objectivity but of varying quality, circulates continually via press releases and social media, deluging regulators, commentators, and the public in a glut of messaging. Innovation and the deregulatory climate ostensibly necessary to foster and sustain it are popular topics, and claims about autonomous innovation, productive experimentation, and virtuous moderation gain legitimacy in part through their incessant repetition.

Alarmist rhetoric about the downside risks of government intrusion into processes better managed by the private sector also plays an important role in shaping regulatory and public opinion. Consider again the disputes about the scope and wisdom of the statutory immunity afforded by section 230. Another interesting feature of those debates is the stridency of section 230's defenders. Attempts to bring legislative and technological creativity to bear on the increasingly incontrovertible evidence of platform affordances for hate, unreason, harassment, and intimidation are routinely met with carefully tended hysteria about censorship. Libertarian tech policy pundits have trumpeted their alarm about purported attacks on "The Most Important Law about the Internet," painting proposals by thoughtful scholars and commentators as stalking horses for censorship and authoritarian rule. Female proponents of legislation addressing such issues as cyberstalking and revenge porn have come in for particularly scathing ridicule.[117]

A different and more subtle example of the effects of framing on public discourse about information policy is the rise and fall of the "information superhighway" metaphor that dominated information policy discourse in the 1990s and early 2000s. Formerly ubiquitous, the metaphor is now widely mocked as outdated and technically unsophisticated.[118] Yet it invited regulatory scrutiny and oversight in a way that the cloud metaphor does not. To take just one example of a comparison that the superhighway metaphor invites, we don't define passive restraint obligations solely by reference to industry-determined best practices in automotive design or by relying on financial intermediaries to sue automakers for manufacturing and design defects. The cloud metaphor, by contrast, actively resists regulatory oversight; the essence of clouds lies precisely in their ability to evade our grasp.[119] The move to the cloud asserts the primacy of private ordering, and the results are far from ethereal. The vulnerabilities resulting from inadequate security may be informational rather than physical, but they are both real and pervasive.

As these examples suggest, deep capture strategies are concerned not only with results in particular cases but also with crafting and reinforcing master narratives that become deeply internalized, and they do not target only regulators but also cultural influencers, public intellectuals, and academic thought leaders.[120]

Some deep capture strategies, however, have targeted the scholarly community specifically. Google/Alphabet in particular has spent lavishly to fund academic centers and research fellowships; other platform giants, most notably Microsoft, have built affiliated research groups and recruited leading scholars in new media, information studies, and technology studies to staff them.[121] Data-mining company Palantir has

constituted a blue-ribbon advisory board composed of prominent privacy scholars while continuing to offer a core suite of products and services designed to give federal, state, and local law enforcement the ability to conduct pervasive, collaborative, long-term dataveillance of populations.[122] More generally, scholars in a variety of fields, but especially in law, public policy, and economics, have eagerly embraced both new platform-based tools for reputation-building and new opportunities funded by technology companies to mingle face-to-face with journalists, public intellectuals, government officials, and prominent entrepreneurs.[123]

In the case of Google/Alphabet, a 2017 scandal involving the firing of the entire competition group at a Google-funded policy think tank made especially clear that the massive outlays in support of policy research do have a few strings attached.[124] Allegations of influence-manufacturing levied by Google's competitors, however, often ring hollow. One recent loudly publicized effort to raise questions about Google's investments in scholarly production fell flat after it was revealed that funding for the initiative had come from a company embroiled in litigation with Google and that the data quality was poor and the allegations of bias unsubstantiated and scattershot.[125] Google is simply very good at a game that is much more widely played, and whose tacit rules and conditions are well understood.

As channels for influencing public and policymaker opinion have proliferated and the quest to become an influencer has intensified—and as the intermingling of academic and corporate-funded information policy research has become more pervasive—the boundaries of scholarship as a category have become correspondingly less clear. Policy interventions in the domain of information policy exist on a continuum that encompasses everything from scholarly books and articles to think-tank-funded books, position papers, and amicus briefs to op-eds and opinion columns to blogs and tweets. Many pieces of legal and economic scholarship in particular are versioned in all of these forms, making it hard to tell where on the continuum and from what stance relative to the policy process they originated.

For their part, scholars who have benefitted personally or institutionally from the largesse of information-economy firms bristle at the suggestion that they might have been co-opted as a result. Their research agendas and opinions, they insist, remain their own. That answer is not wrong so much as it is incomplete. The power of cultural conditioning is deep. Like the divine right of kings in the age of exploration, or like manifest destiny during the westward settlement of the Americas, the logics of innovative and expressive immunity are fast on the way to becoming constitutive ideologies of the economic age. They are both inextricably intertwined with the reigning governmentality and experienced by those invoking them as simply just so.

Law and the Construction of Information Power, Revisited

As patterns of immunity for informational harms have crystallized, they have begun to reflect an increasingly stark imbalance. Information platforms and other information businesses are largely unaccountable for practices of behavioral microtargeting and content optimization that amplify collective unreason and for the security vulnerabilities that distributed architectures for data harvesting, storage, and

processing engender. Ordinary individuals, meanwhile, are left essentially unprotected against a wide range of very real harms, and processes that have worked for centuries to foster deliberative dialogue and democratic self-government are revealed to be newly fragile and unthinkably vulnerable.

Defenders of free speech at any cost are right to note that throughout history, moral panics about new communication technologies have produced calls for censorship and control. As we are about to see in Chapter 4, that pattern continues today. But the history of information and communication technologies—like that of other new technologies—is not simply a history of moral panics, legal overcorrections, and heroic libertarian struggles. New sociotechnical relations surrounding communication, participation, and power have both challenged and reinforced economic and political power, and those struggling to define the conditions of information exchange and control have advanced a diverse variety of goals and interests. In the contemporary information economy, the ongoing construction of constitutional, statutory, and de facto immunities for information-processing activities principally benefits powerful economic interests in their quest to construct a device for jacking directly into the volatile and fractious collective id.

The communicative spaces produced by platform-based, massively intermediated information infrastructures are not neutral spaces. They are spaces optimized for eliciting automatic, instinctual reactions and for engendering, amplifying, and exploiting cascade-based diffusion, polarization, and relativization. Public discourse in a democratic society is, and should be, contentious and unruly, but there is also a difference between bending and breaking. Constitutional and policy precepts formulated under different sociotechnical conditions do not automatically port to the conditions that now exist; they must be translated. Conceptual frameworks that begin by defining the problems away do not simply disable courts and policymakers from crafting appropriate forms of regulatory oversight. They make the possibility of finding a different way forward difficult even to imagine.

---

[1] Ithiel De Sola Pool, *Technologies of Freedom* (Cambridge, Mass.: Harvard University Press, 1983); see also Jack Balkin, "Digital Speech and Democratic Culture," *New York University Law Review* 79(1) (2004): 1-58.

[2] Mark Andrejevic, *Infoglut: How Too Much Information Is Changing the Way We Think and Know* (New York: Routledge, 2013), 9-10.

[3] Andrejevic, *Infoglut*, 2-3.

[4] For an overview, see Paul D. MacLean, "The Limbic System ('Visceral Brain') in Relation to Central Gray and Reticulum of the Brain Stem: Evidence of Interdependence in Emotional Processes," *Psychosomatic Medicine* 17 no. 5 (1955): 355-366. Current models have moved beyond rigid functional segregation to recognize that, for example, the neurological processes that produce learning and memory extend across multiple brain regions. Within those models, however, the structures in the limbic region remain pivotal. See, for example, James L. McGaugh, et al., "Involvement of the Amygdala in Memory Storage: Interaction with Other Brain Systems," *PNAS* 93 no. 24 (1996): 13508-13514.

