

# Buffalo Law Review

---

Volume 66 | Number 5

Article 1

---


12-1-2018

## The First Amendment in the Second Gilded Age

Jack M. Balkin

*The Information Society Project, Yale Law School*

Follow this and additional works at: <https://digitalcommons.law.buffalo.edu/buffalolawreview>

 Part of the [Constitutional Law Commons](#), [First Amendment Commons](#), and the [Privacy Law Commons](#)

---

### Recommended Citation

Jack M. Balkin, *The First Amendment in the Second Gilded Age*, 66 Buff. L. Rev. 979 (2018).

Available at: <https://digitalcommons.law.buffalo.edu/buffalolawreview/vol66/iss5/1>

This James McCormick Mitchell Lecture is brought to you for free and open access by the Law Journals at Digital Commons @ University at Buffalo School of Law. It has been accepted for inclusion in Buffalo Law Review by an authorized editor of Digital Commons @ University at Buffalo School of Law. For more information, please contact [lawscholar@buffalo.edu](mailto:lawscholar@buffalo.edu).

# Buffalo Law Review

---

VOLUME 66

DECEMBER 2018

NUMBER 5

---

**2018 James McCormick Mitchell Lecture**

## **The First Amendment in the Second Gilded Age**

JACK M. BALKIN†

INTRODUCTION<sup>1</sup>

We are now well into America's Second Gilded Age. The First Gilded Age was the era of industrial capitalism that began in the 1870s and 1880s and continued through the first years of the twentieth century, leading to the Progressive Era.<sup>2</sup> It produced huge fortunes, political corruption, and vast inequalities of wealth, so much so that people became concerned that they would endanger American democracy.

---

† Knight Professor of Constitutional Law and the First Amendment; Director, The Information Society Project, Yale Law School. This lecture is based on the 2018 James McCormick Mitchell Lecture that I gave at the University of Buffalo School of Law on April 13, 2018. My thanks to the faculty of the University of Buffalo for the invitation and for their gracious hospitality.

1. The introduction to this article was adapted and revised for a blog post on the Law and Political Economy Blog. Jack M. Balkin, *The Political Economy of Freedom of Speech in the Second Gilded Age*, L. & POL. ECON., (July 4, 2018), <https://lpeblog.org/2018/07/04/the-political-economy-of-freedom-of-speech-in-the-second-gilded-age/>.

2. On the First Gilded Age, see RICHARD WHITE, *THE REPUBLIC FOR WHICH IT STANDS: THE UNITED STATES DURING RECONSTRUCTION AND THE GILDED AGE, 1865–1896* (2017).

The Second Gilded Age begins, more or less, with the beginning of the digital revolution in the 1980s, but it really takes off in the early years of the commercial Internet in the 1990s, and it continues to the present day. It is characterized by the rise of social media and the development and implementation of algorithms, artificial intelligence, and robotics. For this reason I call our present era the Algorithmic Society.

If the First Gilded Age is the age of industrial capitalism, the Second Gilded Age is the age of digital or informational capitalism. It too has produced great fortunes and led to concerns that increasing concentrations of wealth and economic inequality are endangering American democracy. Like the First Gilded Age, it is also a time of deep political corruption and despair about the future of American democracy. It has not yet given way to a second Progressive Era, but every day I see signs that this is where we are headed.

There is a large literature criticizing the judicial doctrines of the First Amendment and how they are slanted toward the interests of corporations (and capital generally) in the Second Gilded Age.<sup>3</sup> The most obvious examples are the federal courts' recent decisions on commercial speech and campaign finance regulation.<sup>4</sup> These are interesting

---

3. See, e.g., Charlotte Garden, *The Deregulatory First Amendment at Work*, 51 HARV. CIV. RTS.-CIV. LIBERTIES L. REV. 323 (2016); Jeremy K. Kessler & David E. Pozen, *The Search for an Egalitarian First Amendment*, 118 COLUM. L. REV. 1953 (2018); Jedediah Purdy, *Beyond the Bosses' Constitution: Toward a Social-Democratic First Amendment*, 118 COLUM. L. REV. 2161 (2018); Amanda Shanor, *The New Lochner*, 2016 WIS. L. REV. 133 (2016); Tim Wu, *The Right to Evade Regulation: How Corporations Hijacked the First Amendment*, NEW REPUBLIC (June 3, 2013), <http://newrepublic.com/article/113294/how-corporations-hijacked-first-amendment-evade-regulation>.

4. See, e.g., *Janus v. Am. Fed'n of State, Cty. & Mun. Emps., Council 31*, 138 S. Ct. 2448, 2478 (2018) (holding that requiring nonmembers of public sector unions to pay fees toward collective bargaining violates the First Amendment); *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2378 (2018) (striking down California law requiring pro-life pregnancy centers to provide certain factual information to patients); *Harris v. Quinn*, 134 S. Ct.

and important topics, but they are not the subject of today's lecture.

Instead, I want to focus on what we might call the political economy of free speech in the digital age. The basic question is this: How does our political and economic system pay for a digital public sphere? The answer is that it pays for it largely through digital surveillance and through finding new ways to make money out of personal data. Digital capitalism in the Second Gilded Age features an implicit bargain: a seemingly unlimited freedom to speak in exchange for the right to surveil and manipulate end-users. In this lecture I discuss the economic and political forces that shaped this bargain and their costs. I will use the recent scandal over Facebook's privacy policies as an example of the problem.

The First Amendment plays a role in this story, but not the role that you might expect. One of the interesting features of the digital age is that the protection of freedom of expression has begun to detach from the judicial doctrines of the First Amendment, so that, as interpreted by courts, the First Amendment is increasingly irrelevant to the protection of freedom of speech online.<sup>5</sup>

---

2618, 2644 (2014) (striking down agency-fee provision of Illinois's Public Labor Relations Act); *McCutcheon v. FEC*, 572 U.S. 185, 227 (2014) (striking down aggregate limits on federal campaign contributions); *Ariz. Free Enter. Club's Freedom Club PAC v. Bennett*, 564 U.S. 721, 754, 755 (2011) (striking down Arizona law providing "matching funds" to publicly funded state candidates when privately funded opponents spend over a certain amount); *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 580 (2011) (striking down a Vermont law restricting the sale and disclosure of physicians' prescription records); *Citizens United v. FEC*, 558 U.S. 310, 372 (2010) (striking down statutory limits on corporate electioneering).

5. Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1152 (2018) [hereinafter Balkin, *Free Speech in the Algorithmic Society*]; Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 432–33, 443–44 (2009). See generally Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 19–22, 46–51 (2004) [hereinafter Balkin, *Digital Speech and Democratic Culture*].

Why is that? Well, much of our practical ability to speak online depends on an infrastructure of digital communication—broadband companies, domain name registrars and registries, webhosting services, caching and security services, search engines, and social media companies. That infrastructure is owned and operated by private parties, not by the state. Thus, in most cases, the businesses that provide the digital infrastructure of free expression are not state actors bound by the First Amendment. If we want to protect people’s privacy and freedom of speech from overreaching by digital media companies, the First Amendment will not be our primary line of defense. Nor will the Fourth Amendment, or the rest of the Bill of Rights, for that matter.

