VIRGINIA LAW REVIEW ONLINE

VOLUME 105 FEBRUARY 2019 1-17

FOREWORD

FACEBOOK UNBOUND?

*Ashley Deeks**

The concept of checks and balances is a core tenet of our democracy; we fear letting any single institution become overly powerful or insufficiently accountable. As Americans, we naturally apply this concept first and foremost to the interactions among our three branches of government, given the principle's constitutional origins. What happens, though, when a handful of exceedingly powerful private actors—today's behemoth technology companies—begin to have as much control over our lives as the government does? Should the same impulse that drives our commitment to interbranch checks and balances kick in? How can we ensure that our democracy remains *our* democracy, even when digitized?

In the past, when highly powerful industries have emerged, our democratic system often has responded by erecting legal and regulatory frameworks around them. We applied antitrust laws to break up the railroads and oil companies.[1] We established the Food and Drug Administration and the National Highway Traffic Safety Administration to ensure that drug and car manufacturers take adequate measures to

* E. James Kelly Jr.-Class of 1965 Research Professor of Law, University of Virginia Law School. Thanks to Professor Jennifer Daskal, Professor Rebecca Hamilton, and Professor Rebecca Ingber for very helpful comments.

[1] See, e.g., United States v. Trans-Missouri Freight Ass'n, 166 U.S. 290 (1897) (applying antitrust law to the railroad industry); United States v. Joint Traffic Ass'n, 171 U.S. 505 (1898) (same); Standard Oil Co. v. United States, 221 U.S. 1 (1911) (applying antitrust law to the oil industry).

protect citizens' health and welfare.[2] And we heavily regulate common carriers, such as transportation and telecommunications providers, to ensure that they don't discriminate against groups within the general public.[3] Yet our three branches of government have engaged in only limited ways with technology companies such as Facebook, Google, and Amazon, even though these companies dominate their industries and have a tremendous influence on every corner of our lives—as various contributions to this symposium illustrate. Our government also has failed to regulate the use of high-technology tools that implicate our privacy, such as facial-recognition software and other controversial uses of machine-learning algorithms. Why has the government been slow to engage? Further, assuming that our society disfavors institutions that accrue unchecked power, especially when they wield that power in a way that affects our physical safety, our privacy, and our democratic arena, are there feasible ways to impose constructive constraints?

As an initial step in thinking about these questions, this essay examines a different context in which our checks and balances have proven weak: the national security space. It recounts the basic challenges that the other two branches have faced in checking the Executive's national security activities. The essay then identifies the ways in which those challenges resonate in the context of checking technology companies, helping us to understand why it has proven difficult for Congress and the courts (and the Executive) to weave a set of legal constraints around technology companies that offer us social media platforms, build advanced law enforcement tools, and employ machine learning algorithms to help us search, buy, and drive.[4] The essay explores alternative sources of constraints on the national security Executive, drawing inspiration from those constraints to envision other ways to shape the behavior of today's technology behemoths and other companies whose products are driven by our data.

[2] What We Do, FDA., https://www.fda.gov/aboutfda/whatwedo/ [https://perma.cc/6WYL-CQNS] (last visited Jan. 8, 2019); Understanding the National Highway Traffic Safety Administration (NHTSA), U.S. Dep't of Transp., https://www.transportation.gov/transition/understanding-national-highway-traffic-safety-administration-nhtsa [https://perma.cc/7L-H4-NDXB] (last visited Jan. 8, 2019).

[3] See, e.g., 47 U.S.C. § 201(a) (2018) (requiring every common carrier engaged in interstate communication by wire or radio to furnish such communication service upon reasonable request therefor); Thomas Nachbar, The Public Network, 17 Comm. L. Con. 67, 76 (2008) (discussing nondiscrimination requirements for package carriers, taxis, and railroads).

[4] See infra Part II.

I. THE NATIONAL SECURITY EXECUTIVE UNBOUND

It has become a truism that the Executive faces limited constraints when it undertakes activities to protect our national security. Congress rarely enacts statutes to restrict executive military and intelligence actions, and the courts are often loath to bar the Executive from taking the actions it deems appropriate. Accompanying this truism is a long-running debate about whether it is problematic that the Executive has accrued this much power. The debate reached a high-water mark with the publication of Eric Posner and Adrian Vermeule's book, *The Executive Unbound*, which argued that the Executive is effectively unconstrained by law and is limited only by politics and public opinion—and that this is unproblematic.[5] A number of scholars critiqued the book as providing an insufficiently nuanced view of how the executive branch operates, as giving inadequate weight to the power of law to constrain,[6] and as failing to appreciate the costs of an unchecked Executive.[7] Few, however, would contest that the Executive has very broad responsibilities in pursuing national security policies and that it can be difficult to force the Executive to alter or abandon those policies.

There are a variety of reasons why the Executive lacks constraints on its national security actions, at least from predictable sources.[8] Congress, the actor best positioned to impose those constraints, often proves both unwilling and unable to cabin the Executive's military and intelligence activities, including the use of wartime detention, targeted killings, and the introduction of troops abroad. First, Congress tends to lack knowledge about the details of such activities, including the advanced technologies

[5] Eric A. Posner & Adrian Vermeule, The Executive Unbound: After the Madisonian Republic 4–14 (2010).

