A HOOVER INSTITUTION ESSAY

Tech Giants at the Crossroads

A MODEST PROPOSAL

JON D. MICHAELS

Series Paper No. 1809

Major technology and social-media companies—think Facebook, Apple, Microsoft, and Google—wield tremendous power. Given their reach, their financial heft, their importance to vast swaths of customers dependent on their goods, services, and platforms, and their ability to influence (if not altogether dictate) transnational public policy, these firms often look and act the part of proprietors, stewards, and even governors of digital public squares.[1]

These firms do so right now at a moment of great political, economic, and technological flux and unease. Today, questions and concerns are regularly voiced over the tech giants' market share; over the ways they run their various digital platforms; over their editorial policies and ability to shape the news; and over their policing of (or failure to police) individuals and groups who use the firms' goods, services, and platforms.[2]

Questions and concerns likewise surround these tech giants' role in supporting US intelligence, law enforcement, and diplomatic operations at a moment when some of those operations are themselves subject to considerable debate and scrutiny.[3]

These firms thus find themselves at the center of two critical, vexing, and ultimately related conversations. First, there is what I'll call the *digital public square* conversation: millions of citizen-consumers rely on technology and social-media companies' goods, services, and fair and stable platforms to remain socially, politically, and economically engaged and empowered.[4] Second, there is the *deputization* conversation: many of those very same technology and social-media companies—so powerful in their dealings with the general public—are expected, pressured, and often obligated to share their data with government agencies, to facilitate or intensify state surveillance over citizen-consumers, and even to advance the state's domestic or foreign policy agenda.

To date, we haven't had great success determining what responsibilities or duties ought to attach to those firms in their dealings with citizen-consumers. Among other things,

we may inquire whether those firms' stewardship over the digital public square is benign? Is it too lax? Ought the government displace the firms as primary regulators? Ultimately, we're worried about the power that the tech giants wield over essential platforms, information, and technologies—and thus about the rights, liberties, and security of the citizen-consumers who've come to rely on those firms.

We likewise haven't made great progress in our efforts to conceptualize the relationship between those very same companies and the government. Specifically, we struggle with the propriety of deputization, as defense, law enforcement, intelligence, and foreign affairs agencies press the tech firms for assistance. Here the concerns center on government's coercive power over those firms, and on the ability of the government to disrupt and distort relations between the firms and citizen-consumers.

Perhaps one problem lies in our treating the *digital public square* and *deputized companies* questions separately. Thinking about the two questions in combination—and thus viewing the technology and social-media firms as potentially both victims and perpetrators in inherently unequal and imbalanced relationships—presents opportunities for a regulatory compromise or bargain that may help fix the pair of problematic links in the broader chain of private-public relations.

Conversation A
Twenty-First Century Public Squares and Mediating the Citizen-Consumer Relationship

Tech giants' stewardship of digital platforms and technologies gives those companies considerable influence over the public qua consumers and qua citizens. As gatekeepers and governors of the digital public square, those companies may deprive users of due process, equal protection, privacy, and various expressive liberties (while at the same time exposing those users to various harms perpetrated by other citizen-consumers).

Digital companies provide essential goods and services to those who expect to be fully—or even passably—engaged economic, social, and political actors. The public's dependence on the likes of Facebook, Microsoft, Apple, and Google is far deeper and more consequential than we often realize—and ought not to be trivialized in ways that offhanded quips about millennials' "addiction" to social media seem to suggest. As the *New York Times*'s technology columnist puts it, "We are, all of us, in inescapable thrall to one of the handful of American technology companies that now dominate much of the global economy."[5] Thus, whether we're gleefully glued to our smartphones

or reluctant, even resentful, users, the fact remains that living in an unavoidably digital world places considerable demands on us. And given that those demands are largely met (*or left unmet*) by tech giants, we find ourselves heavily reliant on a handful of firms.