[5] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Hachette, 2019), 351-52, 376-97.

[6] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Northampton, Mass.:, Edward Elgar, 2015), 41-46, 56-61, 66-67.

[7] Erving Goffman, *The Presentation of Self in Everyday Life* (New York: Anchor Books, 1959).

[8] Scholarly and popular commentary on reputation as a source of individual concern most often focuses on social and professional embarrassment when isolated facts or falsehoods can be taken out of context. See, for example, Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven, Conn.: Yale University Press, 2007), 30-35; Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, 2000). That fundamentally human-centered account of how reputation is created is only part of the story.

[9] Josh Lauer, "From Rumor to Written Record: Credit Reporting and the Invention of Financial Identity in Nineteenth-Century America," *Technology and Culture* 49 no. 2 (2008): 301-324; Josh Lauer, "The Good Consumer: Credit Reporting and the Invention of Financial Identity in the United States, 1840-1940," *Enterprise and Society* 11 no. 4 (2010): 686-694.

[10] "Statement of the Fair Isaac Corporation before the U.S. House of Representatives" (July 28, 2008), https://perma.cc/P3QW-7QSX; Martha Poon, "Scorecards as Devices for Consumer Credit: The Case of Fair, Isaac & Company Incorporated," *The Sociological Review* 55 no. s2 (2007): 284-306.

[11] Robinson + Yu, "Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace" (Oct. 2014), https://perma.cc/283P-FFGF.

[12] Mary L. Carsky, Roger L. Dickinson, & Charles R. Canedy III, "The Evolution of Quality in Consumer Goods," *Journal of Macromarketing* 18 no. 2 (1998): 132-44; Hayagreeva Rao, "Caveat Emptor: The Construction of Nonprofit Consumer Watchdog Organizations," *American Journal of Sociology* 103 no. 4 (1998): 912-61; Lauren Strach & Malcolm Russell, "The Good Housekeeping Seal of Approval: From Innovative Consumer Protection to Popular Badge of Quality," *Essays in Economic & Business History* 21 (2003): 151-166.

[13] Michele Knobel & Colin Lankshear,"What Am I Bid? Reading, Writing, and Ratings at eBay.com," in *Silicon Literacies: Communication, Innovation and Education in the Electronic Age*, ed. Ilana Snyder (New York: Routledge, 2002), 15-30; Axel Bruns, *Gatewatching: Collaborative Online News Production* (New York: Peter Lang, 2005), 31-52.

[14] For a representative sampling of academic thought experiments, see Hasan Masum, Mark Tovey, & Yi-Cheng Zhang, *The Reputation Society* (Cambridge, Mass.: MIT Press, 2011).

[15] Mihaly Heder, "A Black Market for Upvotes and Likes," Working Paper (Mar. 19, 2018), arXiv:1803.07029 ; Michael Luca & Giorgios Zervas, "Fake It Till You Make It: Reputation, Competition, and Yelp Review Fraud," *Management Science* 62 no. 12 (2016): 3412-3427; Dina Mayzlin, Yaniv Dover, & Judith Chevalier, "Promotional Reviews: An Empirical Investigation of Online Review Manipulation," *American Economic Review* 104 no. 8 (2014): 2421-2455.

[16] danah boyd, *It's Complicated: The Social Lives of Networked Teens* (New Haven, Conn.: Yale University Press, 2014); Alice Marwick & danah boyd, "'It's Just Drama': Teen Perspectives on Conflict and Aggression in a Networked Era," *Journal of Youth Studies* 17 no. 9 (2014): 1187-1204.

[17] Ken Bolton, "Manage Your Online Reputation," *Information Outlook* 17 no. 4 (2013): 10-12; Stephanie Kelly, Scott Christen, & Lisa Gueldenzoph Snyder, "An Analysis of Effective Online Reputation Management: A Critical Thinking Social Media Activity," *Journal of Research In Business Education* 55 no. 1 (2013): 24-35. Notably, however, business models premised on more widespread use of portable ratings have yet to achieve durable success. See Rachel Pick, "Whatever Happened to Klout?" *Vice Motherboard* (Feb. 19, 2016), https://perma.cc/7DND-WH4M; Sarah Perez, "Controversial People-Rating App Peeple Goes Live, Has a Plan to Profit from Users' Negative Reviews," *TechCrunch* (Mar. 8, 2016), https://perma.cc/W3U4-QCQB.

[18] Allison Woodruff, "Necessary, Unpleasant, and Disempowering: Reputation Management in the Internet Age," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York: ACM, 2015), 149-158

[19] On SEO, see Eric Enge, Stephan Spencer, Jessie Stricchiola, & Rand Fishkin, *The Art of SEO*, 2d ed. (Sebastopol, CA: O'Reilly Media, 2012); Jayson DeMers, "The Top SEO Trends that Will Dominate 2015," *Forbes Online* (Dec. 8, 2014), https://perma.cc/9HZV-EX9B. On credit repair, see James P. Nehf, "A Legislative Framework for Reducing Fraud in the Credit Repair Industry," *North Carolina Law Review* 70 no. 3 (2003): 781-821; Harland Clarke & Javelin Strategy and Research, "Fee Income Growth Opportunities in the Identity Protection Market" (2011), https://perma.cc/8F98-A6VP.

[20] Rajat Paharia, *Loyalty 3.0: How Big Data and Gamification Are Revolutionizing Customer and Employee Engagement* (New York: McGraw Hill, 2013); Gabe Zichermann & Joselin Linder, *The Gamification*

Revolution: How Leaders Leverage Game Mechanics to Crush the Competition (New York: McGraw Hill, 2013).

[21] Ryan Singel, "Facebook Beacon Tracking Program Draws Privacy Lawsuit," *Wired* (Aug. 14, 2008), https://perma.cc/7NYS-UEWU.

[22] David Kirkpatrick, *The Facebook Effect: The Inside Story of the Company that Is Connecting the World* (New York: Simon & Schuster, 2010), 218-63; Zuboff, *The Age of Surveillance Capitalism*, 159-61, 457-58.

[23] Gary Wolf, "The Data-Driven Life," *New York Times* (Apr. 28, 2010), https://perma.cc/QD3U-E2W7; Emily Singer, "The Measured Life," *MIT Technology Review* (June 21, 2011), https://perma.cc/6QD5-8ZF9.

[24] See, for example, Jennifer Wang, "How Fitbit is Cashing in on the High-Tech Fitness Trend," *Entrepreneur* (July 28, 2012), https://perma.cc/96VW-ZDNT; see also David Pierce, "Goodbye, Wearables. You Had a Stupid Name Anyway," *Wired* (Dec. 23, 2015), https://perma.cc/3WSZ-9XNY.

[25] Alexander Galloway, *Gaming: Essays on Algorithmic Culture* (Minneapolis: University of Minnesota Press, 2006), 6-8, 91-104; see also Julie E. Cohen, "The Surveillance-Innovation Complex: The Irony of the Participatory Turn," in *The Participatory Condition in the Digital Age*, eds. Darin Barney et al. (Minneapolis: University of Minnesota Press, 2016), 207-226.