[6] See, e.g., Aziz Z. Huq, Binding the Executive (By Law or By Politics), 79 U. Chi. L. Rev. 777, 782–83 (2012) (reviewing Posner & Vermeule, supra note 5) (arguing that legal rules and institutions play a "pivotal role" in the production of executive constraint); Saikrishna B. Prakash & Michael D. Ramsey, The Goldilocks Executive, 90 Tex. L. Rev. 973, 973–74 (2012) (reviewing Posner & Vermeule, supra note 5) (arguing that executive officials do not appear to regard themselves as above the law and that legal constraints on the Executive are manifest)..

[7] See, e.g., Peter M. Shane, Madisonianism Misunderstood: A Reply to Posner and Vermeule, Am. Const. Soc'y: ACSblog (Apr. 8, 2011), https://www.acslaw.org/acsblog/madisonianism-misunderstood-a-reply-to-posner-and-vermeule/ [https://perma.cc/G7YA-RZWF] (critiquing Posner and Vermeule for abandoning the rule of law).

[8] For a general discussion of systemic difficulties in checking the national security Executive, see Ashley Deeks, Predicting Enemies, 104 Va. L. Rev. 1529, 1560–63 (2018).

that the military and intelligence agencies are using.[9] Second, identifying sensible solutions for how to regulate these complicated technologies and programs is hard. It requires Congress to strike a nuanced balance between protecting the country and protecting individual life, liberty, privacy, and fair process. Third, Congress fears being blamed if, as a direct or indirect result of its laws, the country suffers an attack or crisis.[10] Finally, when Congress is divided, it faces the ordinary partisan gridlock that occurs whenever it tries to legislate.

The courts have also hesitated to act. Though the Supreme Court issued several high-profile detainee-related decisions in the decade after September 11, 2001, the Court and lower federal courts have avoided reaching decisions on the merits of a range of national security cases related to rendition, surveillance, detention, and military uses of force. Two related instincts seem to drive this. One is the courts' self-perception that they lack the technical, military, and foreign-policy experience to correctly decide these questions.[11] The other is their sense that Congress, not the courts, should make the hard policy decisions embedded in these cases because Congress is politically accountable in a way that the courts are not. In a case about the procedures to which detainees at Guantanamo were entitled, for instance, Judge Brown of the D.C. Circuit wrote in a concurrence that "the circumstances that frustrate the judicial process are the same ones that make this situation particularly ripe for Congress to intervene pursuant to its policy expertise, democratic legitimacy, and oath to uphold and defend the Constitution. These cases present hard questions and hard choices, ones best faced directly."[12] In a case challenging the Executive's alleged plan to target a U.S. citizen abroad, a D.C. district court relied on a lack of standing and the political-question doctrine to avoid the merits, noting that courts are ill-suited to "make real-time assessments of the nature and severity of alleged threats to national

[9] Ashley Deeks, Checks and Balances from Abroad, 83 U. Chi. L. Rev. 65, 70 (2016).

[10] See, e.g., Applying the War Powers Resolution to the War on Terrorism: Hearing Before the Subcomm. on the Constitution, Federalism, and Prop. Rights of the S. Comm. of the Judiciary, 107th Cong. 37 (2002) (statement of Sen. Russ Feingold, Chairman) (noting that Congress is "not necessarily eagerly asserting the powers that it has. It is a pretty good deal for Congress, if tough decisions about war are made by the executive; if things do not go well, they are not responsible").

[11] See, e.g., Crockett v. Reagan, 558 F. Supp. 893, 898 (D.D.C. 1982), aff'd, 720 F.2d 1355 (D.C. Cir. 1983) (noting, in a case involving the role of U.S. forces in El Salvador, that the court "lacks the resources and expertise (which are accessible to the Congress) to resolve disputed questions of fact" related to the military situation).

[12] See Al-Bihani v. Obama, 590 F.3d 866, 882 (D.C. Cir. 2010) (Brown, J., concurring).

security."[13] In these and a host of other cases, courts reveal their preference for avoiding decisions on hard national security questions that test the outer bounds of their expertise.

The end result of these enfeebled checks and balances is a very powerful Executive. However, a discussion of executive constraints that focuses only on the actions of Congress and the courts undersells the existence of other factors that constrain the national security Executive, a point I discuss below.

II. FACEBOOK UNBOUND

Many of the same dynamics that have made it difficult to rein in a powerful national security Executive are playing out in the technology space—leading to what we might call the "Facebook Unbound" phenomenon.[14] Indeed, the academic and foreign-policy conversation about the Executive's undue power in the national security space, which was a constant refrain in the post-9/11 era, has died down, to be replaced by conversation about the undue power of large technology companies.[15] Several essays in this symposium illustrate the companies' power and the lack of restrictions on how they use our data or control content on their platforms, and on how the government uses their products in ways that implicate our privacy. The journalist Farhad Manjoo, for example, has

[13] Al-Aulaqi v. Obama, 727 F. Supp. 2d 1, 9 (D.D.C. 2010).

[14] The reasons for the failures to constrain the national security Executive and technology companies are not unique to these two contexts. However, because there are several important similarities, certain lessons from the national security context can inform how we might proceed in the technology context. Nor do I mean to suggest an overly strong identity between the Executive and powerful technology companies. It should go without saying that there are significant differences between the two. The President faces democratic accountability; the tech companies do not. Unlike the President, tech companies cannot veto legislation. Nor can they invoke executive privilege when Congress asks for information. The companies are not entitled to deference by courts, and it is easier to hold them accountable when they violate the law.