Like every other market, the digital media space is one that invites us to consider questions of fairness, efficiency, quality, and choice. We may ask: is there competition among the tech firms? Is there meaningful consumer choice? Are there barriers to entry and exit, for competitors and consumers alike? Do information asymmetries exist—and, if so, whom do they disadvantage? Are the tech giants acting coercively (as is sometimes alleged) or just unfairly or, perhaps, deceptively? What are the third-party effects incident to the relationship between individual users and the corporate providers of digital content, technologies, and platforms? And are these platforms "safe" places for commercial and political engagement?

Enter the state. The government has no shortage of tools and experiences upon which to draw to correct or lessen the impact of sundry market failures or potential abuses. The government can, for example, regulate rates; insist upon greater transparency; specify consumer protections; mandate equal access; criminalize pernicious practices; and dictate privacy and (some) decency protocols. The government can, further, use antitrust authorities to break up any existing or would-be monopolies and deploy their taxing and spending powers to encourage greater competition.

Yet there are all sorts of reasons why traditional government regulation may not do the trick. Political will is a huge factor, especially given the financial clout of Silicon Valley and the size and scale of tech contributions to congressional and presidential campaigns. Sophistication is another challenge, as the complexity of the tech realm is beyond the grasp of many legislators, regulators, and jurists. Speed is yet a third, as technological advances arrive quickly and frequently, making it difficult for government policy makers to keep up. Fourth, there are important jurisdictional considerations. Does it even make sense to impose national regulations on global companies whose goods, services, and platforms transcend political boundaries?

These impediments to government regulation, while daunting, are not unique. Governments run into at least some of these difficulties in practically every sector of the political economy. What distinguishes the tech space, however, is the significance of the industry, the degree to which the industry is dominated by a handful of firms,

and the fact that the relevant technologies, services, and platforms at issue are ones that impinge on users' political rights and interests (making these firms different from, say, Walmart or General Motors). This is why we may say that the public interacts with the likes of Google and Facebook not solely as consumers but also as citizens. Indeed, for many of us, the virtual worlds of Twitter and Facebook are our best—or at least most attainable—present-day approximations of a public square.[6]

What further distinguishes the tech space is that several of the most prominent tech firms have, or at least at times have had, a cultural cachet that defies our ordinary intuitions about the relationship between customers and big businesses. Simply stated, many of the digital companies have enjoyed long periods of relative popularity. We curse the banks, big oil, airlines, and our health insurance companies. Yet, for quite some time, a substantial number of us have harbored far friendlier feelings toward the tech giants.[7] This lack of adversariness—fueled and reinforced by the giants' often aggressively trumpeted pro-user philosophies that purport to combine libertarian zeal with benevolent paternalism—has dampened the public's demand for government intervention.

As at least somewhat popular proprietors of digital public squares, the tech giants are in a prime position to establish and enforce their own rules governing entry to and enjoyment of said squares. Among other things, the tech firms may elevate, certify, redirect, and even deny opportunities for political expression, social intercourse, and commercial engagement. They may surveil and analyze use patterns. And they may filter, create, and deliver content, of varying degrees of credibility, individually packaged to each of us as discrete account holders.

Tech giants may well be glad to take on these governing responsibilities. Apart from, and in addition to, several of the companies' utopian pretensions, there is the simple business imperative to attract "eyeballs." To do so, the tech giants must find ways to keep us on their platforms, just as Las Vegas hotels endeavor to keep us in their casinos. But as the platforms become more and more all-encompassing—one-stop sites for travel, finance, news, research, politics, dating, and sports and entertainment—and more and more heavily trafficked, the need seemingly arises for comprehensive regulation of these more-than-virtual worlds to make them safe and desirable for users.