[26] On the depoliticized self as the intended product of neoliberal ideology, see Wendy Brown,"Neo-Liberalism and the End of Liberal Democracy," *Theory & Event* 7 no. 1 (2003): 15, https://perma.cc/SZ6K-2U6T; Todd May & Ladelle McWhorter,"Who's Being Disciplined Now? Operations of Power in a Neoliberal World," in *Biopower: Foucault and Beyond*, eds. Vernon W. Cisney & Nicolae Morar (Chicago: University of Chicago Press, 2016), 245-258.

[27] Felix Raczkowski, "It's All Fun and Games…: A History of Ideas Concerning Gamification," in *Proceedings of DiGRA 2013: DeFragging Game Studies*, 344-354 (Atlanta, Georgia: Digital Games Research Association 2013).

[28] Jennifer Whitson, "Gaming the Quantified Self," *Surveillance & Society* 11(1-2) (2013): 163, 169.

[29] Greg Sterling, "Foursquare to Move Check-ins Into 'Swarm' App, to Focus Better on Local Discovery," *Search Engine Land* (May 1, 2014), https://perma.cc/F5HE-PAG4.

[30] On addictive design and its connections to gaming and gambling, see Adam Alter, *Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked* (University Park, Pa.: Penn State University Press, 2017); Natasha Dow Schull, *Addiction by Design: Machine Gambling in Las Vegas* (Princeton: Princeton University Press, 2012).

[31] D.G. Brian Jones & Eric H. Shaw, "A History of Marketing Thought," in *Handbook of Marketing*, eds. Barton A. Weitz & Robin Wensley (Thousand Oaks, Calif.: SAGE Publishing, 2002), 39-65; Robert Bartels, "The Identity Crisis in Marketing," *Journal of Marketing* 38 no. 4 (1974): 73-76.

[32] Zuboff, *The Age of Surveillance Capitalism*, 204-12, 293-97, 361-75, 416-440.

[33] See, for example, Syed Tariq Anwar, "Company Slogans, Morphological Issues, and Corporate Communications," *Corporate Communications: An International Journal* 20 no. 3 (2015): 360-74; S. Adam Brasel & James Gips, "Breaking Through Fast-Forwarding: Brand Information and Visual Attention," *Journal of Marketing* 72 no. 6 (2008): 31-48; Maxime Carron, Francoise Dubois, Nicolas Misdariis, Corinne Talotte, & Patrick Susini, "Designing Sound Identity: Providing New Communication Tools for Building Brands 'Corporate Sound,'" in *Proceedings of the 9th Audio Mostly: A Conference on Interaction With Sound* (New York: ACM, 2014), 15-22, https://perma.cc/3CTM-YGS7; Brigitte Muller, Brigitte, Bruno Kocher, & Antoine Crettaz, "The Effects of Visual Rejuvenation Through Brand Logos," *Journal of Business Research* 66 (2011): 82-88.

[34] Rosemary J. Coombe, *The Cultural Lives of Intellectual Properties: Authorship, Appropriation, and the Law*. (Durham: Duke University Press, 1998).

[35] David Murakami Wood & Kirstie Ball,"Brandscapes of Control? Surveillance, Marketing, and the Co-construction of Subjectivity and Space in Neoliberal Capitalism," *Marketing Theory* 13 no. 1 (2013): 47, 57.

[36] Joseph Turow, *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power* (New Haven, Conn.: Yale University Press, 2017).

[37] See, for example, Jeff Huang et al., "No Clicks, No Problem: Using Cursor Movements to Understand and Improve Search," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*

(New York: ACM, 2011) , 1225-1234; Michal Kosinski, David Stillwell, & Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior," *PNAS* 110 no. 15 (2013): 5802-5805; Wu Youyou, Michal Kosinski, & David Stillwell, "Computer-Based Personality Judgments Are More Accurate than Those Made by Humans," *PNAS* 112 no. 4 (2015): 1036-1040; Hilke Plassmann, Vinod Venkatraman, Scott Huettel, & Carolyn Yoon, "Consumer Neuroscience: Applications, Challenges, and Possible Solutions," *Journal of Marketing Research* 52 no. 4 (2015): 427-435; Vinod Venkatraman, John A. Clithero, Gavan J. Fitzsimons, & Scott A. Huettel, "New Scanner Data for Brand Marketers: How Neuroscience Can Help Better Understand Differences in Brand Preferences," *Journal of Consumer Psychology* 22 no. 1 (2012): 143-153.

[38] See, for example, Natasha Lomas, "Amazon Patents 'Anticipatory' Shipping—To Start Sending Stuff Before You've Bought It," *TechCrunch* (Jan. 18, 2014), https://perma.cc/8SK8-R2WS; Steve Rosenbush, "Facebook Tests Software to Track Your Cursor on Screen," *Wall Street Journal* (Oct. 30, 2013), https://perma.cc/X3XL-FEYK.

[39] Robinson Meyer, "Everything We Know About Facebook's Secret Mood Manipulation Experiment," *The Atlantic* (June 28, 2014), https://perma.cc/YF8Q-LHEK; Paul Armstrong, "Facebook Is Helping Brands Target Teens Who Feel 'Worthless," *Forbes* (May 1, 2017), https://perma.cc/F62G-SNF7; see also "Comments on Research and Ad Targeting," *Newsroom*, Facebook (Apr. 30, 2017) ("Facebook does not offer tools to target people based on their emotional state. . . . Facebook has an established process to review the research we perform. This research did not follow that process, and we are reviewing the details to correct the oversight."), https://perma.cc/WG3D-JQX2. For a general survey of commercial mood-detection techniques in use or under development, see Tasha Glenn & Scott Monteith, "New Measures of Mental State and Behavior Based on Data Collected from Sensors, Smartphones, and the Internet," Current Psychiatric Reports 16 no. 12 (2014): 523-532, doi: 10.1007/s11920-014-0523-3. For an in-depth exploration of the feasibility and difficulties of sentiment mining, see Bo Pang & Lillian Lee, "Opinion Mining and Sentiment Analysis," *Foundations and Trends in Information Retrieval* 2 nos. 1-2 (2008): 1-135.

[40] Franklin Foer, *World Without Mind* (New York: Penguin, 2018), 139.

[41] On the psychology of clickbait, see Bryan Gardiner, "You'll Be Outraged at How Easy It Was to Get You to Click on This Headline," *Wired* (Dec. 18, 2015), https://perma.cc/4QXK-5M56. On the background behavioral psychology research, see George Loewenstein, "The Psychology of Curiosity: A Review and Reinterpretation," *Psychological Bulletin* 116(1) (1994): 75-98. On motivations for sharing, see Alice Marwick, "Why Do People Share Fake News? A Sociotechnical Model of Media Effects," *Georgetown Law Technology Review* 2 no. 2 (2018): 474-512, https://perma.cc/DT4C-94EU.

[42] Foer, *World Without Mind*, 144-46.

[43] See, for example, Olivia Solon & Sam Levin, "How Google's Search Algorithm Spreads False Information with a Rightwing Bias," *The Guardian* (Dec. 16, 2016), https://perma.cc/Z8QZ-PUY7; Carole Cadwalladr, "Google, Democracy and the Truth About Internet Search," *The Guardian* (Dec. 4, 2016), https://perma.cc/A6UA-JKGA; Noam Cohen, "Google's Search Algorithm Isn't Biased; It's Just Not Human, *Wired* (Dec. 14, 2018), https://perma.cc/L35Q-Q3S3; see generally Lucas D. Introna & Helen Nissenbaum, "Shaping the Web: Why the Politics of Search Engines Matter," *The Information Society* 16 no. 3 (2000): 169-185.