[15] See, e.g., How 5 Tech Giants Have Become More Like Governments Than Companies, NPR (Oct. 26, 2017) https://www.npr.org/2017/10/26/560136311/how-5-tech-giants-have-become-more-like-governments-than-companies [https://perma.cc/C58F-ETVD] (interview of Farhad Manjoo, a tech columnist for the New York Times) [hereinafter Tech Giants] ("Amazon is sort of . . . getting its kind of corporate tentacles into a large part of the economy, into shipping, and how warehouses work and robots. Things that will allow it to dominate in the future that we're kind of just not good at regulating at this point."); see also Stephen L. Carter, Too Much Power Lies in Tech Companies' Hands, Bloomberg (Aug. 17, 2017), https://www.bloomberg.com/opinion/articles/2017-08-17/too-much-power-lies-in-tech-companies-hands [https://perma.cc/EM46-SAEY].

adopted the term "Frightful Five" to refer to Amazon, Apple, Facebook, Google, and Microsoft (all of which own other major technology and consumer products companies, including WhatsApp, Instagram, Waze, YouTube, Audible, Zappos, Whole Foods, and Waymo).[16] Other technology companies that have faced limited regulation include social media platforms such as Twitter; manufacturers of self-driving cars; Uber and Lyft; and companies that use "big data" and machine learning algorithms to produce highly sophisticated, privacy-implicating technologies for the U.S. military and federal, state, and local law enforcement.[17]

What unites these companies is their systematic collection and use of vast amounts of user data to make their products more powerful and their use of machine learning algorithms based on that data to make their systems more effective and more profitable. Some observers are untroubled by the relative lack of constraints on these companies and worry far more about the fact that the national security Executive is unbound. After all, the Executive can impose more severe sanctions and direct physical effects on individuals than companies can. In any case, these technology companies wield enormous control over our lives on a daily basis.[18] It is therefore worth exploring why our government has done little to regulate these companies.

The factors that have led to the lack of constraints on these technology companies are markedly similar to those that have produced the national security Executive. First, members of Congress lack sophisticated understandings of how these companies—and the technologies that undergird their products—work. This was brought into sharp relief when the Senate summoned Facebook CEO Mark Zuckerberg to testify about the company's privacy policies, data leaks, and Russian interference with

[16] Farhad Manjoo, Tech's 'Frightful 5' Will Dominate Digital Life for Foreseeable Future, N.Y. Times (Jan. 20, 2016), https://www.nytimes.com/2016/01/21/technology/techs-frightful-5-will-dominate-digital-life-for-foreseeable-future.html [https://perma.cc/8NXJVT-3L]; Tech Giants, supra note 15 (discussing the subsidiaries that the "Frightful Five" own).

[17] See, e.g., Ben Tarnoff, Weaponizing AI is coming. Are algorithmic forever wars our future?, Guardian (Oct. 11, 2018), https://www.theguardian.com/commentisfree/2018/oct/11/war-jedi-algorithmic-warfare-us-military [https://perma.cc/3LNH-E7N2].

[18] See, e.g., Rebecca MacKinnon, Consent of the Networked: The Worldwide Struggle for Internet Freedom 149–65 (2012) (describing major technology companies as "digital sovereigns"); Tech Giants, supra note 15 (discussing how Amazon, Google, Apple, Microsoft, and Facebook affect the economy, our elections, our jobs, and what we buy; how they innovate more aggressively than the U.S. government; how they act as gateways to many other products we use; and how they may suppress others' innovations).

the 2016 U.S. presidential election. At one point, Senator Orrin Hatch asked Zuckerberg how Facebook managed to make money; Zuckerberg, smiling slightly, responded, "Senator, we run ads."[19] As Daniel Solove has written, "There may be a few in Congress with a good understanding of . . . technology, but many lack the foggiest idea about how new technologies work."[20]

Second, knowing what to regulate, in what level of detail, and at what stage in the overall development of technologies such as machine learning is simply hard.[21] Laws can easily be overtaken by events in fast-changing areas such as war fighting or technology.[22] Third, Congress fears undercutting U.S. innovation by regulating too soon, which is not unlike Congress's fear of deliberately reining in the Executive's national security decisions, particularly in the face of threats from other actors who have not chosen to self-constrain.[23] The United States seeks to out-

[19] Nancy Scola, Zuckerberg Survived But Facebook Still Has Problems, Politico (Apr. 10, 2018), https://www.politico.com/story/2018/04/10/zuckerberg-facebook-hearing-senate-474-055 [https://perma.cc/V4JL-37JH].

[20] Daniel J. Solove, Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference, 74 Fordham L. Rev. 747, 771 (2005).

[21] Info. Soc'y Project, Governing Machine Learning (2017), https://law.yale.edu/system/files/area/center/isp/documents/governing_machine_learning_-_final.pdf [https://perma.cc/2PFE-6HBZ] [hereinafter Governing Machine Learning].

[22] Richard H. Pildes, Law and the President, 125 Harv. L. Rev. 1381, 1387 (2012) (reviewing Posner & Vermeule, supra note 5) (summarizing Posner and Vermeule's argument that, because technology is constantly shifting, it is better for Presidents to make their best judgments based on the actual circumstances then governing); Katy Steinmetz, Congress Never Wanted to Regulate Facebook. Until Now, Time (Apr. 12, 2018), http://time.com/5237432/congress-never-wanted-to-regulate-facebook-until-now/ [https://-perma.cc/GF4L-3CMW] ("Congress is always playing catch-up to technology, so statutes it writes can quickly become outdated.").