Absent the firms instituting their own comprehensive governance schemes, the platforms may well descend into anarchy, Hobbesian realms entirely uninviting to all but the most

unreasonable and irresponsible users. (Examples of such hyper-libertarian platforms exist, but to date those platforms are not sufficiently popular or profitable to elevate the proprietors to the status of "tech giants.") Alternatively, platforms may become self-governing, with thick cultural norms developed and imposed in a bottom-up fashion. (Those too, assuming they are ever sustainable, are likely to be small, niche enterprises.) Last, the government can surely attempt to comprehensively regulate, though any such state interventions would be subject to the caveats and qualifications mentioned above.

Under any of these scenarios, the Facebooks and Googles of the world would be ceding control, a costly proposition given that their business models turn, first, on recruiting and retaining users—an aim that requires considerable custodial management of platforms, again to make those platforms as welcoming (and as profitable) as possible; and, second, on possessing the means and authority to surveil those audiences, for the purpose of identifying and then catering to users' special interests as well as for selling highly remunerative advertising space to those keen on reaching carefully curated audiences.

Surely, the tech giants qua regulators are driven primarily by what governing strategies yield the highest profits. For those with an abiding faith in markets (and corresponding doubts about the responsiveness of bureaucracies), profit-sensitive governance might be an acceptable, even desirable, arrangement. After all, the tech giants have strong incentives to govern in ways that the public finds most attractive, thereby enticing new users and keeping existing customers happy and firmly in the fold.

But such faith in markets assumes too much. It assumes knowledgeable customers. It assumes ease of exit and the existence of ready alternatives. It assumes that there are few, if any, relevant interests which cannot be commodified, as well as few, if any, relevant interests apt to be systematically underpriced. (Here I'm thinking about various political and process interests that we may liken to public goods—that is, diffusely beneficial to the user community, if not society as a whole, but insufficiently personally beneficial to any one user to warrant her individual investment.[8]) And it assumes either that there aren't structural economic inequalities that give disproportionate influence to some users over others or that such inequalities don't matter in this particular space, perhaps because the interests of the consumer community are uniform and undifferentiated.

Given the likelihood of firms taking on the role of regulators, the likelihood that there is some misalignment of interests between providers and users, and the likelihood that

there is a divide between what may be of value to consumers and what may be of value to citizens, it may be worthwhile to think of these governed domains as twenty-first century public spaces. In such public spaces, tech giants do more than simply mediate private, commercial affairs. They also mediate political and civic affairs.

Consider the following:

> Expressive rights and potential restrictions on those rights are everywhere implicated when it comes to citizen-consumers and their use of telecom and digital technologies, social-media platforms, and the networks that enable access to those platforms. Many of those rights and restrictions are, again, mediated by the various providers. Denial of service, downgrading of users' "status," insistence on content conformity, the sharing of user profiles, correspondence, and search histories with commercial data brokers, or discriminatory or unequal provision of said service can seriously damage not just our material well-being but also our political voices and ears. Because so many of us spend considerable time and effort "speaking" and "listening" in these highly concentrated and overlapping digital public spaces, the damage is potentially significant. Simply opting out isn't realistic, at least not without forgoing opportunities to remain connected to the debates and conversations of the day.
>
> Added to those potential administrative or managerial harms perpetrated by the tech giants are ones that may be perpetrated by the tech giants when they develop and provide content and take an active role in editing, compiling, packaging, or ranking third-party content. Here we may worry about tech giants peddling false and misleading content, selectively removing other content (perhaps critical of their operating protocols), or sequencing content (especially paid or anonymous content) in a problematic fashion. Again, our worries are particularly acute and, I think, well-founded at a time when huge segments of the American public identify these platforms as the "place" where they get much of their news and when the leading companies have been embroiled in any number of content and advertising scandals involving bots and disseminators of fake news.[9]
>
> A third category of potential harms consists of injuries arising out of what we may call benign neglect: acts or omissions on the part of the tech firms that invite or enable citizen-consumers to mistreat their fellow users. Take, for example, user initiated and executed attacks—bullying, libeling, silencing, "doxing," or marginalizing. We may worry whether the proprietors of the platforms, having

asserted a governance role, are doing enough (or too much) to police these critical spaces, and, moreover, whether they are doing so in a fair, just manner.