The First Amendment is relevant, but in a different way. It may be a potential obstacle to laws that try to regulate private infrastructure owners in order to protect end-users’ freedom of speech and privacy. One example would be the argument, rejected by the D.C. Circuit, but promoted by various corporations, that network neutrality regulations violate the free speech rights of broadband companies.<sup>6</sup>

A second example would be an argument by social media companies that restricting how they use, distribute, or sell the consumer data that they collect in the course of their operations violates the First Amendment, because the data is speech or knowledge, and it is unconstitutional to

---

6. See Stuart Minor Benjamin, *Transmitting, Editing, and Communicating: Determining What “The Freedom of Speech” Encompasses*, 60 DUKE L.J. 1673, 1696–712 (2011) (considering First Amendment challenges to network neutrality and concluding that network neutrality rules and common carriage obligations in telecommunications law do not violate the First Amendment); Susan Crawford, *First Amendment Common Sense*, 127 HARV. L. REV. 2343 (2014) (same). Compare *United States Telecom Ass’n v. FCC*, 825 F.3d 674, 740–44 (D.C. Cir. 2016) (rejecting First Amendment challenge to network neutrality rules), *reh’g denied*, 855 F.3d 381 (D.C. Cir. 2017), *with id.* at 426–35 (Kavanaugh, J., dissenting) (arguing that FCC order violates the First Amendment).

restrict its use, sale, or distribution.<sup>7</sup> The United States has not yet passed comprehensive digital privacy regulation, but when it attempts to, I expect that companies will make precisely this kind of argument against passage; and they will probably use the First Amendment to challenge any such legislation in the federal courts.

In short, the First Amendment, as currently interpreted by federal courts, may be of little help in securing the practical ability to speak through the privately-owned digital infrastructure of communication; in some cases the judicially created doctrines of the First Amendment may even be a positive hindrance.

That is why it is very important to distinguish the political value of freedom of speech from the judicially created doctrines of the First Amendment. To make the principles of the First Amendment live in our current age, we must look beyond the latest pronouncements of the federal courts. We must look at the political economy of digital speech. We must ask what dangers that political economy has created for end-users, and what kinds of reforms would best protect their interests. I've discussed a number of such reforms elsewhere;<sup>8</sup> here I will focus on the duties of good faith and non-manipulation that infrastructure owners should have toward the people who use their facilities to communicate.

The recent scandal over Facebook and Cambridge Analytica is a perfect example of these problems; you might

---

7. See *IMS Health Inc.*, 564 U.S. at 564–66 (applying “heightened judicial scrutiny” to Vermont’s law regulating prescription data because it made content- and speaker-based distinctions); *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1232–33 (10th Cir. 1999) (determining that restrictions on the sale of consumer data about telephone customers was a restriction on commercial speech because it interfered with telephone company’s ability to target customers for advertising purposes); Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 84–86 (2014) (explaining why the right to collect and create information suggests a broad right to record).

8. Jack M. Balkin, *Free Speech is a Triangle*, 118 COLUM. L. REV. 2011 (2018).

say that it is a characteristic scandal of the Second Gilded Age. That is because it revolves around how digital infrastructure companies make their money and how they affect the public sphere in the process. The scandal also reveals a basic problem of freedom of speech in the Second Gilded Age: Digital privacy undergirds our freedom of expression,<sup>9</sup> but the way we pay for freedom of expression perpetually threatens our digital privacy. This is the irony of the digital era: An era that promised unbounded opportunities for freedom of expression is also an era of increasing digital control and surveillance. The same technological advances allow both results.

I'll use the Facebook/Cambridge Analytica scandal to explain how the conditions that make free speech possible have changed from the twentieth to the twenty-first centuries. I will also use it to introduce one of the key concepts I've advocated for in previous work—the idea that digital media companies are *information fiduciaries* who have duties of care and loyalty toward their end-users.<sup>10</sup>

#### THE DIFFERENCE BETWEEN TWENTIETH-CENTURY AND TWENTY-FIRST-CENTURY MEDIA

What are the characteristic differences between twentieth-century media and twenty-first-century media? The media that developed during the twentieth century (and that continue to this day) are primarily *mass media*—newspapers, publishing houses, and broadcast media like radio, television and cable. Mass media feature a relatively small number of speakers who publish or transmit content to mass audiences. In mass communication, many people form the audience, but few get to participate as speakers. Thus, its basic structure is few-to-many. There have always

---

9. See generally NEIL RICHARDS, *INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE* (2015).

10. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

been exceptions of course: telephone communication is one-to-one. Ham radio equipment allows people with relatively little money to broadcast. But for the most part, the twentieth-century's dominant media were closed to the vast majority of people who wanted to publish or broadcast their own content.

A second important feature of twentieth-century-style media is that the publishers, broadcasters, and movie studios produce most of the content they publish or broadcast, or else contract with a relatively small number of people and businesses to provide content. The business of mass media is *not* to publish the content of the vast majority of ordinary citizens—rather, the latter form their *audience*, not their content providers. That's why mass communication industries developed with various specialties: producers, directors, editors, actors, announcers, entertainers, and so on.

By contrast, twenty-first-century media are organized differently. They do not assume that only a small number of people will speak to a vast audience. Communication is not only one-to-many or few-to-many. It is also many-to-many. Everyone can participate in twenty-first-century communications media. This makes them more like telephones, but with an important difference. Instead of communicating with one other person, people can communicate with an indefinite number of people. They can also engage in mass communication. They can also be broadcasters.

The promise of twenty-first-century media is what I have called a democratic culture—a culture of mass participation rather than the culture of mass audiences that characterized the twentieth century.<sup>11</sup> Everyone can, in theory, participate in mass communication, and everyone can have access to media that, in theory, could be viewed or

---

11. See Balkin, *Digital Speech and Democratic Culture*, *supra* note 5, at 9–12.



read by people around the world, even if, in practice, not everyone is interested in everything that everyone else has to say. People can address themselves to a small number of people, but they can also speak to an indefinite public.

The media companies of the early twenty-first century are also different from those that arose in the early to mid-twentieth century. Their primary business is not broadcasting their own content or the content of a small number of business partners. Rather, their job is to transmit or serve as a platform for everyone's content, and their business models actively encourage mass participation. Very few people got to write for the twentieth-century version of the *New York Times*. But everyone can post on Facebook, and, moreover, Facebook wants you to post, as often as possible. Google wants you to create as many webpages as you like so that it can index them. Pinterest and Instagram want you to post lots of photos, Twitter wants you to tweet to your heart's content, and so on.

*How to pay for the public sphere*

The political economy of freedom of speech concerns, among other things, how to pay for a system of free expression in a given technological and social context. Despite the name, a system of free expression is not itself free; it requires investments in capital and infrastructure, particular forms of labor (and skills), and a set of social practices that interact with the communications technology of the time.

This question—how to pay for a robust sphere of public discourse—is at the heart of the Facebook/Cambridge Analytica scandal. That is because the scandal emerged from how Facebook finances its platform for social communication. Facebook makes its money primarily through selling advertising, matching advertisers with end-users. It performs this matching by collecting, processing, and analyzing data about its end-users. Now if end-users

aren't on Facebook, they won't see those ads, so it's important to make sure that end-users remain online as much as possible. To this end, Facebook also uses the same data to curate its feeds, trying to come up with ever new ways to entice its end-users to stay on the site and give Facebook ever more of their attention.