[44] For prescient work exploring the interconnections between subjectivity and scale, see Luke Stark, "Algorithmic Psychometrics and the Scalable Subject," *Social Studies of Science* 48, no. 2 (2018): 204-231; see also Nick Couldry & Andreas Hepp, *The Mediated Construction of Reality* (Malden, Mass.: Polity, 2017), 187.

[45] Eric S. Raymond, *The Cathedral and the Bazaar* (Sebastopol, CA: O'Reilly Media, 1999), 30; see Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven: Yale University Press, 2006), 59-90; Axel Bruns, *Blogs, Wikipedia, Second Life, and Beyond: From Production to Produsage* (New York: Peter Lang, 2008), 101-136; Karen Hellekson & Kristina Busse, eds., *Fan Fiction and Fan Communities in the Age of the Internet*, eds. (Jefferson, NC: McFarland Books, 2006); Aaron Delwiche & Jennifer Jacobs Henderson, eds., *The Participatory Cultures Handbook* (New York: Routledge, 2012).

[46] James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations* (New York: Anchor, 2004); see

also Clay Shirky, *Here Comes Everybody: The Power of Organizing without Organization* (New York: Penguin, 2008); Amy N. Langville & Carl D. Meyer, *Google's PageRank and Beyond: The Science of Search Engine Ratings* (Princeton: Princeton University Press, 2012), 25-30; David Easley & Jon Kleinberg, *Networks, Crowds, and Markets: Reasoning About a Highly Connected World* (New York: Cambridge University Press, 2010), 258-362.

[47] See Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, (New York: Basic Books, 2012); Zeynep Tufecki, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven, Conn.: Yale University Press, 2017); Deen Freelon et al., "Beyond the Hashtags: #Ferguson, #BlackLivesMatter, and the Online Struggle for Offline Justice," Center for Media & Social Impact (2016), https://perma.cc/UWR4-6SUN.

[48] See Timur Kuran & Cass R. Sunstein, "Availability Cascades and Risk Regulation," *Stanford Law Review* 51 no. 4 (1999): 683-768; April Mara Barton, "Application of Cascade Theory to Online Systems: A Study of Email and Google Cascades," *Minnesota Journal of Law, Science, and Technology* 10 no. 2 (2009): 473-502.

[49] Matthew Gentzkow, "Polarization in 2016," Toulouse Network of Information Technology White Paper (2016), https://perma.cc/5AVV-PPFP.

[50] On homogeneity and polarization, see Cass Sunstein, *Going to Extremes: How Like Minds Unite and Divide* (New York: Oxford University Press, 2009). On algorithmically reinforced polarization in the networked digital information environment, see Andrejevic, *Infoglut*, 42-61; Marwick, "Why Do People Share Fake News?"; Walter Quattrociocchi, Antonio Scala, & Cass R. Sunstein, "Echo Chambers on Facebook," John M. Olin Center for Law & Economics, Harvard Law School, Discussion Paper No. 877 (2016). The term "filter bubble" has entered the popular lexicon as a way of conveying these effects, but to the extent it suggests that people are completely insulated from encounters with opposing narratives and views, it may also be misleading.

[51] Yochai Benkler, Robert Faris, & Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (New York: Oxford University Press, 2018); Russell Muirhead & Nancy Rosenblum, "The New Conspiracists," *Dissent* (Winter 2018), https://perma.cc/4CAX-BLQ6.

[52] Andrejevic, *Infoglut*, 12; see, for example, Alfred Hermida, et al., "Share, Like, Recommend: Decoding the Social Media News Consumer," *Journalism Studies* 13 no. 5-6: 815-824; Jason Turcotte, et al., "News Recommendations from Social Media Opinion Leaders: Effects on Media Trust and Information Seeking," *Journal of Computer-Mediated Communication* 20 no. 5 (2015): 520-535.

[53] Andrejevic, *Infoglut*, 15-18; see, for example, Jonathan Albright, "Untrue-Tube: Monetizing Misery and Disinformation," *Medium* (Feb. 25, 2018), https://perma.cc/Y6BM-CQCD; Bill Scher, "Why the NRA Always Wins," *Politico* (Feb. 19, 2018), https://perma.cc/SC7Y-UA7U; Julia Carrie Wong, "How Facebook and YouTube Help Spread Anti-Vaxxer Propaganda," *The Guardian* (Feb. 1, 2019), https://perma.cc/68GE-8TJL.

[54] On the "pizzagate" story, see David A. Graham, "The 'Comet Pizza' Gunman Provides a Glimpse of a Frightening Future," *The Atlantic* (Dec. 5, 2016), https://perma.cc/J9L8-DEZL. On the various origins of efforts to spread misinformation and disinformation online, see, for example, Samanth Subramanian, "Inside the Macedonian Fake-News Complex," *Wired* (Feb. 15, 2017), https://perma.cc/528F-F48Q; "Tall Tales Spread by Alex Jones Breed Dangerous Plots," Southern Poverty Law Center: Intelligence Report (Feb, 15, 2017), https://perma.cc/28A8-ZFWR; Olivia Solon & Sabrina Siddiqui, "Russia-Backed Facebook Posts 'Reached 126m Americans' During U.S. Election," *Guardian* (Oct. 31, 2017), https://perma.cc/6REY-NMDX; Carole Cadwalladr & Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *Guardian* (Mar. 17, 2018), https://perma.cc/92UL-VMU8.

[55] Katherine Viner, "How Technology Disrupted the Truth," *Guardian* (Jul. 12, 2016), https://perma.cc/K6AU-YZYR; Carole Cadwalladr, "The Great British Brexit Robbery: How Our Democracy was Hijacked," *Guardian* (May 7, 2017), https://perma.cc/UZ6R-BBQU; Christopher Paul & Miriam Matthew, "The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It," RAND Corporation: Perspectives (2016), https://perma.cc/CLB5-A5AG.

[56] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Cambridge, Mass.: Harvard University Press, 2014); Whitney Phillips, *This Is Why We Can't Have Nice Things* (Cambridge, Mass.: MIT Press, 2015).

[57] Rebecca Lewis, "Alternative Influence: Broadcasting the Reactionary Right on YouTube," Data & Society (Sept. 18, 2018), https://perma.cc/63H4-QJAL; Alice Marwick & Rebecca Lewis, "Media Manipulation & Disinformation Online," Data & Society (2017), https://perma.cc/356L-XZQA; Kenneth Roth, "World Report 2017: The Dangerous Rise of Populism," Human Rights Watch (2017), https://perma.cc/Q7AC-VKYS; "The Online Hate Index," Anti-Defamation League (last visited Apr. 11, 2019, https:/perma.cc/SZ8A-B2CU; Julia Angwin, Madeleine Varner, & Ariana Tobin, "Facebook Enabled Advertisers to Reach 'Jew Haters," *ProPublica* (Sept. 14, 2017), https://perma.cc/9UD8-L9KG; see also Snigdha Poonam & Samarth Bansal, "Misinformation Is Endangering India's Election," *The Atlantic* (Apr. 1, 2019), https://perma.cc/V5WQ-2SHJ; Amanda Taub & Max Fisher, "When Countries Are Tinderboxes and Facebook Is a Match," *New York Times* (Apr. 21, 2018), https://perma.cc/LBC4-WGZQ.