[23] Klint Finley, Obama Wants the Government to Help Develop AI, Wired (Oct. 12, 2016), https://www.wired.com/2016/10/obama-envisions-ai-new-apollo-program/ [https://perma.-cc/3TEH-FX6E] (quoting President Obama as stating, "The way I've been thinking about the regulatory structure as AI emerges is that, early in a technology, a thousand flowers should bloom. And the government should add a relatively light touch. . . . As technologies emerge and mature, then figuring out how they get incorporated into existing regulatory structures becomes a tougher problem, and the government needs to be involved a little bit more."); David Shepardson & Susan Heavey, Amazon, Apple, others to testify before U.S. Senate on data privacy September 26, Reuters (Sept. 12, 2018), https://ww w.reuters.com/article/us-usa-tech-congress/amazon-apple-others-to-testify-before-u-s-senate-on-data-privacy-september-26-idUSKCN1LS25P [https://perma.cc/G5JV-9WGW] (quoting Sen. John Thune as stating that Commerce Committee hearing would allow tech companies to testify about "what Congress can do to promote clear privacy expectations without hurting innovation"); see also Governing Machine Learning, supra note 21 (reflecting participants' views that standardizing the regulation of machine learning "would stifle innovation in a nascent industry, attempt to

innovate China; members of Congress will not want to stand accused of slowing down U.S. companies that are developing artificial intelligence, for instance, while Chinese companies press ahead. Finally, partisanship has kicked in when Congress *has* tried to regulate.[24]

This is not to say that Congress has enacted no rules regulating technology. In the past few years, Congress has been able to enact laws regulating cross-border data requests by law enforcement,[25] holding online platforms accountable if they are used to facilitate sex trafficking,[26] and updating the Foreign Intelligence Surveillance Act.[27] However, it has failed in its efforts to legislate on the use of encryption, election security (as Jacob Rush details in his contribution), "hacking back," and drone safety, and it has not tried to regulate facial-recognition software.[28] Efforts to impose federal data-privacy laws on companies are just getting underway.[29]

As with national security issues, some judges have articulated a view that they lack the capacity to correctly assess complicated technical tools

solve for problems that haven't yet arisen, and potentially create barriers to entry for new entrants").

[24] See, e.g., Paul Blumenthal, The Last Time Congress Threatened to Enact Digital Privacy Laws, It Didn't Go So Well, Huff. Post (July 27, 2018), https://www.huffingtonpost.com/entry/congress-digital-privacy-laws_us_5af0c587e4b0ab5c3d68b98b [https://perma.cc/82TJ-ESVA].

[25] Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, Div. V, § 103 (2018) (codified at 18 U.S.C. § 2703(h)).

[26] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, § 4, 132 Stat. 1253, 1254 (2018) (codified at 47 U.S.C. § 230(e)).

[27] FISA Amendments Reauthorization Act of 2017, Pub. L. No.115-118, 132 Stat. 3 (2018) (codified at 50 U.S.C. §§ 1881 –1881g).

[28] See, e.g., Jacob Rush, Hacking the Right to Vote, 105 Va. L. Rev. Online 67 (2019) (discussing Congress's failure to regulate election security); Dustin Volz, Mark Hosenball & Joseph Menn, Push for encryption law falters despite Apple case spotlight, Reuters (May 27, 2016), https://www.reuters.com/article/us-usa-encryption-legislation-idUSKCN0YI0EM [https://perma.cc/93WR-UQB6] (discussing Congress's failure to regulate encryption). A draft bill that would authorize companies to "hack back" in certain situations has been pending for several years. Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).

[29] Press Release, U.S. Sen. Ron Wyden of Or., Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy (Nov. 1, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy [https://perma.cc/4KKH-J4RH]. There are some existing federal privacy laws in specific areas, such as health care and student records. See Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, §§ 221, 264, 110 Stat. 1936, 2009, 2033 (1996); Family Educational and Privacy Rights Act, 20 U.S.C. § 1232g (2012). Further, California has enacted its own data privacy law. California Consumer Privacy Act of 2018, AB-375 (June 29, 2018).

and that Congress rather than the courts should be making the hard policy decisions in these areas.[30] In several recent cases that implicated law enforcement uses of new technologies, Justice Alito argued that it is far more desirable for Congress to articulate appropriate uses of law enforcement technologies than for the courts to decide those questions.[31] Although the Court did ultimately reach decisions in these cases, the Court in *Carpenter v. United States* asserted that it was producing a narrow holding that applied only to the specific technology at issue.[32] And in *United States v. Jones*, the majority relied on a Fourth Amendment trespass analysis to produce a relatively narrow opinion that would not reach technologies such as remote GPS tracking.[33] Finally, the Court obviously decides what cases to hear, and recently declined to grant certiorari in a case involving the use of predictive algorithms in criminal sentencing.[34]

Where we are dealing with constraints (or the lack thereof) on private companies, we also must ask whether the Executive has imposed regulations or other constraints. The Trump administration seems uninterested in taking steps to influence the behavior of social media platforms, even if it had authority to do so. The President seems to embrace, rather than bemoan, the divisive aspects of social media that Sarah Haan describes. Further, the Executive currently has limited incentives to shape the production and use of tools that law enforcement

[30] See Orin Kerr, The Fourth Amendment and New Technologies, 102 Mich. L. Rev. 801, 875 (2004) ("Judges struggle to understand even the basic facts of such technologies.").