Twentieth-century media was paid for by a combination of advertising, sales of media goods, and subscription fees. Newspaper companies sold individual newspapers on newsstands and in stores; they sold subscriptions; and they also sold advertising space. Broadcasters were in a somewhat different position. Because, until very recently, all broadcast radio was free, radio stations made money primarily through selling ads. Book publishers got most of their money from the purchases of books, and in some cases, through subscription services like book-of-the-month clubs. Relatively little money came from advertising within books, although magazines often have lots of advertisements that help pay for the costs of publication. Cable companies made money through a combination of subscriptions, pay-per-view, and advertising.

If a company depends on advertising, it's very important to place the ads in front of people who might want to buy the products. But in the twentieth century, advertising could not be easily or precisely targeted at the individual level. One could do a bit of targeting—magazines, for example, appeal to different audiences, as do radio stations that specialize in certain kinds of music. Advertisers who wanted to reach people interested in sports or in fashion might advertise in *Sports Illustrated* or *Elle*, respectively.

Yet general-interest newspapers did not want to appeal to specialized audiences like magazines or radio stations did because they relied heavily on classified advertisements, and so they wanted to appeal to the widest possible audience. The desire for the broadest possible audience limited their strategies for targeted advertising.

Some twentieth-century media attempted to target advertisements, but the techniques were not very precise, and aimed mostly at large demographic categories. Other media actively sought general audiences and therefore found targeting counterproductive, although the ads might be directed at those consumers most likely to purchase goods—for example, the fabled 18–49 demographic.

These are the business models that financed twentieth-century media, and hence financed the system of free expression, and the creation of a robust public sphere with diverse and antagonistic sources of information and opinion. The economic structure of twentieth-century media shaped what kind of public sphere we would have.

We are in a different world now. But in this new world, the same basic problems remain. What business models make it possible for an economy to produce a robust public sphere of discussion and debate? How do we ensure diverse and antagonistic sources of information and opinion? How do we finance the kind of public sphere that is necessary for democracy, whether political democracy, or, as in my own theory of the First Amendment, cultural democracy?

It is entirely possible that we won't be able to finance the kind of digital public sphere that is best for political or cultural democracy. After all, the public sphere produced by the twentieth-century media ecology was skewed in many different ways; it had its own blind spots and biases.

The quality of the digital public sphere will depend in part on the business models of twenty-first-century media companies: Facebook, Google, YouTube, Twitter, Pinterest, and Instagram, are the most well-known examples. These companies originally didn't think of themselves as media companies at all, but rather as technology companies. Gradually, they came to understand that they were the most important players in the digital public sphere, and that, in different ways, they acted as gatekeepers, as

newspapers and broadcast stations had in the twentieth century.<sup>12</sup> These digital companies, in short, discovered that they were media companies whether they liked it or not.<sup>13</sup>

The twentieth-century public sphere depended heavily on for-profit business models. Is there any alternative? One way of avoiding dependence on for-profit business models would be to turn to public provisioning. Some nations have national broadcasters, for example, the BBC in Great Britain, or the CBC in Canada.<sup>14</sup> Some countries also have state-owned newspapers, although this is somewhat rarer in Western democracies.<sup>15</sup>

The government could own and run the broadband system within a country. It's certainly possible to have municipal wifi, although broadband companies have done their best to try to prevent it in the United States. One could also create a nationalized social media company—a sort of public option to Facebook and Twitter. One could even have a nationalized search engine—because one can't have an effective system of digital communication without search engines.

Nationalization of search engines and social media has been less frequent in Western democracies, partly due to the enormous startup costs for each country. Moreover, at least in the United States, a national search engine that made decisions about which links to prioritize and which to demote, or a government social media company that imposed the kinds of civility rules that Facebook and

---

12. See Balkin, *Free Speech in the Algorithmic Society*, *supra* note 5, at 1180–81.

13. *Id.* at 1181.

14. *Who We Are: At a Glance*, Linked to *Inside the BBC*, BBC, <https://www.bbc.co.uk/corporate2/insidethebbc/howweare/ataglance> (last visited Oct. 4, 2018); *Who We Are, What We Do: Canadian*, CBC, <http://www.cbc.radio-canada.ca/en/explore/who-we-are-what-we-do/canadian/> (last visited Oct. 4, 2018).

15. See Simeon Djankov et al., *Who Owns the Media?*, 46 J.L. & ECON. 341, 363 (2003).

Twitter employ, might raise serious problems under the First Amendment—unless all of its activities could be classified as government speech.<sup>16</sup> In China, however, there are close links between the government and the largest search engine Baidu, and between the government and the dominant social media companies, all of whom cooperate with the central government's requests for surveillance and censorship.<sup>17</sup> That, of course, is because the Chinese government wants to regulate and surveil its citizens' speech far more than Western democracies would tolerate.<sup>18</sup>

In the United States, as in many other places in the world, the Internet infrastructure is not owned by the government. Broadband companies, wifi companies, search engines, and social media platforms are privately owned. That means that the digital public sphere is not publicly provisioned. It has to turn a profit.

How do these companies make money? For basic Internet services—such as broadband companies, webhosting services, storage services, and domain name registries and registrars—the answer has generally been subscription, as it was for twentieth-century media like telephones and cable television.

But for search engines and social media platforms, the business model has largely been driven by advertising. Moreover, twenty-first-century technology made it possible to engage in targeted advertising of individuals in ways that were never possible in the twentieth century.

---

16. *Compare* Walker v. Tex. Div., Sons of Confederate Veterans, Inc., 135 S. Ct. 2239, 2253 (2015) (holding that government may make content distinctions with respect to its own speech), *with* Reed v. Town of Gilbert, Ariz., 135 S. Ct. 2218, 2231 (2015) (holding that content based regulations of private speech are subject to strict scrutiny).

17. *Social Media and Censorship in China: How Is It Different to the West?*, BBC (Sept. 26, 2017), <http://www.bbc.co.uk/newsbeat/article/41398423/social-media-and-censorship-in-china-how-is-it-different-to-the-west>.

18. *Id.*

THE INFRASTRUCTURE OF FREE EXPRESSION IS THE  
INFRASTRUCTURE OF SURVEILLANCE

Individualized targeting becomes possible because everything that people do online produces (or can produce) recordable data—the location of their computer or phone, the answers they give to quizzes, the goods they purchase, the sites they visit, the people they contact, the files they download, even their keystrokes. Every action in cyberspace is potentially recordable; it is just a matter of whether the recording is implemented and the data is stored. Companies can use all of this data to construct social graphs of individuals: who they talk to, who their friends are, what sites they visit, what they purchase, what they like and dislike, and so on. This also allows the construction of metadata and digital dossiers about individuals, which, in turn, assist companies (and governments) in forming judgments and predictions about them.

This degree of data surveillance and inference was not really possible in the twentieth century. For example, if you purchased a paperback book, the publisher could not tell whether you had actually read the book. But with Kindle applications, Amazon can tell how far you have read in a book and how long it took you. Your reading habits are traceable.