[58] "Europe's Rising Far Right: A Guide to the Most Prominent Parties," *New York Times* (Dec. 4, 2016), https://perma.cc/7XYU-RHKP; Sasha Polakow-Suransky, "The Ruthlessly Effective Rebranding of Europe's New Far Right," *The Guardian* (Nov. 1, 2016), https://perma.cc/5GNT-CYLM; Ben Schreckinger, "The Alt-Right Comes to Washington," *Politico* (Jan./Feb. 2017), https://perma.cc/2BEJ-6UB3; Jason Wilson, "Hiding in Plain Sight: How the Alt-Right Is Weaponizing Irony to Spread Fascism," *Guardian* (May 23, 2017), https://perma.cc/T7UK-S8E9; George Hawley, "The Alt-Right Is Not Who You Think They Are," *American Conservative* (Aug. 25, 2017), https://perma.cc/LG6M-PB5Q. For more in-depth explorations of the alt-right's cultural origins, see Angela Nagle, *Kill All Normies: The Online Culture Wars from Tumblr and 4chan to the Alt-Right and Trump* (Washington, DC: Zero Press, 2017); Phillips, *This Is Why We Can't Have Nice Things*, 95-136. On extremist techniques for hijacking mainstream media coverage, see Whitney Phillips, "The Oxygen of Amplification: Better Practices for Reporting on Extremists, Antagonists, and Manipulators," Data & Society (May 22, 2018), https://perma.cc/ S8HZ-BKEM.

[59] Frederick Mark Gedicks,"Incorporation of the Establishment Clause Against the States: A Logical, Textual, and Historical Account," *Indiana Law Journal* 88 no. 2 (2013): 669-722, 693-96; John Harrison, "Power, Duty, and Facial Invalidity," *University of Pennsylvania Journal of Constitutional Law* 16 no. 2 (2013): 501-547, 509-512; Henry M. Hart, Jr. & Albert M. Sacks, *The Legal Process: Basic Problems in the Application of Law*, eds. William N. Eskridge, Jr. & Philip P. Frickey (St. Paul, Minn: West Academic, 1994), 135.

[60] Daniel Castro, Director, Center for Data Innovation, Letter to Nicole Wong, White House Office of Science and Technology Policy (Mar. 31, 2014), https://perma.cc/Y3T5-EJ3D.

[61] Michael Zaneis, Senior Vice President and General Counsel, Interactive Advertising Bureau, Testimony before the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, Hearing on Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale? (Mar. 29, 2012), https://perma.cc/HS68-THGG; see also, for example, Bob Liodice, President and CEO, Association of National Advertisers, Inc. on Behalf of the Digital Advertising Alliance, Testimony before the Senate Committee on Commerce, Science, and Transportation, Hearing on the Need for Privacy Protections: Is Industry Self-Regulation Adequate? (June 28, 2012), https://perma.cc/T5VY-ZWQ4; Randall Rothenberg, President and CEO, Interactive Advertising Bureau, Testimony before Subcommittee on Information Technology of the House Oversight and Government Reform Committee, Hearing on Oversight of Federal Political Advertisement Laws and Regulations (Oct. 24, 2017), https://perma.cc/4CDA-LP4H.

[62] See, for example, Berin Szoka & Adam Thierer, "Targeted Online Advertising: What's the Harm and Where Are We Heading?," *Progress on Point* 16 no. 2 (Feb. 26, 2009), http://perma.cc/CRU4-GZYE; Larry Downes, "A Rational Response to the Privacy 'Crisis," *Cato Institute Policy Analysis,* No. 716 (Jan. 7, 2013), https://perma.cc/U4B8-BZHP; Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules" (Oct. 21, 2017), Information Technology & Innovation Foundation, https://perma.cc/V3Q6-YSTS; Alan McQuinn & Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use," Information Technology and Innovation Foundation (July 2018), https://perma.cc/KC6E-H7Q4.

[63] See, for example, Mark MacCarthy, "In Defense of Big Data Analytics," in *The Cambridge Handbook of Consumer Privacy*, eds. Evan Selinger, Jules Polonetsky, & Omer Tene (New York: Cambridge University Press, 2018), 47-78; Omer Tene & Jules Polonetsky,"Privacy in the Age of Big Data: A Time for Big Decisions," *Stanford Law Review Online*, 64 (2012): 63-69. .

[64] Jacob Goldenberg, Donald R. Lehmann, & David Mazursky, "The Idea Itself and the Circumstances of Its Emergence as Predictors of New Product Success," *Management Science* 47 no. 1 (2001): 69-84.
[65] See, for example, U.S. Department of Commerce, Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" (Dec. 16, 2010), https://perma.cc/9QXL-Q53S; U.S. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012, https://perma.cc/PW3F-T5WB; White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (2012), https://perma.cc/XM53-RAKH; Subcommittee on Online Investigations of the Senate Committee on Homeland Security and Governmental Affairs, Hearing on Online Advertising and Hidden Hazards to Consumer Security and Data Privacy (May 15, 2014) (remarks of Senator John McCain), https://perma.cc/55DC-XWYN; see also FTC Staff Report, "Internet of Things: Privacy and Security in a Connected World" (Jan. 2015), 19-25, 47-48 (summarizing comments by workshop participants emphasizing the need for balance and for self-regulation), https://perma.cc/MR3R-2ZCM.
[66] See, for example, Cameron F. Kerry, General Counsel, U.S. Department of Commerce, "Remarks to the European Parliament," Interparliamentary Committee Meeting on The Reform of the EU Data Protection Framework: Building Trust in a Digital and Global World (Oct. 10, 2012), https://perma.cc/P2NV-LQMF; William E. Kennard, U.S. Ambassador to the European Union, "Remarks at Forum Europe's Third Annual European Data Protection and Privacy Conference" (Dec. 4, 2012), https://perma.cc/C7C8-PX4V; Natasha Singer, "Data Protection Laws, an Ocean Apart, *New York Times* (Feb. 2, 2013), https://perma.cc/AC7K-T3SQ; Anthony Gardner, U.S. Ambassador to the European Union, "Facing Legal Challenges in U.S.–EU Relations," Mackenzie Stuart Lecture at Cambridge University (Jan. 29, 2015), https://perma.cc/7PRK-C4EL.
[67] On the incentivizing effects of climate change policy, see American Energy Innovation Council, "Catalyzing American Ingenuity: The Role of Government in Energy Innovation" (2012), https://perma.cc/JNQ5-D9BD; Dennis Hirsch,"The Glass House Effect: Big Data, the New Oil, and the Power of Analogy," *Maine Law Review*, 66 no. 2 (2014): 373-395.
[68] On security threats flowing from data harvesting ecologies, see Paul Ohm,"Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* 57 no. 6 (2010): 1701, 1748; Danielle Keats Citron,"Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age," *Southern California Law Review* 80 no. 2 (2007): 241-297.
[69] For discussion of finance as innovation, see Chapter 1, pp. 26-29.
[70] Vincent Mosco, *The Digital Sublime* (Cambridge, Mass: MIT Press, 2004); David Nye, *American Technological Sublime* (Cambridge, Mass.: MIT Press, 1994). On the singularity, see Richard Dooling, *Rapture for the Geeks: When AI Outsmarts IQ* (New York: Crown, 2008); Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York: Viking, 2006); Brandon Keim, "Will the Singularity Make Us Happier?," *Wired* (May 30, 2008), http://perma.cc/BE53-ZZ88.
[71] Christian Schubert, "How to Evaluate Creative Destruction: Reconstructing Schumpeter's Approach," *Cambridge Journal of Economics* 37 no. 2 (2013): 227-250; John A. Dove & Russell S. Sobel, "Entrepreneurial Creative Destruction and Legal Federalism," in *The Law and Economics of Federalism*, ed. Jonathan Klick (Northampton, Mass.: Edward Elgar, 2017), 214-237.
[72] Manish Singh, "India's Database with Biometric Details of its Billion Citizens Ignites Privacy Debate," *Mashable* (Feb. 13, 2017), https://perma.cc/4W4F-WQ78; Usha Ramanathan, "Opinion: Data is the New Gold and Aadhaar is the Tool to Get it," *Scroll.in* (Dec. 30, 2016), https://perma.cc/BMK3-48UU; N.S. Ramnath, "Aadhaar: A Quiet Disruption," *Founding Fuel* (June 25, 2016), https://perma.cc/2QY8-F6VL; K.C. Deepika, "JAM and India Stack Will Push Innovation: Nandan Nilekani," *The Hindu* (Mar. 25, 2016), https://perma.cc/JE7B-XS7N; M. Rajshekhar & Anumeha Yadav, "How the Government Gains When Private Companies Use Aadhaar," *Scroll.in* (Mar. 24, 2016), https://perma.cc/LHP4-K7S9.
[73] For discussions of this issue from differing perspectives, see Tal Z. Zarsky,"The Privacy/Innovation Conundrum," *Lewis and Clark Law Review* 19 no. 1 (2015): 115-168; Helena Ursic & Bart Custers, "Legal Barriers and Enablers to Big Data Reuse: A Critical Assessment of the Challenges for the EU Law," *European Data Protection Review* 2 no. 2 (2016): 209-221.
[74] Kirstie Ball & Laureen Snider, eds., *The Surveillance-Industrial Complex: A Political Economy of Surveillance* (New York: Routledge, 2013); Ben Hayes, "The Surveillance-Industrial Complex," in