[31] See Carpenter v. United States, 138 S. Ct. 2206, 2261 (2018) (Alito, J., dissenting); Riley v. California, 134 S. Ct. 2473, 2497–98 (2014) (Alito, J., concurring in part and concurring in the judgment). In *Carpenter*, Justice Alito wrote, "Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope."

[32] *Carpenter*, 138 S.Ct. at 2220 ("Our decision today is a narrow one. . . . We do not . . . call into question conventional surveillance techniques and tools . . . . Further, our opinion does not consider other collection techniques involving foreign affairs or national security. . . . [W]hen considering new innovations . . . the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'" (quoting Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944))). Paul Ohm argues that the opinion is in fact sweeping in its consequences, however. Paul Ohm, The Many Revolutions of Carpenter, 32 Harv. J.L. & Tech. (forthcoming 2019) (manuscript at 1–3), https://osf.io/preprints/lawarxiv/bsedj/ [https://perma.cc/B6HL-GS6F].

[33] 565 U.S. 400, 409–11 (2012).

[34] Loomis v. Wisconsin, SCOTUSblog, http://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/ [https://perma.cc/AC9D-3Z5P] (last visited Nov. 10, 2018) (listing the Supreme Court's denial of certiorari on June 26, 2017).

and military actors have started to deploy, such as facial-recognition software, body-worn cameras, and cell-site location information.[35] Finally, the Federal Trade Commission examined but chose not to bring an antitrust case against Google and the Trump administration does not appear poised to pursue an antitrust case against Amazon.[36] In short, the Executive has done little to bind Facebook and the various other types of technology companies described in this essay. We thus find ourselves confronting broadly unregulated technology actors that know and use oceans of information about us, holding vast amounts of power over what we read, buy, watch, think, and drive.

III. CONSTRAINING OUR UNBOUNDED ACTORS

Even though traditional checks and balances by Congress and the courts do not function very well in the national security space, the Executive nevertheless confronts certain constraints on its behavior. Most prominently, citizens can choose to vote the President out of office. There are a number of other, more nuanced ways in which the executive branch checks itself and is checked by nontraditional actors. First, the Executive often seeks public support for its decisions, which may require it to be more transparent than it would otherwise prefer.[37] In a recent example, President Obama disclosed how the Executive made decisions about targeted killings and what constraints it imposed on itself.[38] Sometimes leaks by government officials foist involuntary transparency on the Executive, too. Second, the Executive often makes changes to its national security policies when it faces litigation challenging those policies and it

[35] MacKinnon, supra note 18, at 175.

[36] Hal Singer, The FTC's Decision to Reject the Search Antitrust Case against Google, Forbes (Dec. 5, 2012), https://www.forbes.com/sites/halsinger/2012/12/05/the-ftcs-decision-to-reject-the-search-antitrust-case-against-google/ [https://perma.cc/2JBJ-GK97]; Laura Stevens, Why a Trump-Led Antitrust Case Against Amazon is a Long Shot, Wall St. J. (Mar. 31, 2018), https://wsj.com/articles/why-a-trump-led-antitrust-case-against-amazon-is-a-long-shot-1522501200 [https://perma.cc/9LN9-5EL2].

[37] See, e.g., Richard Neustadt, Presidential Power and the Modern Presidents 185 (1990) (identifying public standing as a source of presidential influence); Posner & Vermeule, supra note 5, at 113–53 (discussing ways the Executive can garner public support, including through transparency).

[38] Press Release, White House, Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities (May 23, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism [https://perma.cc/D23M-PXYR].

fears that it might lose the case.[39] Third, executive-branch lawyers, who often have a commitment to law as a guiding principle, help ensure that the executive branch generally complies with applicable laws and policies, even when it is inconvenient to do so.[40] Fourth, the Executive often needs to rely on allies for assistance in executing its foreign policy and national security decisions, which means that U.S. national security activities are sometimes indirectly subject to allies' legal and policy constraints.[41] Finally, the Executive itself engages with (or willingly brings itself under the supervision of) actors who are perceived as more neutral, such as the federal judges on the Foreign Intelligence Surveillance Court or the Department of Homeland Security's Office for Civil Rights and Civil Liberties.

Assuming that Congress will be unable—at least in the short term—to produce significant legislation on privacy, machine learning algorithms, or law enforcement uses of tools such as facial-recognition software, the same types of mechanisms that constrain the national security Executive might helpfully constrain the technologies and companies that are the subject of this symposium.

Public pressure and critiques already have played an important role in prompting companies such as Facebook and Twitter to establish more robust policies on user privacy and content regulation. This pressure has also forced the companies to be more transparent about their privacy and content moderation policies and the algorithms that they use to identify trolls and harassers.[42] Further, public criticism has led Facebook to remove the accounts of particular actors, including those of twenty Burmese officials and organizations responsible for what the United

[39] Ashley Deeks, The Observer Effect: National Security Litigation, Executive Policy Changes, and Judicial Deference, 82 Fordham L. Rev. 827, 838 (2013).

[40] Curtis A. Bradley & Trevor W. Morrison, Presidential Power, Historical Practice, and Legal Constraint, 113 Colum. L. Rev. 1097, 1132–33 (2013); Ashley Deeks, The Substance of Secret Agreements and the Role of Government Lawyers, 111 AJIL Unbound 474, 476 (2018).

[41] Deeks, supra note 9, at 76–77; Ashley Deeks, Intelligence Communities, Peer Constraints, and the Law, 7 Harv. Nat'l Sec. J. 1, 4–5 (2015).

[42] Sarah Frier, Facebook Publishes Content Removal Policies for the First Time, Bloomberg (Apr. 24, 2018), https://www.bloomberg.com/news/articles/2018-04-24/face boo k-publishes-content-removal-policies-for-the-first-time [https://perma.cc/4T4E-CFV7] (noti- ng that the "release of the document follows frequent criticism and confusion about the company's policies"); Julia Carrie Wong, Twitter Announces Global Change to Algorithm in Effort to Tackle Harassment, Guardian (May 15, 2018), https://www.theguardian.com/technology/2018/may/15/twitter-ranking-algorithm-change-trolling-harassment-abuse [https://perma.cc/9LR5-THZT].

Nations concluded was genocide against the Rohingya.[43] These new pressures come not only from the technologies' users but also from the companies' employees.[44] Facing demands from its employees, Google declined to extend its contract with the Defense Department, under which the company provided support to a project deploying machine learning algorithms to war zones.[45] Amazon is facing a similar challenge: 450 of its employees reportedly wrote to CEO Jeff Bezos to demand that Amazon cease selling its facial-recognition software (which the company calls Rekognition) to police.[46]

Like the national security Executive, these companies also are keenly attuned to potential litigation or legislation, and often change their behavior in an effort to fend off those alternatives. Microsoft in particular has been forward-leaning in an effort to help shape any legislation that might come down the pike. In testimony before the U.K. Parliament about regulation of artificial intelligence ("AI"), a Microsoft official told the committee that regulating AI was a job "for the tech industry, the Government, NGOs and the people who will ultimately consume the services" and that it was important "to find a way of convening those four parties together to drive forward that conversation."[47] Microsoft has also asked Congress to regulate facial-recognition software and has suggested specific areas on which Congress might focus.[48] Microsoft, Twitter, and

[43] Antoni Slodkowski, Facebook Bans Myanmar Army Chief, Others in Unprecedented Move, Reuters (Aug. 27, 2018), https://www.reuters.com/article/us-myanmar-facebook-/facebook-bans-myanmar-army-chief-others-in-unprecedented-move-idUSKCN1LC0R7 [https://perma.cc/MU2B-RJU5].

[44] See Kate Klonick, The New Governors: The People, Rules, and Processes Governing Online Speech, 131 Harv. L. Rev. 1598, 1627–28 (2018); Farhad Manjoo, Why the Google Walkout was a Watershed Moment in Tech, N.Y. Times (Nov. 7, 2018), https://www.nytimes.com/2018/11/07/technology/google-walkout-watershed-tech.html [https://perma.cc/52SF-DS75] ("Protests by [Google's] workers are an important new avenue for pressure; the very people who make these companies work can change what they do in the world.").

[45] Daisuke Wakabayashi & Scott Shane, Google Will Not Renew Pentagon Contract That Upset Employees, N.Y. Times (June 1, 2018), https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html [https://perma.cc/TAN3-N7QB].

[46] Isabel Asher Hamilton, An Amazon Staffer Says Over 450 Employees Wrote to Jeff Bezos Demanding Amazon Stop Selling Facial-Recognition Software to Police, Bus. Insider (Oct. 17, 2018), https://www.businessinsider.com/amazon-employee-letter-jeff-bezos-facial-recognition-software-police-2018-10 [https://perma.cc/4C93-ARDP].

[47] Science and Technology Committee, Robotics and Artificial Intelligence, 2016–17, HC 145, ¶ 66 (UK).

[48] Brad Smith, Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility, Microsoft: Microsoft on the Issues (Jul. 13, 2018),

Google all revealed how Russian agents had used their platforms in the lead-up to their officials' testimony before Congress, where they expected to be asked about that topic.[49] Facebook announced its strengthened advertising disclosure policies in an attempt to preempt a bill imposing such requirements by law.[50] More recently, Facebook revealed its intention to create an international body to adjudicate content decisions, which may well be an effort to stave off more stringent regulation by Congress.[51] There are exceptions: Google's CEO declined to appear before Congress, for example, even though he faced significant public pressure to do so.[52] In general, though, even if Congress cannot unite to enact laws, it has managed to convene congressional hearings that have extracted important information and policy changes from the companies.

Foreign governments have also imposed constraints on U.S. technology companies. Just as the U.S. military and intelligence communities sometimes find themselves bound by foreign laws during overseas operations, the U.S. tech companies face direct exposure to foreign legal systems, which have in several cases imposed onerous laws and penalties on them. For example, the EU's General Data Protection Regulation ("GDPR") requires companies that process personal data to obtain the affirmative consent of those whose data they are using (the "data subject").[53] Those processors must also provide, at the data subject's request, any information they have on the subject; must rectify inaccurate personal data; and must erase the subject's data at her request. Finally, the GDPR generally prohibits companies from transferring

https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility [https://perma.cc/MT9Q-GZW4].

[49] Mike Isaac & Daisuke Wakabayashi, Russian Influence Reached 126 Million Through Facebook Alone, N.Y. Times (Oct. 30, 2017), https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html [https://perma.cc/UW23-ZGG5].

[50] Id.