Given the unique and influential role played by the handful of tech giants in mediating our political and civic affairs, the centrality and significance (for better or worse) of these digital public spaces, and the complications associated with direct government regulation, perhaps the moment is right for the giants to step up and govern the platforms as a sovereign state actor would.

What would this mean in practice? Among other things, users claiming injury or deprivation might be accorded due process to challenge wrongful denials or terminations of service or access. Restrictions on user speech (as well as any instances of the providers privileging certain forms of speech over others) might require a reasoned justification in keeping with the First Amendment's time, place, and manner jurisprudence. Users might also be granted the right to demand access to the plans and protocols firms use to govern their digital expanses. And, last, users might enjoy protection against unreasonable searches and seizures by service and content providers (more on this below). Government regulators, for their part, might need to remain vigilant, prepared to jump in if or when the tech giants prove unable or unwilling to act as truly public stewards of these essentially public spaces.

This is, to be sure, brief and cursory—just a first pass reconceptualization of the duties and responsibilities of tech giants.[10] At first blush, there seems to be insufficient incentive or motivation for the tech giants to embrace the role of truly public stewards (that is, de facto state actors). Yet once we come to appreciate that the user-provider relationship is only one-half of the equation, we may quickly realize why such an "embrace" is likely in the best interests of the tech giants.

Conversation B
Mediating the Client/State Relationship

Tech companies are encouraged, pressured, and ordered to facilitate government counterterrorism and law enforcement operations, doing so in ways that may conflict with said companies' commercial priorities and, perhaps, public obligations.

The deputization of American telecom, computer software and hardware, and social-media firms (not to mention financial, travel, and parcel companies) has garnered serious attention for well over a decade. Over that span, some of the names of the key

players have changed, as have the particular partnerships, the technologies, and the specific "asks." But, generally speaking, the government has shown itself to be creative and remarkably persistent in its efforts to team up (1) with those who can serve as force multipliers, providing the government with extra pairs of eyes and ears and thereby thickening the state's surveillance web; and (2) with those who can provide the government with special, privileged access, far greater and easier access than the government could obtain on its own.[11]

What I just referred to as special, privileged access is in part a function of important *legal-status* differentials. As a matter of regulatory, statutory, and constitutional law, private individuals and organizations are often better positioned to obtain, analyze, retain, and share personal information than are their more stringently regulated government counterparts.[12] Special, privileged access is also a function of *social or cultural* expectations. Targets of surveillance may well be more likely to disclose sensitive information to businesses under the once entirely reasonable assumption that private firms use that information to advance commercial aims—and nothing else.[13]

Reports on the breadth and depth of deputization relationships remain spotty. Anecdotal accounts do, however, suggest that some firms have shown themselves particularly willing to help, while others prove more reluctant.[14] And this is true whether the deputization arrangement is part of a financial or regulatory quid pro quo or is instead a response to a simple request for assistance.[15] (Corporate compliance pursuant to some legal directive such as a court order is, by my lights, qualitatively different from deputization. I say that even though legal compulsion may itself be met with more or less resistance.[16])

The problems with domineering, neglectful, or simply arbitrary governance of digital public spaces by tech giants should be apparent enough—and there are seemingly no offsetting benefits associated with such shaky stewardship. By contrast, the problems with deputization (and thus with heavy-handed treatment of the tech giants) are more abstract—and may at least seem to be counterbalanced by some presumed benefits, including heightened public safety and greater homeland security as a result of the government's enhanced surveillance capabilities.