Routledge Handbook of Surveillance Studies, eds. Kirstie Ball, Keven D. Haggerty & David Lyon (New York: Routledge, 2012), 167-175.

[75] Adam Winkler, *We the Corporations: How American Businesses Won Their Civil Rights* (New York: W.W. Norton, 2018).

[76] For discussion of the origins of the neoliberal First Amendment as an advocacy movement, see Amanda Shanor, "The New *Lochner*," *Wisconsin Law Review* 2016 no. 1 (2016): 133, 138-63. For policy papers addressing the specific issue of information privacy regulation, see Solveig Singleton, "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector, *Cato Institute Policy Analysis*, No. 295 (Jan. 22, 1998), at https://perma.cc/B34M-NFS2; and Adam Thierer & Berin Szoka, "What Unites Advocates of Speech Controls & Privacy Regulation?," *Progress on Point* 16 no. 19 (Nov. 2009), https://perma.cc/C9UX-HDF5. An influential article advancing the First Amendment challenge to information privacy regulation was Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Keep People from Speaking about You," *Stanford Law Review* 52 no. 5 (2002): 1049-1124. For a more recent analysis extending the argument to data-driven algorithmic processes, see Jane R. Bambauer, "Is Data Speech?" *Stanford Law Review* 66 no. 1 (2014): 57-120.

[77] See Central Hudson Gas & Electric Corp. v. Public Service Commission, 447 U.S. 557, 561-66 (1980). For a useful overview of the doctrine and of scholarly perspectives on its coherence, see Felix T. Wu, "The Commercial Difference," *William & Mary Law Review* 58 no. 6 (2017): 2005-61.

[78] 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). For a sampling of perspectives on the meaning of the marketplace metaphor and its significance for free speech jurisprudence more generally, see Vincent Blasi, "Holmes and the Marketplace of Ideas," *The Supreme Court Review* 2004: 1-46; Stanley Ingber, "The Marketplace of Ideas: A Legitimizing Myth," *Duke Law Journal* 1984 no. 1 (1984): 1-91; Robert C. Post, "Reconciling Theory and Doctrine in First Amendment Jurisprudence," *California Law Review* 88 no. 6 (2000): 2353-2374.

[79] Sorrell v. IMS Health, Inc., 564 U.S. 552, 563-70 (2011).

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

[81] For more detailed discussion of this issue, see Chapter 6, pp. 178-81.

[82] Jesselyn Cook, "From Nazis to Incels: How One Tech Company Helps Hate Groups Thrive," *Huffington Post* (July 25, 2018), https://perma.cc/W4Z3-CF8X; Mark Bergen, "YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant," *Bloomberg* (Apr. 2, 2019), https://gtownlaw.li/2I8KoZK.

[83] For an especially rich articulation, which originated as a white paper commissioned by Google, see Eugene Volokh & Donald Falk, "First Amendment Protection of Search Engine Search Results," *Journal of Law, Economics and Policy* 8 no. 4 (2012); 883-899.

[84] Hal R. Varian, "Beyond Big Data," *Business Economics*, 49 no. 1 (2014): 27-31.

[85] On the emotional contagion experiment, see Adam D.I. Kramer, Jamie E. Guillory, & Jeffrey T. Hancock, "Experimental Evidence of Massive-scale Emotional Contagion through Social Networks," *Proceedings of the National Academy of Sciences* 111 no. 24 (2014): 8788-8790; see James Grimmelmann & Leslie Meltzer Henry, Letter to Inder M. Verma, Editor-in-Chief of *Proceedings of the National Academy of Sciences* (July 17, 2014), https://perma.cc/KG6F-XDMQ; Duncan J. Watts, "Stop Complaining about the Facebook Study. It's a Golden Age for Research," *The Guardian* (July 7, 2014), https://perma.cc/7UMH-NZGG. On the voter mobilization experiment, see Robert M. Bond, Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle & James H. Fowler, "A 61-Million-Person Experiment in Social Influence and Political Mobilization," *Nature* 489 (2012): 295-29; Robinson Meyer, "How Facebook Could Skew an Election," *The Atlantic* (Nov. 4, 2014), https://perma.cc/ZN6D-PQL5/.

[86] "About," Google AI (last visited Dec. 14, 2018), https://perma.cc/6XXX-UXZH; Mark Zuckerberg, "Building Global Community," Facebook (Feb. 16, 2017), https://perma.cc/LVJ7-LCRT; see also Mark Zuckerberg, "I Want to Share Some Thoughts on Facebook and the Election," Facebook (Nov. 12, 2016), https://perma.cc/7TKZ-PNHZ; "Transcript of Mark Zuckerberg's Senate Hearing," *Washington Post* (Apr. 10, 2018), https://perma.cc/2UQ5-CWYD; Gary Price, "Now Available: Keyword Searchable Video of Google CEO Sundar Pichai's Testimony Before U.S. House Judiciary Committee," *InfoDocket* (Dec. 11, 2018), https://perma.cc/462J-JAMG; Colin Crowell, "Our Approach to Bots and Misinformation," *Twitter Blog* (June 14, 2017), https://perma.cc/K5AN-UACB.

[87] Robert Cannon, "The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway," *Federal Communications Law Journal* 49 no. 1 (1996): 51-94.

[88] Communications Decency Act of 1996, Pub. L. 104-104, title V, §509, 110 Stat. 137, codified as amended at 47 U.S.C. § 230(a)(3); see, for example, Congressional Record, Feb. 1, 1996, H1175 (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."), https://perma.cc/QJ5Y-QLL2; see also "Senator Wyden's Speech to the Section 230 Anniversary Conference," Ron Wyden (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."), https://perma.cc/9QBP-V2WA.