[51] Neil Malhotra, Benoit Monin & Michael Tomz, Does Private Regulation Preempt Public Regulation?, Am. Pol. Sci. Rev. 1 (2018); Evelyn Douek, Facebook's New 'Supreme Court' Could Revolutionize Online Speech, Lawfare (Nov. 19. 2018), https://www.lawfareblog.com/facebooks-new-supreme-court-could-revolutionize-online-speech [https://perma.cc/AHM4-WEMA].

[52] Steven T. Dennis, Senators Criticize Google CEO for Declining to Testify, Bloomberg (Aug. 28, 2018), https://www.bloomberg.com/news/articles/2018-08-28/google-ceo-pichai-faulted-by-senators-for-declining-to-testify [https://perma.cc/4K4E-2R5Q].

[53] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 7, 2016 O.J. (L 119) 2.

personal data outside the EU, unless the European Commission determines that the data protection laws of the receiving jurisdiction are adequate.[54] Although formally directed only to companies that are located in the EU or that provide services to or monitor the behavior of people in the EU, the GDPR's impact has been global. Virtually all of the companies discussed in this essay must comply with the GDPR. The EU also fined Google $2.7 billion for disadvantaging its competition by steering search engine users toward its comparison-shopping site.[55] The EU apparently also is considering whether to bring a case against Amazon.[56] In short, foreign governments have constrained U.S. tech companies, even when the U.S. government itself has not.

Finally, these companies have sometimes turned to neutral actors to increase their credibility among users and Congress. As Sarah Haan details, Facebook has enlisted the help of third parties to fact check and identify fake news.[57] Further, Facebook's plan to set up an independent body to adjudicate content takedowns would draw on the credibility of actors perceived as neutral and expert.[58] Tech companies including Google, Microsoft, Facebook, Nokia, and Ericsson have joined the Global Network Initiative, which commits them to respect freedom of expression and privacy rights when faced with government pressure to turn over user data or restrict communications.[59] Other companies have supported nonprofits such as OpenAI (the goal of which is to ensure that advanced AI capabilities are used for good, not harm) and the Partnership on Artificial Intelligence to Benefit People and Society, which Google, Facebook, Amazon, IBM, and Microsoft formed to establish ethical standards and best practices for AI researchers.[60] The companies have

[54] Id. arts. 44–46, at 8–9.

[55] Robert Levine, Antitrust Law Never Envisioned Massive Tech Companies Like Google, Bos. Globe (June 13, 2018), https://www.bostonglobe.com/ideas/2018/06/13/google-hugely-powerful-antitrust-law-job/E1eqrlQ01g11DRM8I9FxwO/story.html [https://perma.cc/ZH7D-TEVR].

[56] Guadalupe Gonzales, E.U. Antitrust Commission Sets Sights on Amazon. Here's Why, Inc. (Sept. 21, 2018), https://www.inc.com/guadalupe-gonzalez/amazon-margrethe-vestager-preliminary-investigation.html [https://perma.cc/EP6Z-4SHB].

[57] Sarah C. Haan, Facebook's Alternative Facts, 105 Va. L. Rev. Online 18 (2019).

[58] Mark Zuckerberg, A Blueprint for Content Governance and Enforcement, Facebook (Nov. 15, 2018), https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/ [https://perma.cc/TR8R-DDQ6].

[59] Global Network Initiative, https://globalnetworkinitiative.org [https://perma.cc/X66R-8JL3] (last visited Dec. 3, 2018).

[60] Greg Brockman & Ilya Sutskever, Introducing OpenAI, OpenAI: Blog (Dec. 11, 2015), https://blog.openai.com/introducing-openai/ [https://perma.cc/J3V2-NL4C]; Alex Hern,

taken all these steps to retain their users' support for their products and policies (and so maintain their profits).

Most recently—in a move that reflects the operation of three of these constraints at once—Facebook agreed to allow French regulators to monitor Facebook's policies and tools to observe how the company combats hate speech and to help structure future French regulatory efforts to fight online hate speech more generally.[61] This reflects an effort by Facebook to shape prospective legislation; a decision by a foreign government to impose pressure on the practices of a U.S. platform; and an attempt by Facebook to persuade its users that it is making serious efforts to improve its policies by inviting a kind of "neutral arbiter" to observe its practices. We are likely to see more of all of these types of constraints unless and until—and perhaps even after—legislators decide to act.

IV. MOVING FORWARD

Notwithstanding these different flavors of alternative constraints, the lack of consistent checks by Congress and courts on these technology companies means that the constraints are unpredictable, partial, and of questionable durability. As a result, there is still an important role for statutory constraints, should Congress find the political will to impose them. This is not to say that Congress should regulate for regulation's sake. Restrictions should be deliberate, balanced, effective, and sensitive to the speed at which technologies develop. In an ideal world, our democratic institutions would reassert themselves to develop legislation

'Partnership on AI' Formed by Google, Facebook, Amazon, IBM and Microsoft, Guardian (Sept. 28, 2016), https://www.theguardian.com/technology/2016/sep/28/google-facebook-amazon-ibm-microsoft-partnership-on-ai-tech-firms [https://perma.cc/EG74-RJVD].