One can generalize this point. Almost every new media application of the early twenty-first century is both a method of communication and a method of surveillance. Twenty-first-century media offer ever more precise methods for surveilling and predicting the behavior of their end-users and the people those end-users communicate with.

Nor is that all. We are rapidly moving into a world dominated by the Internet of Things and personal robots. In the Internet of Things, every appliance, indeed, every possession, can, in theory, reveal information about its owners and operators. People don't even have to communicate with other human beings to be surveilled. A

whole new generation of applications and appliances are devoted to getting you to talk to them: Siri, Alexa, Cortana, and their friends really want to know what you think.

There is an ironic similarity to the world of *Downton Abbey*, the BBC series about British nobility in the first part of the twentieth century and their relationships with their servants. The butlers, valets, maids, and footmen are always standing by ready to serve the nobility. They are always present, and they don't say anything unless they are spoken to, but they are always listening. There is a well-known saying that "No man is a hero to his own valet." I would say that no one is a hero to Siri or Alexa.

A twentieth-century radio station could not surveil its listeners, and a twentieth-century television could not surveil its viewers—unless they agreed to be a Nielsen family. With cable television, however, it became possible to have limited forms of surveillance, and so it is no surprise that Congress passed an early form of privacy legislation to govern cable.<sup>19</sup>

By contrast, in twenty-first-century media, surveillance is the norm rather than the exception. Everything becomes traceable, and the possibilities for surveillance explode. Even if firms only collect very basic metadata—whom end-users contacted, what sites they visited, and for how long—firms can still generate a great deal of information about their end-users and those they communicate with.

With sufficient computing power and computer storage, companies can analyze this data and make judgments. But a further characteristic of the digital age is that over time the cost of computation and the cost of storage become ever more inexpensive, thus, facilitating new forms of surveillance, analysis, and prediction.

Surveillance, data collection, and data analysis are, by

---

19. See Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984).

now, central to the twenty-first-century media ecology and, for that matter, to twenty-first-century capitalism. Surveillance, data collection, and data analysis fund key aspects of the digital infrastructure—as well as many other applications and services. This means that the infrastructure of freedom of expression—the infrastructure that you use to communicate with your friends and relatives, the infrastructure that you use to post your cat videos, the infrastructure that you use to post pictures of your vacation so that all of your friends will be jealous of you, the infrastructure that you use to post your engagement announcements or your birthday celebration—is also the infrastructure that companies use to surveil you and to record your movements, contacts, habits, likes, and dislikes. The two are one and the same.

The infrastructure of digital free expression is the infrastructure of digital surveillance.

Once again, the government could provide all of this infrastructure—from broadband to social networks to search engines—and fund it with tax revenues or deficit spending. But in that case, the infrastructure of free expression would be the infrastructure of *government* surveillance. As it is, the government repeatedly seeks to harness the technologies of private surveillance for its own ends. If the government owned the infrastructure, it could eliminate the middle man. It could collect enormous amounts of data about people's habits, locations, and preferences simply by operating social media and search engines, which it could then analyze to make predictions about people's likely behavior. The Fourth Amendment would provide little restraint, because, by hypothesis, people willingly offer data about themselves in order to use the government-provided service.

Therefore, to the extent that one turns to government provisioning as an alternative to private companies, it will be necessary to have extremely strong safeguards against the collection, collation, and analysis of data willingly given



to government infrastructure providers. Put more bluntly, politicians, law enforcement officials, and bureaucrats alike would have to have the political will to prevent the government (and themselves) from collecting all that data and using it. I think it is very unlikely that government actors will be able to restrain themselves.

Failing the development of a public option, then, the current system primarily involves a system of private digital surveillance, which both private entities and governments seek to harness for their own ends.

The grand bargain of twenty-first-century media looks like this: Privately-owned infrastructure companies will provide you with many different valuable services. They will provide you with a search engine that is nothing short of miraculous—that allows you to find anything you want virtually instantaneously. They will provide you with social media that allow you to publish and express almost anything your heart could desire. Indeed, they will encourage you to publish and to communicate with others, repeatedly and incessantly. End-users get all of these services, all of this stuff—and they get it all for free. And in return, media owners get to collect their data, analyze it, and use it to predict, control, and nudge what end-users do.

It is theoretically possible that search engines and social media sites could forsake data collection and analysis by forsaking advertising revenue. They could move to a subscription service—that is how broadband and DNS registries operate. We have already seen this business model in operation with various streaming services such as Spotify, Pandora, Hulu, and Netflix. These companies offer a combination of subscription and free services that are paid for by data surveillance. Yet it's important to recognize that even if social media companies offered tiered services like Spotify and Pandora—that is, free services plus subscription services—there is no reason to think that the result would be less surveillance of the people who pay for the subscriptions. Subscribers might get fewer ads in their

feeds, but their social graph and personal data might be just as valuable to the company and to its business partners.

In any case, a subscription model has disadvantages for social media companies because it might produce a far smaller user base, and therefore less interesting and intriguing content that would keep end-users coming back for more. By contrast, Facebook's existing business model of free services in exchange for data surveillance leads it to try to get as many people as possible to join Facebook, to visit the site as often as possible, to engage with the site as often as possible, and spend as much time on the site as possible.

The twentieth-century model of broadcast media and mass media was a model of scarcity of media access; not everyone got to publish in the *New York Times* or broadcast on CBS. The scarcity of twenty-first-century media is the scarcity of attention—the scarcity of eyeballs.<sup>20</sup> To continue to grow—and thus continue to please its shareholders—Facebook has two choices. First, it can attempt to increase the total number of end-users. Facebook already has some two billion users in a world of seven billion potential customers.<sup>21</sup> Second, Facebook can grow by finding ever new ways to get its end-users to spend more and more time on the site. The second strategy dominates over time, and this is why, as Tim Wu has explained, social media sites like Facebook try to addict you—to engage you and keep

---

20. See Herbert A. Simon, Designing Organizations for an Information-Rich World, in *COMPUTERS, COMMUNICATIONS, AND THE PUBLIC INTEREST* 37, 40 (Martin Greenberger ed., 1971) (“[A] wealth of information creates a poverty of attention . . .”); ZEYNEP TUFEKCI, TWITTER AND TEAR GAS: THE POWER AND FRAGILITY OF NETWORKED PROTEST 271 (2017); Balkin, *Digital Speech and Democratic Culture*, *supra* note 5, at 7 (“The digital revolution made a different kind of scarcity salient. It is not the scarcity of bandwidth but the scarcity of audiences, and, in particular, scarcity of audience attention.”).

21. *Number of Monthly Active Facebook Users Worldwide as of 2nd Quarter 2018 (in Millions)*, STATISTA, <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> (last visited Oct. 2, 2018).

you coming back for more, and more, and more.<sup>22</sup> The theoretical limit for a company like Facebook is all seven billion people in the world spending twenty-four hours a day on Facebook—unless, somehow, they get the folks on Alpha Centauri to sign up.

### THREE PROBLEMS FOR THE TWENTY-FIRST-CENTURY MODEL

The implicit bargain of twenty-first-century media capitalism produces three interrelated issues: the problem of private governance, the problem of new-school speech regulation, and the problem of private surveillance. I have already written a great deal about the first two,<sup>23</sup> and so I will only mention them in passing.