[89] For a summary of the traditional rules and a comprehensive review of the case law through 2009, see David S. Ardia, "Free Speech Savior or Shield for Scoundrels? An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act," *Loyola of Los Angeles Law Review* 43 no.2 (2010): 373-506.

[90] Jane R. Bambauer & Derek E. Bambauer, "Vanished," *Virginia Journal of Law and Technology* 18 no. 1 (2013): 137-177.

[91] James Grimmelmann, "Speech Engines," *Minnesota Law Review* 98 no. 2 (2014); 868-952.

[92] Adi Kamdar, "EFF's Guide to CDA 230: The Most Important Law Protecting Online Speech" (Dec. 6, 2012), https://perma.cc/Z799-TY8P; see, for example, Anupam Chander, "How Law Made Silicon Valley," *Emory Law Journal* 63 no. 3 (2014): 639-94; Anupam Chander & Vivek Krishnamurthy, "The Myth of Platform Neutrality," *Georgetown Law Technology Review* 2 no. 2 (2018): 400-416, https://perma.cc/WLS6-CQ35; Cindy Cohn, "Bad Facts Make Bad Law: How Platform Censorship Has Failed So Far and How to Ensure that the Response to Neo-Nazis Doesn't Make It Worse," *Georgetown Law Technology Review* 2 no. 2 (2018): 432-51, https://perma.cc/9WDH-CMK5; Sarah Jeong, "Revenge Porn Is Bad. Criminalizing It Is Worse," *Wired* (Oct. 28, 2013), https://perma.cc/7AZP-P9VL; Daphne Keller, "Internet Platforms: Observations on Speech, Danger, and Money," Aegis Series Paper No. 1807, Hoover Institution (June 13, 2018), https://perma.cc/N43P-F89T. Two notable recent attempts to retheorize the problem of online speech regulation are Jack Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation," *U.C. Davis Law Review* 51 no. 3 (2017): 1149-1210; Kyle Langvardt, "A New Deal for the Online Public Sphere," *George Mason Law Review* 26 no. 2 (forthcoming 2019).

[93] David Carr, "The Evolving Mission of Google," *New York Times* (Mar. 21, 2011), https://perma.cc/8UPE-N3BF; Deepa Seetharaman, "Facebook Leaders Call It a Tech Company, Not a Media Company," *Wall Street Journal* (Oct. 25, 2016), https://perma.cc/DY2N-QWL8.

[94] Citizens United v. Federal Election Comm'n, 558 U.S. 310, 353 (2010). The beginnings of a more up-to-date appreciation of contemporary networked media appear in Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017).

[95] Elisa Shearer & Jeffrey Gottfried, Pew Research Center, "News Use Across Social Media Platforms" (Sept. 7, 2017), https://perma.cc/2ZHT-PBFA; Amy Mitchell, et al., Pew Research Center, "The Modern News Consumer" (July 7, 2016), 5-8, https://perma.cc/SJ5S-M93H; "Mobile Fact Sheet," Pew Research Center (Jan. 12, 2017), https://perma.cc/V84A-CAJD.

[96] Marwick, "Why Do People Share Fake News?"; Benkler, Faris, & Roberts, *Network Propaganda*, 225-233.

[97] Julie E. Cohen, "The Zombie First Amemdment," *William & Mary Law Review*, 56 no. 4 (2015): 1119-1158.

[98] Ellen P. Goodman, "Media Policy Out of the Box: Content Abundance, Attention Scarcity, and the Failures of Digital Markets," *Berkeley Technology Law Journal* 19 no. 4 (2004): 1389-1472; Tom Wheeler, "Trump FCC Deregulation Policy Threatens Local Broadcasting," Techtank, Brookings Institution (July

11, 2017), https://perma.cc/JP85-LXHB. On the growing concentration of media ownership, see Ben H. Bagdikian, The New Media Monopoly (Boston, Mass.: Beacon Press, 2004), 27-54.

[99] On moderation as the essential commodity that platforms provide, see Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media* (New Haven, Conn.: Yale University Press, 2018).

[100] Kent Walker, "A Principle that Should Not Be Forgotten," *Google Europe Blog* (May 19, 2016), https://perma.cc/TD5J-RGN6; Natasha Lomas, "Google Super Successful at Spinning Europe's Right to Be Forgotten Ruling as Farce," *TechCrunch* (July 4, 2014), https://perma.cc/6NYT-XXFG; see also Natasha Lomas, "Wikimedia Attacks Europe's Right to Be Forgotten Ruling as Threat to Its Mission," *TechCrunch* (Aug. 6, 2014), https://perma.cc/B83S-MECK.

[101] Google Spain SL v. Agencia Espanola de Proteccion de Datos (AEPD), Case No. C-131/12 (ECJ 13 May 2014), ¶¶ 81, 85-86; see also European Commission Directorate-General for Justice and Consumers, Article 29 Data Protection Working Party, "Guidelines on Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales, C-131/14" (Nov. 26, 2014), https://perma.cc/MJ54-WK55.

[102] Julia Powles & Enrique Chaparro, "How Google Determined Our Right to Be Forgotten," *The Guardian* (Feb. 18, 2015), https://perma.cc/A85M-Z43S.

[103] See, for example, California HealthCare Foundation, "How Smartphones Are Changing Health Care for Consumers and Providers" (Apr. 2010), https://perma.cc/CQM9-U6XX; Federal Reserve, "Consumers and Mobile Financial Services" (Mar. 2015), https://perma.cc/55FA-MAUD; "Reinventing Wheels," Special Reports, *Economist* (Mar. 1, 2018), https://perma.cc/D44S-79TY; "Unlocking the Promise of a Connected World: Using the Cloud to Enable the Internet of Things," Oracle White Paper (Sept. 2015), https://perma.cc/ANP6-UMYA; "12 Benefits of Cloud Computing," *Salesforce: Hub* (last visited Aug. 6, 2018), https://perma.cc/TH35-RXYB.

[104] See, for example, U.S. Bureau of Justice Statistics, Press Release, "17.6 Million U.S. Residents Experienced Identity Theft in 2014" (Sept. 27, 2015), https://perma.cc/A4VU-TRJN; Erika Harrell, "Victims of Identity Theft, 2014," U.S. Bureau of Justice Statistics Bulletin No. NCJ 248991 (Sept. 2015), https://perma.cc/7CXB-B6WT.

[105] Brief Amicus Curiae of Electronic Transactions Association on Behalf of Appellant Wyndham Hotels and Resorts, LLC, Federal Trade Commission v. Wyndham Worldwide Corp, No. 14-3514, U.S. Court of Appeals, Third Circuit, Oct. 14, 2014; Statement of David Wagner, President, Entrust, Inc., Hearing before the Senate Committee on Commerce, Science, and Transportation, "Protecting Personal Consumer Information from Cyber Attacks and Data Breaches" (Mar. 26, 2014), https://perma.cc/8SXS-8X73; Statement of Dan Liutikas, Chief Legal Officer, CompTIA, Hearing before the House Subcommittee on Commerce, Manufacturing, and Trade, "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?" (July 18, 2013), https://perma.cc/S45B-ZV8L.