[61] Tony Romm & James McAuley, Facebook Will Let French Regulators Study Its Efforts to Fight Hate Speech, Wash. Post (Nov. 12, 2018), https://www.washingtonpost.com/technology/2018/11/12/facebook-will-let-french-regulators-study-its-efforts-fight-hate-speech/ [https://perma.cc/L5QU-VYWB].

in five primary areas: antitrust,[62] the appropriate use of algorithms,[63] privacy, the responsibilities of technology platforms for the content they host, and the use by law enforcement of high-tech tools such as facial-recognition software. A host of proposals already exists on each topic, including in Katelyn Ringrose's essay on body cameras and facial-recognition systems. As another example, Congress could legislate norms for the development and deployment of machine learning algorithms at a relatively high level of generality (identifying impermissible sources of data, requiring companies to test input data and outputs for systematic bias, and requiring a level of algorithmic explanation when algorithmic decision-making affects individuals).[64] Institutionally, Congress could also bring on board more staffers with technological experience; create opportunities for technology fellows from think tanks and educational institutions; and restore the Office of Technology Assessment, a 200-member congressional support agency that operated from 1972 to 1995 and that researched and summarized technological and scientific matters for Congress.[65]

[62] Ted Cruz has called for use of antitrust laws to break up power of Facebook and others. Press Release, U.S. Sen. for Texas Ted Cruz, Sen. Cruz: We Have an Obligation to Defend the First Amendment Right of Every American on Social Media Platforms (Apr. 12, 2018), https://www.cruz.senate.gov/?p=press_release&id=3723 (accessed Jan. 8, 2019); see also Robert Levine, Antitrust Law Never Envisioned Massive Tech Companies Like Google, Bost. Globe: Ideas (June 13, 2018), https://www.bostonglobe.com/ideas/2 018/06/13/google-hugely-powerful-antitrust-law-job/E1eqrlQ01g11DRM8I9FxwO/story.html [https://perma.cc/L424-7XKW].

[63] See Mariano-Florentino Cuellar, Cyberdelegation and the Administrative State 10–14 (Stan. Pub. L. & Legal Theory Res. Paper Series, Working Paper No. 2754385, 2016), http s://ssrn.com/abstract=2754385 [https://perma.cc/2EPS-EZT8] (contemplating the executive branch's use of algorithms to regulate and adjudicate); Daniel Newman, Inside Look: The World's Largest Tech Companies are Making Massive AI Investments, Forbes (Jan. 17, 2017), https://www.forbes.com/sites/danielnewman/2017/01/17/inside-look-the-worlds-largest-tech-companies-are-making-massive-ai-investments/#54ff6f3c4af2 [https://perma.cc/HM-5D-W374] (describing how Amazon, Google, Apple, Microsoft are all investing heavily in AI).

[64] See Governing Machine Learning, supra note 21 (suggesting that regulation could mandate levels of explainability, prevent specific types of bias, or specify what types of models or data sets could be used for which purposes); Finale Doshi-Velez & Mason Kortz, Accountability of AI Under the Law: The Role of Explanation 5–7 (Berkman Klein Ctr. for Internet & Soc'y, Working Paper, 2017), http://nrs.harvard.edu/urn-3:HUL.InstRepos:3437 2584 [https://perma.cc/7GQ7-BB7K].

[65] Mitch Ambrose, Another Physicist Congressman Attempts to Revive the Office of Technology Assessment, Am. Inst. of Physics (Jan. 20, 2016), https://www.aip.org/fyi/2016/another-physicist-congressman-attempts-revive-office-technology-assessment [https://perma.cc/B73D-WUJL].

Courts, too, will prove invaluable as these technologies develop. In a world of "competing facts," courts reveal the absolute value of neutral arbiters, which are missing from the interactions between cops wearing body cameras and suspects; between Facebook users on the extremes of an issue; and between the U.S. government and those it places on "no fly" lists pursuant to machine learning algorithms.[66] Of course, courts do not generally choose the disputes that come before them, and their decisions are by definition backward-looking (though they have forward-looking implications).[67] Another approach includes self-regulation: Law enforcement actors in the Executive (and within states) could choose to self-regulate when they employ algorithms, as the Obama administration did for targeted killing and as New York City is contemplating for its automated decisions.[68] Finally, there obviously is a role for individuals, private lawyers, and nongovernmental organizations to engage in thoughtful self-help, as Adam Gershowitz's essay details in the policing and civil-justice context.[69] Grass-roots citizens' movements can work to persuade companies "that respecting and protecting their users' universally recognized human rights is in their long-term commercial self-interest."[70]

Our three branches of government have not yet engaged deeply on the difficult questions of how to shape the technologies that drive every aspect of our future. Understanding why that engagement has been slow opens up possibilities for addressing the underlying obstructions and deploying with purpose the alternative forms of constraint described here.

[66] Danielle Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1252 (2008).

[67] Glenn S. Gerstell, Gen. Couns., Nat'l Sec. Agency, Keynote Address to the American Bar Association 28th Annual Review of the Field of National Security Law Conference (Nov. 1, 2018) (transcript available at https://www.nsa.gov/news-features/speeches-testimonies/Article/1675727/keynote-address-by-glenn-s-gerstell-general-counsel-nsa-to-the-american-bar-ass/ [https://perma.cc/LK7N-YVGT]).

[68] Projects, NYC Mayor's Office of Operations, https://www1.nyc.gov/site/operations/projects/ads-task-force.page [https://perma.cc/74BJ-R2YT] (last visited Dec. 3, 2018).

[69] Adam Gershowitz, Criminal Justice Apps: A Modest Step Towards Democratizing the Criminal Process, 105 Va. L. Rev. Online 37 (2019).

[70] MacKinnon, supra note 18, at 175.