#### *Private governance*

The first set of issues concern how social media govern us and the spaces we use to communicate with each other. The problems of social media governance are manipulation on the one hand, and arbitrariness and non-transparency on the other.

First, social media curate and shape what we experience on their sites. For example, people get personalized feeds on Facebook—they don't get all possible posts of Facebook friends in the order in which they were posted. Rather, Facebook tries to decide which posts will be most engaging—most compulsive, interesting, and

---

22. TIM WU, *THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS* 289–302 (2016) (describing how social media companies attempt to attract advertisers by cornering the market on attention and addicting customers); Tim Wu, *Subtle and Insidious, Technology Is Designed to Addict Us*, WASH. POST, [https://www.washingtonpost.com/opinions/subtle-and-insidious-technology-is-designed-to-addict-us/2017/03/02/5b983ef4-fcee-11e6-99b4-9e613afeb09f\\_story.html?utm\\_term=.74b2a3a0012f](https://www.washingtonpost.com/opinions/subtle-and-insidious-technology-is-designed-to-addict-us/2017/03/02/5b983ef4-fcee-11e6-99b4-9e613afeb09f_story.html?utm_term=.74b2a3a0012f) (last visited Nov. 11, 2018) (“[F]or a product like Facebook, success and user addiction are the same thing.”).

23. Balkin, *Free Speech in the Algorithmic Society*, *supra* note 5; Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 Harv. L. Rev. 2296 (2014) [hereinafter Balkin, *Old-School/New-School Speech Regulation*].

addictive.<sup>24</sup> It also tries to organize the order of posts to make them more interesting and entertaining. Facebook may also include posts or items from people who are not one's Facebook friends in order to create an entertaining, engaging, and absorbing—some would say addictive—experience.<sup>25</sup> This creates a potential conflict of interest: social media companies have natural incentives to manipulate and even addict their end-users to increase their profits.

Second, because social media companies encourage as many people as possible to use their sites, the inevitable result is incivility, trolling, and abuse. Digital media create both a sense of immediacy and a sense of distance between people; when this happens, some end-users will behave in ways that they would be ashamed to behave when confronting others face to face. Social media sites therefore have to take on the role of governors, enforcing civility norms and policing for threats, abuse, and harassment.

In this way, as Kate Klonick has argued, social media companies become governors of their spaces, and not merely facilitators of communication.<sup>26</sup> Social media companies spend an increasing amount of their time policing their sites and deciding when and whether to take things down; and when social media companies remove posts, suspend users, or ban them, their operations are usually not

---

24. See, e.g., Victor Luckerson, *Here's How Facebook's News Feed Actually Works*, TIME (July 9, 2015), <http://time.com/collection-post/3950525/facebook-news-feed-algorithm/> (“[M]ost users see only a sliver of the potential posts in their network each day.”).

25. Paul Lewis, *‘Our Minds Can Be Hijacked’: The Tech Insiders Who Fear a Smartphone Dystopia*, GUARDIAN (Oct. 6, 2017, 1:00 AM), <https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia> (interviewing former employees at Google and Facebook who report that technologies are designed to addict users and monopolize their attention).

26. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1635–48 (2018) (describing bureaucracies at Facebook, YouTube, and Twitter).

transparent and offer little in the way of procedural due process.<sup>27</sup>

*New-school speech regulation*

A second issue is what I call “new-school” speech regulation. In more traditional, or “old-school” speech regulation, states aim at speakers and twentieth-century publishers and mass media. In “new-school” speech regulation, states aim at owners of digital infrastructure in order to get them to control or censor online speakers who may be too numerous, difficult to locate, anonymous, or outside the country.<sup>28</sup> New-school speech regulation, in other words, is the state’s attempt to harness private infrastructure owners’ growing capacity to surveil and govern the people who use the infrastructure, and to turn these capacities to the state’s purposes. Examples are the European Union’s “right to be forgotten,”<sup>29</sup> and the E.U.’s new digital hate speech rules—which involve agreements with the big four media companies.<sup>30</sup>

Just as states try to use private infrastructure to block or censor speech, they also try to use it to assist them with surveillance.<sup>31</sup> Data flows continuously through digital companies’ facilities, creating ever more data and

---

27. *Id.* at 1648.

28. Balkin, *Free Speech in the Algorithmic Society*, *supra* note 5, at 1175; Balkin, *Old-School/New-School Speech Regulation*, *supra* note 23, at 2298.

29. See Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317, ¶ 91; Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 *DUKE L.J.* 981, 986 (2018).

30. See *Code of Conduct on Countering Illegal Hate Speech Online*, STATEWATCH, <https://www.statewatch.org/news/2017/sep/eu-com-illegal-content-online-code-of-conduct.pdf> (last visited Aug. 1, 2018); *Countering Illegal Hate Speech Online #NoPlace4Hate*, EUR. COMMISSION (July 11, 2018), [https://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=54300](https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300) [<https://perma.cc/L29F-3YGP>].

31. Balkin, *Old-School/New-School Speech Regulation*, *supra* note 23, at 2297.

metadata. All of this is especially intriguing to nation-states, who would like to make judgments and predictions, to locate and identify people, and to trace and predict crimes and national security threats.<sup>32</sup> The information collected by infrastructure owners becomes a tempting target for nation-states—ever more tempting as infrastructure providers become better and better at collecting and analyzing this sort of information. Call this the problem of public surveillance.<sup>33</sup>

### *Private surveillance*

The third problem—which brings us to the Facebook/Cambridge Analytica scandal—is not the problem of state surveillance, but the problem of private surveillance. According to the grand bargain of surveillance capitalism, Facebook, Google and other media businesses offer free or heavily subsidized services in exchange for subjecting end-users to ever more effective ways of collecting and analyzing data that people produce whenever they interact with their sites. The goal is to turn this resource into money. Companies achieve this goal through private surveillance, data collection, and analysis—and by either selling end-users to advertisers, or else selling the data to others.

A familiar saying in the industry is that Big Data is the New Oil.<sup>34</sup> Data is a resource that is there for the taking—just as pools of oil were just lying under the surface before the Industrial Revolution.

If entrepreneurs like John D. Rockefeller could figure

---

32. *Id.* at 1155–57.

33. *See id.* at 2304–06, 2320, 2329–30 (explaining why private infrastructure is a tempting target for governments).

34. Jonathan Vanian, *Why Data Is the New Oil*, FORTUNE (July 12, 2016), <http://fortune.com/2016/07/11/data-oil-brainstorm-tech>; *see* Michael Palmer, *Data Is the New Oil*, ANA MARKETING MAESTROS (Nov. 3, 2006, 5:43 AM), [http://ana.blogs.com/maestros/2006/11/data\\_is\\_the\\_new.html](http://ana.blogs.com/maestros/2006/11/data_is_the_new.html).

out how to take that oil and refine it and sell it to other people, they could finance industrial capitalism and make a fortune in the process. In the same way, everyone leaves traces of themselves and their activities—data—whenever they use digital devices and wherever they go on the Internet, and if somebody can just figure out how to collect it, and refine it, and analyze it, harness it to make calculations and predictions, or sell it to others to make calculations and predictions, they can drive modern digital capitalism—that is, surveillance capitalism—and they can make a fortune in the process.