Yet we must not forget that, among other things, deputization poses serious challenges for the companies and opens them up to legal and financial liability, while contributing to the erosion of goodwill that many of these companies have (or had) with the general

public. These tech giants are, no doubt, aware of their assumed or contractual duties to their customers; mindful of customer backlash; uneasy about what their competitors may or may not be providing the government; fearful to say "no" to a government which not only regulates their industry in various ways but also serves as a major purchaser of tech products and services; and cognizant of the awkward position deputization and related forms of collaboration may put them in vis-à-vis other governments with which they likewise transact business.

Given these various pressures and liabilities, the tech giants may well prefer the greater clarity that attaches to bright-line rules imposed on them by the government. Such rules could eliminate the legal, political, and economic ambiguities associated with informal deputization. Instead, firms would be treated as de facto state actors required to cooperate with counterterrorism and law enforcement investigations when—and only when—(1) some nontrivial showing of legal process is satisfied and (2) the firms abide by the (often considerably more stringent) privacy and transparency laws that bind the government. Having to follow such bright-line rules would enable the tech companies to credibly deny any agency in specific surveillance operations—and thus avoid the type of public blame that today attaches whenever citizen-consumers view companies as willing, even eager, facilitators of state surveillance. Additionally, having to follow bright-line rules would ensure that the tech companies won't have to look over their shoulders, guessing what their competitors are or aren't doing to support the government—and wondering what, if any, perks those competitors may be receiving in exchange for their voluntary assistance.

All of that is to say that the ironclad application and extension of public law duties, obligations, and restrictions to the tech giants may, perhaps counterintuitively, be liberating to those firms, which gain certainty, reduce risk, and deflect the ire of citizen-consumers and foreign governments alike. As is often the case in regulatory spaces, legal certainty is a prized commodity, even to those who bear the burden of heightened regulatory responsibilities.

Briefly, treating the deputies as extensions of the state might obligate courts to further chip away at the so-called "third-party doctrine." As currently formulated, the third-party doctrine allows the government to obtain from firms all sorts of sensitive customer data without first securing a warrant or issuing a subpoena. The government may do so on the theory that customers who share information with various businesses have no reasonable expectation of privacy in that information. Thus, while

government officials need a court order to access customer data directly (or to obligate an uncooperative firm to share that data), no legal process is due in the case of private firms volunteering to share vast troves of customer information with the government.[17] Given the pervasive and at times problematic ties between firms and the government, that doctrine, and its underlying rationale, seems increasingly suspect.

We might further expect an extension of all government-specific privacy restrictions—that is, those that limit government access, analysis, and retention—to all deputized companies, even those not classified as tech giants.

Last, we might anticipate prohibitions placed on companies partnering with the government from soliciting upfront, blanket consumer waivers, whereby consumers contractually agree to allow unmitigated data collection, analysis, and even repackaging as a condition of service or as a condition of cheaper or better service. Were outright prohibitions on privacy waivers deemed too strong, a more modest intervention might require companies facilitating government investigations to first offer the equivalent of a *Miranda* warning to all would-be users.[18] In effect, users would be advised that they have the right to refuse privacy waivers and that their failure to do so may be used against them in civil and criminal proceedings.

Joining the Two Conversations

In these layered relationships, one might see the tech giants as middle managers who both take and dish out workplace unpleasantries. When it comes to deputization, Facebook, Google, and the rest of their cohort may be credibly cast as *victims of government overreach*, pressured to cooperate. After all, it is very hard to refuse the government. The firms certainly don't want to be blamed if there is indeed a genuine national security danger. And, again, the firms have all sorts of other regulatory and commercial connections to the government and thus are loath to refuse state entreaties. At the same time, when it comes to tech firms regulating citizen-consumers (and their access to their goods, services, and platforms), those firms run the risk of being viewed as *perpetrators of corporate overreach*.