[106] Statement of Rep. Fred Upton, House Subcommittee on Commerce, Manufacturing, and Trade, Markup of "Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015," Mar. 24, 2015, https://perma.cc/3WTM-4QFK; Exhibit A to Statement of Geoffrey Manne, "The FTC at 100: Views from the Academic Experts," Hearing before the House Subcommittee on Commerce, Manufacturing, and Trade (Feb. 28, 2014), https://perma.cc/79WP-XHAP; "California Bill Analysis, A.B. No. 710," Assembly Committee on the Judiciary (Apr. 29, 2014), https://perma.cc/XR9F-X98L.

[107] U.S. Chamber of Commerce, "Hill Letter Regarding the Data Security and Breach Notification Act" (Apr. 15, 2015) ("Given the complexity and expense of responding to a data breach, the Chamber cautions that the bill's flawed liability provisions would further penalize an entity that is itself a victim of data breach by drawing away valuable resources necessary to fix the breach [and] notify customers."), https://perma.cc/V452-55X8.

[108] California Bill Analysis, A.B. No. 1710, Assembly Committee on the Judiciary (Apr. 29, 2014) (summarizing arguments by opponents that protective data breach legislation "would result in over-notification that would ultimately confuse California consumers").

[109] Paul Schwartz & Edward Janger, "Notification of Data Security Breaches," *Michigan Law Review*, 105 no. 5 (2007): 913-984; Sasha Romanosky, Rahul Telang, & Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?," *Journal of Policy Analysis & Management* 30 no. 2 (2011): 256-286.

[110] Steptoe & Johnson, LLP, "Comparison of US State and Federal Security Breach Notification Laws" (Aug. 26, 2015), https://perma.cc/92J3-RMR3.
[111] Regulation (EU) 2016/679, Art. 33, 2016 O.J. (L 119).
[112] See FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (denying motion to dismiss on the ground that FTC lacked UDAAP enforcement authority over data security practices), *aff'd*, 799 F.3d 236 (3d Cir. 2015); LabMD v. FTC, 894 F.3d 1221 (11th Cir. 2018) (invalidating cease and desist order because it did not describe the data security practices prohibited as substandard so requirements for compliance were unclear).
[113] Adam J. Levitin, "Private Disordering? Payment Card Fraud Liability Rules," *Brooklyn Journal of Corporate, Financial & Commercial Law* 5 no. 1 (2010): 1-48; Adam J. Levitin, "Pandora's Digital Box: The Promise and Perils of Digital Wallets," *University of Pennsylvania Law Review* 166 no. 2 (2018): 305-376.
[114] Jon Hanson & David Yosifon, "The Situation: An Introduction to the Situational Character, Critical Realism, Power Economics, and Deep Capture," *University of Pennsylvania Law Review* 152 no. 1 (2003): 129, 212-30.
[115] Oscar H. Gandy, Jr., *Beyond Agenda Setting: Information Subsidies and Public Policy* (New York: Ablex, 1982).
[116] See, for example, Copia Institute, https://copia.is/; Information Technology and Innovation Foundation, https://itif.org/; Tech America, https://www.techamerica.org/; Tech Freedom, http://techfreedom.org/; see also Donald E. Abelson, "Think Tanks in the United States," in *Think Tanks Across Nations: A Comparative Approach*, eds. Diane Stone, et al. (Manchester, UK: Manchester University Press, 1998), 107-126; Thomas Medvetz, *Think Tanks in America* (Chicago: University of Chicago Press, 2012), 1–22, 47–129.
[117] For a sampling of reform proposals, see Danielle Keats Citron & Benjamin Wittes, "The Internet Will Not Break: Denying Bad Samaritans §230 Immunity," *Fordham Law Review* 86 no. 2 (2018): 401-424; Grimmelmann, "Speech Engines," 893-936; Frank Pasquale, "Reforming the Law of Reputation," *Loyola University Chicago Law Journal*, 47 no. 2 (2015): 515-40. For some responses, see Mike Masnick, "Law Professor Pens Ridiculous, Nearly Fact-Free, Misleading Attack On The Most Important Law On The Internet," *TechDirt* (Nov. 3, 2015), https://perma.cc/53W5-S9WS (attacking Ann Bartow and Danielle Citron); Mike Masnick, "Federal Revenge Porn Bill Will Look to Criminalize Websites," *TechDirt* (Apr. 2, 2014), https://perma.cc/KPU9-PXJ9 (attacking Mary Anne Franks); "Law Professor Claims Any Internet Company 'Research' on Users without Review Board Approval Is Illegal," *TechDirt* (Sept. 24, 2014), https://perma.cc/8W2E-TPCC (criticizing James Grimmelmann); Eric Goldman, "Congress Is About To Ruin Its Online Free Speech Masterpiece (Cross-Post)," *Technology & Marketing Law Blog* (Sept. 24, 2017), https://perma.cc/8EA7-VQ2Z; Sarah Jeong, "Revenge Porn Is Bad. Criminalizing It Is Worse," *Wired* (Oct. 28, 2013), https://perma.cc/7AZP-P9VL.
[118] See, for example, Declan McCullagh, "The Mother of Gore's Invention," *Wired* (Oct. 17, 2000), https://perma.cc/ZC76-8MFU; Donna Wentworth, "What's Stupider Than Calling the Internet an 'Information Superhighway'?," Electronic Frontier Foundation (July 5, 2005), https://perma.cc/4X5D-JET2; Nate Anderson, "Time Capsule: The Rough Guide to the Internet . . . from 1999," *Ars Technica* (Dec. 15, 2009), https://perma.cc/7MD9-TYRF.
[119] Tung-Hui Hu, *A Prehistory of the Cloud* (Cambridge, Mass.: MIT Press, 2015).
[120] On corporate public relations strategies as deep capture strategies, see generally Kirk Hallahan, "Political Public Relations and Strategic Framing," in *Political Public Relations: Principles and Applications*, eds. Jesper Stromback & Spiro Kiousis (New York: Routledge, 2011), 177-213; see also Robert L. Heath & Damian Waymer, "Corporate Issues Management and Political Public Relations," in *Political Public Relations*, 138-156.
[121] Brody Mullins & Jack Nicas, "Paying Professors: Inside Google's Academic Influence Campaign," *Wall Street Journal* (July 14, 2017), https://perma.cc/3QLE-75PG.
[122] "Announcing the Palantir Council on Privacy and Civil Liberties," Palantir, https://perma.cc/2KQH-AX5B (last visited June 16, 2018); Mark Harris, "How Peter Thiel's Secretive Data Company Pushed Into Policing," *Wired* (Aug. 9, 2017), https://perma.cc/R9X8-268W.
[123] Examples include South by Southwest (SXSW), https://www.sxsw.com/, the Consumer Electronics Show (CES), https://www.ces.tech/, and the Virtuous Circle Summit, https://vc.internetassociation.org/.

[124] Kenneth P. Vogel, "New America, a Google-Funded Think Tank, Faces Backlash for Firing a Google Critic," *New York Times* (Sept. 1, 2017), https://perma.cc/Y5VG-46XY; Kashmir Hill, "Yes, Google Uses Its Power to Quash Ideas It Doesn't Like—I Know Because It Happened to Me," *Gizmodo* (Aug. 31, 2017), https://perma.cc/VCK5-AU5X; Danny Vinik, "Inside the New Battle Against Google," *Politico* (Sept. 17, 2017), https://perma.cc/6L3U-XSVW.

[125] Joe Mullin, "Anti-Google Research Group in Washington is Funded by Oracle," *Ars Technica* (Aug. 19, 2016), https://perma.cc/8M2L-RMC4.