#### WORKING FOR THE MAN

Just as industrial capitalism made great fortunes, so too has digital capitalism. Instead of Rockefeller, and Vanderbilt, and Carnegie, we have Gates, and Zuckerberg, and Brin, and Schmidt. Just as poorly paid workers in lousy working conditions contributed to the fortunes of the First Gilded Age, so everyone, at home or at work, in pajamas or in business attire, contributes to the fortunes of the Second Gilded Age. We are all working for the Man.

All of us are workers in data factories, whether we know it or not. Every time you click on a link in Google, every time you visit Facebook, every time you post on Twitter, every time you upload a cat video on YouTube, you are working for the Man.

Not Vanderbilt, Alphabet. Not Rockefeller, Zuckerberg.

This phenomenon is twenty-first-century capitalism's appropriation and reconfiguration of open-source or peer-production methods, described and theorized in the early 2000s by Yochai Benkler.<sup>35</sup> Benkler described how Linux developers and Wikipedia created valuable information goods through peer-production, with relatively little

---

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

investment in bureaucracies and management hierarchies.<sup>36</sup> Where Benkler saw possibilities for freer, more participatory, and less coercive methods of business organization and peer production, digital capitalists have seen ways of saving money by reorganizing unpaid labor and collecting data about end-users in order to produce greater profits. This penguin is spying on you, collecting your data, and waddling all the way to the bank.

All end-users contribute to the production of an information good—the social media site—and its source of wealth, that is, data. People visit Facebook and create data; they like or dislike posts and create data; they post new content and create data; and they attract others to the site to read or view what they have posted. Even when you see something you don't like on Twitter or Facebook, you are still working for the Man. Perhaps somebody made a racist or abusive comment. You click a button to report the tweet or post, or you send a message arguing that such-and-such a post or comment is in violation of the company's terms of service. Even then, you are still working for the Man. Why? Because the site needs an army of people to discover when others violate its terms of service or community policies, and you are helping provide that service.<sup>37</sup> And in return, what do you get? Not a salary. You get a free service in which your data—and those of your friends and relatives—is used to keep you coming back to the site, and to sell you to advertisers and business partners.

That is why, although people say that Data is the New Oil, I like to say that Data is Soylent Green.<sup>38</sup> As Charlton

---

36. *Id.* at 60, 64–67, 70–73.

37. Catherine Buni & Soraya Chemaly, *The Secret Rules of the Internet*, VERGE (Apr. 13, 2016), <https://www.theverge.com/2016/4/13/11387934/internet-moderator-history-youtube-facebook-reddit-censorship-free-speech> (“[U]sers are not so much customers as uncompensated digital laborers who play dynamic and indispensable functions (despite being largely uninformed about the ways in which their labor is being used and capitalized).”).

38. Balkin, *Free Speech in the Algorithmic Society*, *supra* note 5, at 1154–57.



Heston reminds us, Soy lent Green is people.<sup>39</sup> You are your data, and that data is the raw material of digital capitalism. In the political economy of the early twenty-first century, your data is the price of your freedom of expression.

As noted above, digital media companies like Facebook are always trying to find new ways to squeeze money out of this raw material. One way to make money is to let other people use the social graph of end-users. Businesses can create applications which they can either place on Facebook's site itself, or they can use Facebook's login as their entry to the application. Once the end-user signs in to Facebook, the third party can gain access to their social graph—and, in some cases, the social graph of their Facebook friends—and use that data to provide services, do market research, sell advertisements, predict behavior, and so on. Facebook, in turn, can take a cut of the profits from the business.<sup>40</sup> This was Facebook's approach in its initial years, and although it has modified its business practices over the years, it is also the approach of many other digital companies that collect your data and share it with third parties.

Facebook has also provided pro bono access to scientific researchers, who could download personal data to engage in scientific studies.<sup>41</sup> This strategy doesn't make Facebook

---

39. SOYLENT GREEN (Metro-Goldwyn-Mayer Studios Inc. 1973); BradZ1, *IT'S PEOPLE!*, YOUTUBE (Nov. 19, 2007), <https://www.youtube.com/watch?v=8Sp-VFBbjpE>.

40. Paul Lewis, *'Utterly Horrifying': Ex-Facebook Insider Says Covert Data Harvesting Was Routine*, GUARDIAN (Mar. 20, 2018, 7:46 AM), <https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas> (explaining that under the policy, “a majority of Facebook users' could have had their data harvested by app developers without their knowledge”).

41. See *id.*; James Sanders & Dan Patterson, *Facebook Data Privacy Scandal: A Cheat Sheet*, TECHREPUBLIC (Oct. 25, 2018), <https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/>.

money directly, but it enhances its connections with data scientists around the world.

This is essentially what happened in the Cambridge Analytica scandal. Aleksandr Kogan, a data scientist, used Amazon's Mechanical Turk to find people who were willing to take a personality quiz for a dollar.<sup>42</sup> Mechanical Turk organizes the labor of strangers by offering them small amounts of money to perform particular tasks. This is another example of how money-making enterprises have adapted distributed peer-production systems for their own purposes.

People who took the quiz signed in to Facebook with their username and password. This, in turn, gave Kogan access to the Facebook data associated with the people answering the quiz, as well as the data of all of their Facebook friends, a practice that was apparently permissible under Facebook's then-existing data sharing policies.<sup>43</sup> This is how approximately 300,000 users allowed Kogan access to the data of some 87 million people.<sup>44</sup> Under such a regime, the more popular a person is—the more Facebook friends they have—the more valuable they are to the company and its partners.

But Kogan wasn't simply a data scientist. He was also

---

42. Carole Cadwalladr & Emma Graham-Harrison, *How Cambridge Analytica Turned Facebook 'Likes' into a Lucrative Political Tool*, GUARDIAN (Mar. 17, 2018, 9:02 AM), <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm>; Alex Pasternack, *A Facebook Scientist Tied to Cambridge Analytica Has Quietly Left Facebook*, FAST COMPANY (Sept. 6, 2018), <https://www.fastcompany.com/90231904/a-facebook-employee-tied-to-cambridge-analytica-quietly-left-facebook>.

43. Cadwalladr & Graham-Harrison, *supra* note 42.

44. See Michael Riley et al., *Understanding the Facebook-Cambridge Analytica Story*, WASH. POST (Apr. 9, 2018), [https://www.washingtonpost.com/business/understanding-the-facebook-cambridge-analytica-story-quicktake/2018/04/09/0f18d91c-3c1c-11e8-955b-7d2e19b79966\\_story.html](https://www.washingtonpost.com/business/understanding-the-facebook-cambridge-analytica-story-quicktake/2018/04/09/0f18d91c-3c1c-11e8-955b-7d2e19b79966_story.html) (estimating that 300,000 people participated and that 87 million users had their data harvested).

in cahoots with Cambridge Analytica.<sup>45</sup> Thus, he misrepresented himself to Facebook. He participated in Facebook's platform policy for researchers and scientists, but he turned over the data to Cambridge Analytica, a for-profit political consulting company that uses personal data to serve targeted political ads based on psychological profiles.<sup>46</sup>

#### INFORMATION FIDUCIARIES

This led to a scandal. But what exactly is the nature of this scandal? We should distinguish its various parts. One aspect is foreign participation in American elections in violation of federal campaign finance laws. Cambridge Analytica is a U.K. political consulting firm and employs many people who are not American citizens.<sup>47</sup>

A second aspect—targeted political ads—is not really much of a scandal. Political ads are core protected speech under the First Amendment. And political ads do not lose their First Amendment protection simply because they are targeted.

Targeted political ads—saying one thing to one group of people and another to another group of people—is as American as apple pie, or more correctly as apple pie to one group of Americans and cherry pie to another group. Indeed, ever more precise targeting of political advertisements is the wave of the future, if the future has

---

45. Cadwalladr & Graham-Harrison, *supra* note 42.

46. *Id.*

47. Paul Seamus Ryan, *Cambridge Analytica and Its Foreign National Staff Violated U.S. Laws*, JUST SECURITY (Mar. 26, 2018), <https://www.justsecurity.org/54272/complaint-filed-cambridge-analytica-foreign-national-staff-violated-u-s-campaign-finance-law/>; Craig Timberg & Tom Hamburger, *Former Cambridge Analytica Workers Say Firm Sent Foreigners to Advise U.S. Campaigns*, WASH. POST (Mar. 25, 2018), [https://www.washingtonpost.com/politics/former-cambridge-analytica-workers-say-firm-sent-foreigners-to-advise-us-campaigns/2018/03/25/6a0d7d90-2fa2-11e8-911f-ca7f68bff0fc\\_story.html?noredirect=on&utm\\_term=.afcb22899ae1](https://www.washingtonpost.com/politics/former-cambridge-analytica-workers-say-firm-sent-foreigners-to-advise-us-campaigns/2018/03/25/6a0d7d90-2fa2-11e8-911f-ca7f68bff0fc_story.html?noredirect=on&utm_term=.afcb22899ae1).

not already arrived.<sup>48</sup> To make targeting effective, of course, political operatives will need to know more and more about voters, which means that they will need lots of data about them, which means that they will either have to collect the data themselves or purchase it from others. Hence, digital capitalism predictably leads to new forms of political surveillance—political in the sense that it is operated by and for political parties, candidates, and their campaigns.

This is the model of the political organization as database<sup>49</sup>—the organization of politics around the same techniques that digital companies have already mastered to advertise products, just as earlier political operatives copied and mastered the techniques of Madison Avenue and twentieth-century advertisers.<sup>50</sup>

A third aspect of the scandal is most important for purposes of this lecture. The problem was not the revelation that Facebook had entered into an unusual business arrangement with a single company. The true scandal was that giving third parties access to personal data, and using personal data to manipulate people, were ordinary, run-of-the-mill business practices. Facebook's dealings with Cambridge Analytica were the tip of a very large iceberg.<sup>51</sup>

Understood in this way, the Cambridge Analytical scandal went to the heart of the grand bargain that pays for the digital public sphere. It laid bare a central problem of

---

48. See Antonio García Martínez, *How Trump Conquered Facebook—Without Russian Ads*, WIRED, (Feb. 23, 2018, 10:03 AM), <https://www.wired.com/story/how-trump-conquered-facebookwithout-russian-ads/>.

49. Jack M. Balkin, *The Last Days of Disco: Why the American Political System is Dysfunctional*, 94 B.U. L. REV. 1159, 1185–86 (2014) (describing the phenomenon of “The Party as Database,” in which a “party’s electoral success depends increasingly on its abilities at data mining and political surveillance of potential voters and messaging to those voters.”).

50. See JOE MCGINNISS, *THE SELLING OF THE PRESIDENT: THE CLASSICAL ACCOUNT OF THE PACKAGING OF A CANDIDATE* (Penguin Books 1988) (1968) (describing the use of Madison Avenue techniques in the 1968 presidential campaign).

51. Lewis, *supra* note 40; Sanders & Patterson, *supra* note 41.

our age: how to preserve the benefits of a freely accessible online public sphere while preventing digital companies from abusing their roles as collectors, analyzers, and users of personal data.

In order to do this, we have to rethink the role that digital companies play in our lives, borrow some old ideas from the law of the professions, and apply them to the twenty-first-century companies who collect, analyze and use our personal data for profit.

The central idea is this: We should regard the digital media companies who collect and use our personal data as *information fiduciaries* toward their end-users.<sup>52</sup> Because they are information fiduciaries, they have special duties of care, confidentiality, and loyalty toward their end-users.<sup>53</sup> Many of the biggest players in the Second Gilded Age—Facebook, Twitter, Google and Microsoft—are information fiduciaries.

What makes these companies information fiduciaries? People increasingly depend on these companies to perform services for them. The companies know a great deal about their end-users, and they can use that knowledge in many ways, but their end-users know next to nothing about their internal operations.<sup>54</sup> As a result, their end-users are especially vulnerable to these companies, and they have to trust that the companies will not abuse them, betray them, or manipulate them to increase the company's profit margins.

These four features of the situation—(1) the company provides special services based on special expertise; (2) there is a great asymmetry in knowledge between the company and its clients; (3) clients are especially vulnerable to the company because of the company's knowledge about

---

52. Balkin, *supra* note 10, at 1221.

53. *Id.* at 1207–08.

54. *Id.* at 1224–25.

them; and (4) the need for clients to trust the company to receive the benefit of the service—are standard reasons why the law recognizes fiduciary relationships.<sup>55</sup>

The law has long understood that special relationships of vulnerability and trust require special fiduciary obligations.<sup>56</sup> Examples are professionals like doctors, lawyers, and estate managers.<sup>57</sup> Each of them gains special information about their clients that could easily be used to their clients' disadvantage. For this reason, law requires them to act as fiduciaries toward their clients, with special duties of care, good faith, loyalty, and non-manipulation.<sup>58</sup>

A new class of fiduciaries has emerged in the Second Gilded Age. These new fiduciaries are the digital companies that perform a wide range of individualized services for us in return for the collection and monetization of our data. Social media and search engine companies in particular are among these new information fiduciaries of the digital age.

For example, Facebook provides an important service—a social network—that many people find not only valuable but indispensable. In the course of providing that service, people provide enormous amounts of data about themselves, making them (and their friends and loved ones) ever more vulnerable to Facebook. Their lives become transparent to Facebook, but Facebook's operations are not transparent to them. They have to trust that Facebook will not use its special knowledge and abilities to abuse them or manipulate them for its own profit and advantage. Facebook's right to hold and use personal data, in other words, depends on its fiduciary duty not to take advantage of its end-users' vulnerability. It has a duty not to abuse the trust that vulnerable end-users must place in Facebook in

---

55. *Id.* at 1221–23.

56. *Id.* at 1219.

57. *Id.* at 1208–09.