As this essay endeavors to show, by looking at the tech giants as the bridge between two sets of unequal relationships, we can glean some hope for a more synthetic understanding of the dynamic interplay of all three groups—state, firm, and citizen-consumer—and, with luck, arrive at some sort of compromise.[19]

If we were thinking *only* about protecting citizen-consumers' rights by blanketing the digital polis with constitutional safeguards, the companies would surely object. And if we were thinking *only* about protecting corporations from the various informal and unspoken pressures applied by government intelligence, counterterrorism, and law enforcement officials, the government would surely object just as vigorously. But by packaging the two, the tech firms may be more favorably disposed, accepting the restrictions in their dealings with the public at large as fair payment for the benefits they accrue from a more certain, less informally and ambiguously coercive legal relationship with the government. Likewise, this packaging might satisfy the government, which ought to care not just about facilitating various intelligence and surveillance operations but also about safeguarding and enriching the digital polis.

Of course, the devil is in the details, and big challenges remain. Among other things, we would need to define the reach of the digital polis, identify what industries and providers are within the ambit of these digital public spaces, and explain what specifically would satisfy the terms of, say, due process for the denial of service. Moreover, we would have to grapple with the question of precedent-setting—and what else would be demanded of companies once they are treated as state actors.

All of these questions and concerns would surely have to be worked out. But, for now, I hope this admittedly cursory sketch sheds some light on the ways in which two critical, urgent conversations—and two pressing sets of controversies—can be usefully connected, adding perspective and, perhaps, illuminating a path forward.

NOTES

1 See, e.g., Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech," *Harvard Law Review* 131 (2018): 1598; Franklin Foer, "Facebook's War on Free Will," *Guardian*, September 19, 2017, accessed June 29, 2018, https://www.theguardian.com/technology/2017/sep/19/facebooks-war-on-free-will; Farhad Manjoo, "How 5 Tech Giants Have Become More like Governments than Companies," interview by Terry Gross, *Fresh Air*, NPR, October 26, 2017, accessed June 29, 2018, https://www.npr.org/2017/10/26/560136311/how-5-tech-giants-have-become-more-like-governments-than-companies.

2 See, e.g., Greg Ip, "The Antitrust Case Against Facebook, Google and Amazon," *Wall Street Journal*, January 16, 2018, accessed June 29, 2018, https://www.wsj.com/articles/the-antitrust-case-against-facebook-google-amazon-and-apple-1516121561. Also see, e.g., Danielle Keats Citron and Helen Norton, "Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age," *Boston University Law Review* 91 (2011): 1435; Klonick, "The New Governors"; "Taming the Beast," *Economist*, May 28, 2016, accessed June 29, 2018, https://www.economist.com/news/business/21699465-european-governments-are-not-alone-wondering-how-deal-digital-giants-taming; Molly Price, "Democrats Urge Facebook and Twitter to Probe Russian Bots," C|net, January 23, 2018, accessed June 29, 2018, https://www.cnet.com

/news/facebook-and-twitter-asked-again-to-investigate-russian-bots; Aja Romano, "At Long Last, Twitter Has Begun Banning (Some, Not All) Nazis," *Vox*, December 18, 2017, accessed June 29, 2018, https://www.vox.com/2017/12/18/16790864/twitter-bans-nazis-hate-groups. Also see, e.g., Davey Alba, "Facebook's Officially a Media Company. Time to Act like One," *Wired*, March 6, 2017, accessed June 29, 2018, https://www.wired.com/2017/03/facebooks-officially-media-company-time-act-like-one; Jeffrey Gottfried and Elisa Shearer, "News Use Across Social Media Platforms 2016," Pew Research Center, May 26, 2016, accessed June 29, 2018, http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016; Angela Moon, "Two-Thirds of American Adults Get News from Social Media: Survey," Reuters, September 8, 2017, accessed June 29, 2018, https://www.reuters.com/article/us-usa-internet-socialmedia/two-thirds-of-american-adults-get-news-from-social-media-survey-idUSKCN1BJ2A8; Klonick, "The New Governors"; Adrienne LaFrance, "Donald Trump Is Testing Twitter's Harassment Policy," *Atlantic*, July 2, 2017, accessed June 29, 2018, https://www.theatlantic.com/politics/archive/2017/07/the-president-of-the-united-states-is-testing-twitters-harassment-policy/532497.