58. TAMAR FRANKEL, FIDUCIARY LAW 106–08 (2011); Balkin, *supra* note 10, at 1205–09.

order for the company to provide its services. As Mark Zuckerberg himself has said, if the company abuses that trust, “we don’t deserve” to have your data.<sup>59</sup>

This fiduciary duty arises out of a contractual relationship—the terms of service or end-user license agreement—that digital companies require of their end-users. But duties of an information fiduciary are not limited to the specific terms of Facebook’s privacy policy—a complicated contract that few people have actually read. If Facebook’s duties were wholly based on the terms of the contract, then it could make those duties vanish simply by changing its privacy policy. Rather, these fiduciary obligations exist on top of the contractual rights of the parties.<sup>60</sup>

Information fiduciaries have three basic duties: a duty of care, a duty of confidentiality, and a duty of loyalty.<sup>61</sup> The duties of care and confidentiality require information fiduciaries to keep data secure and not to disclose it to third parties unless those third parties are equally trustworthy and agree to the same duties of care, confidentiality, and loyalty as the fiduciary.<sup>62</sup> Thus, a digital company has a duty to protect its end-users not merely from its own actions, but also from the actions of those with whom it shares data. Fiduciary obligations “run with the data,” so that a digital company like Facebook has an obligation to ensure that whenever it allows another person or business to see, view, or employ Facebook’s end-users’ data, these

---

59. Lianna Brinded, *Facebook Is Buying Print Ads to Apologize for the Cambridge Analytica Scandal*, QUARTZ (Mar. 25, 2018), <https://qz.com/1236981/facebook-and-mark-zuckerberg-buy-newspaper-ads-to-say-sorry/>.

60. See FRANKEL, *supra* note 58, at 42–45; Balkin, *supra* note 10, at 1207.

61. See Balkin, *supra* note 10, at 1206–08; Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L.J. 879, 882 (explaining that fiduciaries “must be loyal to the interests of the other person” and that “[t]he fiduciary’s duties go beyond mere fairness and honesty; they oblige him to act to further the beneficiary’s best interests”).

62. Balkin, *supra* note 10, at 1220.

persons and businesses must take on the same duties of trust and non-manipulation that Facebook itself must take on.<sup>63</sup>

Finally, the duty of loyalty means that an information fiduciary must not use data to advantage itself at the expense of its end-users, and it must proactively work to avoid creating and acting on conflicts of interest between itself and its end-users.<sup>64</sup> What this means in practice will depend on the nature of the business.<sup>65</sup> Social media, like many other digital companies, exchange free or heavily subsidized services for the right to match end-users with advertisers, including individually targeted ads. This in itself could give rise to a conflict of interest, and regularly has. But unless we are to outlaw all targeted advertisements to subsidize digital services (which I would oppose and might raise First Amendment concerns), the proper solution is to limit the ways that digital companies may use their customers' data. The goal, in other words, is to ameliorate or forestall the conflict of interest by requiring companies to act in good faith, forbidding them from manipulating or harming their end-users to increase their profits, requiring them to vet and oversee contractual partners with whom they share data, and preventing them from giving access to third-parties who will manipulate or harm their end-users.

The Cambridge Analytica scandal shows how these fiduciary obligations work in practice. Facebook failed at all three of them. It failed in its duties of care and

---

63. *Id.* (duties “run with the data”); *id.* at 1233 (arguing that digital information fiduciaries “may also have duties to ensure that, when they sell or convey this information to others, duties of non-disclosure and non-manipulation travel with the data”).

64. *Id.* at 1208.

65. FRANKEL, *supra* note 58, at 53 (noting that “[t]he process of recognizing new fiduciary relationships is ongoing,” depending on the nature of their services, the power relations and temptations they create, and the ability of institutions and markets to control them); Balkin, *supra* note 10, at 1223, 1228.



confidentiality because it did not vet its contractual partners carefully enough. It did not make sure that it shared end-user data only with trustworthy persons and companies, and it did not ensure that its partners agreed to the same duties of care, confidentiality and loyalty. It did not sufficiently oversee and audit what Kogan and Cambridge Analytica did with end-user data, and it did not take steps to keep them from violating the interests of its end-users for their own profit and advantage. Although Kogan passed himself off as only a non-profit researcher, Facebook made many similar arrangements with for-profit companies in which it took a share of revenues in exchange for data access. Thus, Facebook failed at its duty of loyalty because it allowed third-parties to manipulate its end-users in order to make more money for itself. Finally, when Facebook learned about Kogan and Cambridge Analytica's behavior, it did not act quickly and effectively to claw back all of its end-user's data to protect them from further breaches of data security and further manipulation.

In short, the Cambridge Analytica scandal demonstrated most of the things that an information fiduciary should *not* do with its end-users' data. That is what made it such a characteristic scandal of the Second Gilded Age. It exposed how the grand bargain of free services for data—the bargain that makes the digital public sphere possible—allows companies to betray the trust of the vast numbers of people who rely on these companies in their everyday lives.

Because of the economic logic that underpins the digital public sphere, capitalism has created a new system of relationships between us and digital media companies. These relationships have created new forms of digital vulnerability, and therefore these relationships should be fiduciary relationships, relationships of trust. When companies breach such a relationship of trust, they are not protected by the First Amendment any more than doctors and lawyers are protected by the First Amendment when

they disclose sensitive information about their clients and patients.<sup>66</sup>

I have given only a general introduction to the obligations of digital information fiduciaries, and there is much more that has to be worked out over time. There will also be close cases in which it is not clear whether a digital enterprise should be treated as an information fiduciary. To deal with this problem, Jonathan Zittrain of Harvard Law School and I have laid out a basic proposal for a Digital Millennium Privacy Act.<sup>67</sup> The DMPA would propose a new grand bargain to protect digital privacy. It would grant companies a safe harbor from state privacy regulation if companies agree to take on the fiduciary duties of care, confidentiality, and loyalty toward their end-users.

#### CONCLUSION

The Cambridge Analytica scandal is evidence that there is something deeply wrong with the grand bargain that pays for freedom of expression in the Second Gilded Age. The point of the concept of information fiduciaries is to rewrite that bargain, and to place the political economy of digital speech in the Second Gilded Age on a fairer, more decent footing.

The Second Gilded Age has produced vast fortunes, and some of the most powerful companies that have ever existed. But it has also given rise to a new class of fiduciaries: companies with obligations of trust and good faith to their end-users and to the public as a whole.

As the First Gilded Age drew to a close near the end of the nineteenth century, things looked pretty grim for

---

66. See Balkin, *supra* note 10, at 1210–20 (explaining why fiduciary relationships are treated differently under the First Amendment).

67. Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016), <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/>.

American democracy. Government was essentially for sale. America was dominated by what Teddy Roosevelt called “the great malefactors of wealth.”<sup>68</sup> Americans seemed locked into a political economy of ever increasing oligarchy and corruption. And if you had asked people about American politics in 1895, they might well have despaired about the future of American democracy.

But we know what happened after that. There was a renaissance of reform and an era of gradual improvement of American democracy, not perfect in all respects, but certainly better than things stood at the end of the nineteenth century. That is the message that I want to leave you with. What we did once before, during the First Gilded Age at the end of the nineteenth century, we can do again, in the Second Gilded Age, at the beginning of the twenty-first century. It will require a refusal to settle for the status quo, and a belief in the long run success of democracy. It will require mobilization, it will require protest, and above all, it will require the long grind of politics. But it has been done before, and we can do it once again.

---

68. Theodore Roosevelt, Address of President Roosevelt on the Occasion of the Laying of the Corner Stone of the Pilgrim Memorial Monument, Provincetown, MA, (Aug. 20, 1907), *in* Washington, DC, Government Printing Office, 1907, at 47.