3 See, e.g., Jon D. Michaels, "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror," *California Law Review* 96 (2008): 901, accessed June 29, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1279867. Also see, e.g., Kim Zetter, "Apple's FBI Battle Is Complicated. Here's What's Really Going On," *Wired*, February 18, 2016, accessed June 29, 2018, https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on; Sue Pleming, "U.S. State Department Speaks to Twitter over Iran," Reuters, June 16, 2009, accessed June 29, 2018, https://www.reuters.com/article/us-iran-election-twitter-usa/u-s-state-department-speaks-to-twitter-over-iran-idUSWBT01137420090616.

4 By citizens, I mean members of a political community, which I take to be at least somewhat different from and generally broader than those the state formally recognizes as such.

5 Farhad Manjoo, "Tech's Frightful Five: They've Got Us," *New York Times*, May 10, 2017, accessed June 29, 2018, https://www.nytimes.com/2017/05/10/technology/techs-frightful-five-theyve-got-us.html.

6 See, e.g., Ariadne Vromen, Brian D. Loader, Michael A. Xenos, and Francisco Bailo, "Everyday Making through Facebook Engagement: Young Citizens' Political Interactions in Australia, the United Kingdom and the United States," *Political Studies* 64, no. 3 (2016): 513; Maeve Duggan and Aaron Smith, "Social Media and Political Engagement," Pew Research Center, October 25, 2016, accessed June 29, 2018, http://www.pewinternet.org/2016/10/25/political-engagement-and-social-media.

7 See, e.g., Chloe Aiello, Facebook Hit an All-Time High, Marking Full Recovery from Data Scandal, *CNBC*, July 6, 2018, accessed July 7, 2018, https://www.cnbc.com/2018/07/06/facebook-hits-all-time-high-marking-full-recovery-from-data-scandal.html?__source=sharebar%7Ctwitter&par=sharebar; Tim Bajarin, "6 Reasons Apple Is So Successful," *Time*, May 7, 2012, accessed June 29, 2018, http://techland.time.com/2012/05/07/six-reasons-why-apple-is-successful; Klint Finley, "What Tech Backlash? Google, Facebook Still Rank High in Polls," *Wired*, October 12, 2017, accessed June 29, 2018, https://www.wired.com/story/what-tech-backlash-google-facebook-still-rank-high-in-polls; Jason Murdock, "Mark Zuckerberg Says 'Delete Facebook' Protests Had No Meaningful Impact on His Business," *Newsweek*, April 5, 2018, accessed June 29, 2018, http://www.newsweek.com/zuckerberg-says-deleting-facebook-has-no-meaningful-impact-his-business-872876; Vauhini Vara, "You May Love Apple, But Can You Trust It?" *New Yorker*, September 19, 2014, accessed June 29, 2018, https://www.newyorker.com/business/currency/may-love-apple-can-trust.

8 Cf. CFTC v. Schor, 478 U.S. 833, 859, 863 (Brennan, J., dissenting) (raising concerns that individual litigants will always privilege those benefits "which are immediate, concrete, and easily understood" over those "which are almost entirely prophylactic, and thus often seem remote and not worth the cost in any single case").

9 See, e.g., Gottfried and Shearer, "News Use Across Social Media Platforms"; Moon, "Two-thirds of American Adults." Also, see, e.g., Jon Swaine, "Twitter Admits Far More Russian Bots Posted on Election

than It Had Disclosed," *Guardian*, January 19, 2018, accessed June 29, 2018, https://www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed; Max Greenwood, "Apple CEO: 'Fake News' on Social Media Is Bigger Issue than Russian Ads," *Hill*, November 1, 2017, accessed June 29, 2018, http://thehill.com/policy/technology/358296-apple-ceo-bigger-issue-than-russian-ads-is-fake-news-on-social-media; Ezra Klein, "Mark Zuckerberg on Facebook's Hardest Year, and What Comes Next," *Vox*, April 2, 2018, accessed June 29, 2018, https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge.

10 Note that even if there were considerable support in favor of the tech giants operating as state actors, the extension or application of US constitutional law to those firms would not necessarily be cheered by those who desire an especially aggressive regulatory solution to, among other things, online hate speech. After all, the Constitution may prevent the proprietors of a de facto public platform from imposing particularly stringent civility laws, ones that silence those trafficking in, say, offensive speech. What's more, it is unclear how much affirmative policing of peer-to-peer user behavior would be constitutionally mandated. The Constitution does not, for instance, guarantee individuals a right to be free from abuses perpetrated by their neighbors. So, for many, constitutionalizing digital platforms may not be a total solution.

11 I have described the details of these relationships elsewhere. See, e.g., Michaels, "All the President's Spies"; Jon D. Michaels, "Deputizing Homeland Security," *Texas Law Review* 88 (2010): 1435, accessed June 29, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1696312; Jon D. Michaels, *Constitutional Coup, Privatization's Threat to the American Republic* (Cambridge, MA: Harvard University Press, 2017). See also Kristen E. Eichensehr, "Public-Private Cybersecurity," *Texas Law Review* 95 (2017): 467.

12 See Michaels, *Constitutional Coup*, 190.

13 Ibid.

14 See, e.g., Michaels, "All the President's Spies"; Spencer Ackerman, "Mystery Company Told NSA Spies: Get a Warrant or Get Lost," *Daily Beast*, June 14, 2017, accessed June 29, 2018, https://www.thedailybeast.com/mystery-company-told-nsa-spies-get-a-warrant-or-get-lost.

15 Whether the increasing likelihood of public disclosures potentially embarrassing to the deputized companies (via unauthorized leaks) has had an effect on the tech giants' willingness to assist is an interesting question, but one I leave to the side for present purposes.

16 See, e.g., Ellen Nakashima, "Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks," *Washington Post*, February 17, 2016, accessed June 29, 2018, https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?utm_term=.75e94bdd29a3; Gram Slattery, "Facebook Rallies Social Media Allies in Fight Over NYC Police Search Warrants," *Christian Science Monitor*, August 12, 2014, accessed June 29, 2018, https://www.csmonitor.com/USA/USA-Update/2014/0812/Facebook-rallies-social-media-allies-in-fight-over-NYC-police-search-warrants.

17 See, e.g., Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976). The third-party doctrine has been called into question in *United States v. Jones,* 565 U.S. 400 (2012). See, e.g., *Jones,* 565 U.S. at 417 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."). And, that doctrine has been narrowed in *Carpenter v. United States,* No. 16-402 (June 22, 2018), accessed July 7, 2018, https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

18 Cf. Miranda v. Arizona, 384 U.S. 436 (1966).

19 Cf. Jack M. Balkin and Jonathan Zittrain, "A Grand Bargain to Make Tech Companies Trustworthy," *Atlantic*, October 3, 2016, accessed June 30, 2018, https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346.

The preferred citation for this publication is:
Jon Michaels, "Tech Giants at the Crossroads: A Modest Proposal," Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1809 (July 26, 2018), available at https://www.lawfareblog.com/tech-giants-crossroads-modest-proposal.

About the Author

JON D. MICHAELS

Jon D. Michaels is professor of law at the University of California–Los Angeles School of Law. His recent writings on constitutional, regulatory, and national-security law have appeared in *Foreign Affairs*, the *Harvard Law Review, Yale Law Journal, University of Chicago Law Review*, and *Columbia Law Review*. His new book, *Constitutional Coup: Privatization's Threat to the American Republic*, was published by Harvard University Press.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION