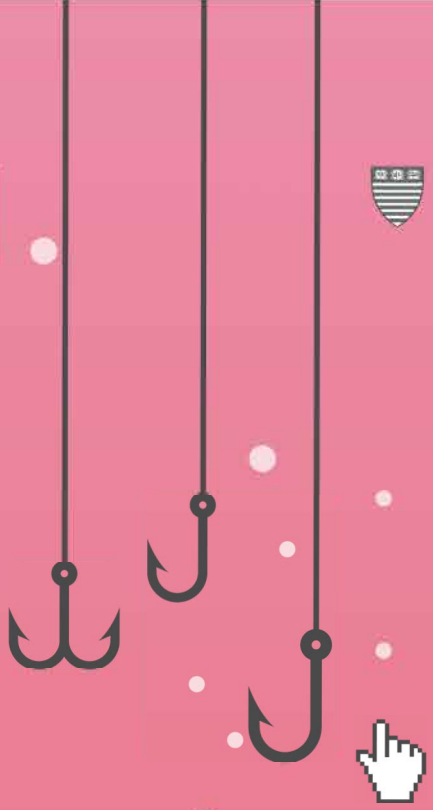
NEW AMERICA

PUBLIC INTEREST TECHNOLOGY

HARVARD Kennedy School
SHORENSTEIN CENTER
on Media, Politics and Public Policy



DIGITAL DECEIT II

A Policy Agenda to Fight Disinformation on the Internet

DIPAYAN GHOSH & BEN SCOTT

SEPTEMBER 2018

About the Author(s)

Dipayan Ghosh is the Pozen Fellow at the Shorenstein Center on Media, Politics and Public Policy at the Harvard Kennedy School, where he works on digital privacy, artificial intelligence, and civil rights. Ghosh previously worked on global privacy and public policy issues at Facebook, where he led strategic efforts to address privacy and security. Prior, Ghosh was a technology and economic policy advisor in the Obama White House. He served across the Office of Science & Technology Policy and the National Economic Council, where he worked on issues concerning big data's impact on consumer privacy and the digital economy. He also served as a fellow with the Public Interest Technology initiative and the Open Technology Institute at New America. Ghosh received a Ph.D. in electrical engineering & computer science at Cornell University.

Ben Scott is a Director of Policy & Advocacy at the Omidyar Network. He also serves on the management board of the Stiftung Neue Verantwortung, a technology policy think tank in Berlin. Previously, he was Senior Advisor at New America and its Open Technology Institute. During the first Obama administration, he was Policy Adviser for Innovation at the US Department of State where he worked at the intersection of technology and foreign policy. Prior to joining the State Department, he led the Washington Office for Free Press, a public interest organization focused on public education and policy advocacy in media and technology. Before joining Free Press, he worked as a legislative aide handling telecommunications policy for then-Rep. Bernie Sanders (I-Vt.) in the U.S. House of Representatives. He holds a Ph.D. in communications from the University of Illinois.

Acknowledgments

We would like to thank the Ford Foundation for its generous support of this work. The views expressed in this report are those of the authors and do not necessarily represent the views of the Ford Foundation, its officers, or employees. We would also like to thank the many people who helped us conceive and develop these ideas. In particular, we would like to thank Gene Kimmelman, Jim Kohlenberger, Karen Kornbluh, Rebecca MacKinnon, Nicco Mele, Tom Patterson, Victor Pickard, Daniel Solove, and Tom Wheeler for reviewing this paper. We would also like to thank Maria Elkin for providing communications support.

About the Shorenstein Center

The Shorenstein Center on Media, Politics and Public Policy is a Harvard University research center dedicated to exploring and illuminating the intersection of press, politics and public policy in theory and practice. The Center strives to bridge the gap between journalists and scholars, and between them and the public. Through teaching and research at the Kennedy School of Government and its program of visiting fellows, conferences and initiatives, the Center is at the forefront of its area of inquiry.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Public Interest Technology

New America's Public Interest Technology team connects technologists to public interest organizations. We aim to improve services to vulnerable communities and strengthen local organizations that serve them.

Contents

Executive Summary

The crisis for democracy posed by digital disinformation demands a new social contract for the internet rooted in transparency, privacy and competition. This is the conclusion we have reached through careful study of the problem of digital disinformation and reflection on potential solutions. This study builds off our first report—**Digital Deceit**—which presents an analysis of how the structure and logic of the tracking-and-targeting data economy undermines the integrity of political communications. In the intervening months, the situation has only worsened—confirming our earlier hypotheses—and underlined the need for a robust public policy agenda.

Digital media platforms did not cause the fractured and irrational politics that plague modern societies. But the economic logic of digital markets too often serves to compound social division by feeding pre-existing biases, affirming false beliefs, and fragmenting media audiences. The companies that control this market are among the most powerful and valuable the world has ever seen. We cannot expect them to regulate themselves. As a democratic society, we must intervene to steer the power and promise of technology to benefit the many rather than the few.

We have developed here a broad policy framework to address the digital threat to democracy, building upon basic principles to recommend a set of specific proposals.

Transparency: As citizens, we have the right to know who is trying to influence our political views and how they are doing it. We must have explicit disclosure about the operation of dominant digital media platforms -- including:

- Real-time and archived information about targeted political advertising;
- Clear accountability for the social impact of automated decision-making;
- Explicit indicators for the presence of non-human accounts in digital media.

Privacy: As individuals with the right to personal autonomy, we must be given more control over how our data is collected, used, and monetized -- especially when it comes to sensitive information that shapes political decision-making. A baseline data privacy law must include:

- Consumer control over data through stronger rights to access and removal;
- Transparency for the user of the full extent of data usage and meaningful consent;
- Stronger enforcement with resources and authority for agency rule-making.

Competition: As consumers, we must have meaningful options to find, send and receive information over digital media. The rise of dominant digital platforms demonstrates how market structure influences social and political outcomes. A new competition policy agenda should include:

- Stronger oversight of mergers and acquisitions;
- Antitrust reform including new enforcement regimes, levies, and essential services regulation;
- Robust data portability and interoperability between services.

There are no single-solution approaches to the problem of digital disinformation that are likely to change outcomes. Only a combination of public policies—all of which are necessary and none of which are sufficient by themselves—that truly address the nature of the business model underlying the internet will begin to show results over time. Despite the scope of the problem we face, there is reason for optimism. The Silicon Valley giants have begun to come to the table with policymakers and civil society leaders in an earnest attempt to take some responsibility. Most importantly, citizens are waking up to the reality that the incredible power of technology can change our lives for the better or for the worse. People are asking questions about whether constant engagement with digital media is healthy for democracy. Awareness and education are the first steps toward organizing and action to build a new social contract for digital democracy.

Introduction

The basic premise of the digital media economy is no secret. Consumers do not pay money for services. They pay in data—personal data that can be tracked, collected, and monetized by selling advertisers access to aggregated swathes of users who are targeted according to their demographic or behavioral characteristics.[1] It is personalized advertising dressed up as a tailored media service powered by the extraction and monetization of personal data.

This "tracking-and-targeting" data economy that trades personal privacy for services has long been criticized as exploitative.[2] But the bargain of the zero price proposition has always appeared to outweigh consumer distaste—and even public outrage—for the privacy implications of the business. That finally may be changing.

Public sentiment has shifted from concern over commercial data privacy—a world where third parties exploit consumer preferences—to what we might call "political data privacy," where third parties exploit ideological biases. The marketplace for targeting online political communications is not new. But the emergence of highly effective malicious actors and the apparent scale of their success in manipulating the American polity has triggered a crisis in confidence in the digital economy because of the threat posed to the integrity of our political system.[3] The specter of "fake news" and digital disinformation haunts our democracy. The public reaction to it may well produce a political momentum for regulating technology markets that has never before found traction.[4]

It is personalized advertising dressed up as a tailored media service powered by the extraction and monetization of personal data.

Since the 2016 presidential election in the United States, there has been a steady drumbeat of revelations about the ways in which the digital media marketplace—and its data driven business model—is compromising the integrity of liberal democracies.[5] The investigations into the prevalence of "fake news" pulled the curtain back on Russian information operations,[6] Cambridge Analytica's privacy-abusing data analytics services,[7] bot and troll armies for hire,[8] echo-chambers of extremist content,[9] and the gradual public realization that the economic logic of

digital media feeds these cancers. The spread of this disease is global and shows no sign of abating any time soon. And it remains unclear whether the industry's attempts thus far at engineering prophylactic cures will prove at all helpful.[10]

The central theme in these scandals is the power of the major digital media platforms to track, target, and segment people into audiences that are highly susceptible to manipulation. These companies have all profited enormously from this market structure, and they have done little to mitigate potential harms. Now that those harms appear to threaten the integrity of our political system, there is a crisis mentality and a call for reform.

Will this explosion of awareness and outrage over violations of "political data privacy" result in a new regulatory regime for the data economy? The positive news is that we have already seen some movement in this direction, most of which has been triggered by the immense level of public scrutiny and inquiry over social media's interaction with the agents of disinformation. In the few months since the Facebook-Cambridge Analytica revelations, we have watched the leading technology firms take up a number of new initiatives that it previously appeared they would never undertake. Among these new steps are, perhaps most notably, Facebook's introduction of its new political ad transparency regime.[11] But these changes have only been instituted because of the public's clamoring for them. Alone, they will never be enough to stave off the impact of disinformation operations. And if the historic decline in the Facebook and Twitter stock prices in the wake of these reforms proves any trend,[12] it only reveals that the priorities of Wall Street will continually reassert themselves with vigor.

Now that those harms appear to threaten the integrity of our political system, there is a crisis mentality and a call for reform.

We believe it is time to establish a new "digital social contract" that codifies digital rights into public law encompassing a set of regulations designed to foster open digital markets while protecting against clear public harms and supporting democratic values. The digital media platforms now dominate our information marketplace, in the process achieving a concentration of wealth and power unprecedented in modern times. As a democratic society, we must now intervene to ensure first order common interests come before monopoly rent-seeking—and to steer the power and promise of technology to benefit the many rather than the

few. The digital rights agenda should be architected around three simple principles:

- **Transparency:** As citizens, we have the right to know who is trying to influence our political views and how they are doing it. We must have explicit disclosure about the operation of the advertising and content curation processes on dominant digital media platforms, including the social impact of algorithms and the presence of non-human accounts.

- **Privacy:** As individuals with the right to personal autonomy, we must be given more control over how our data is collected, used, and monetized, especially when it comes to sensitive information that shapes political decision-making.

- **Competition**: As consumers, we must have meaningful options to find, send and receive information over digital media.

This report offers a framing analysis for each of these public service principles and proposes a policy agenda to shape future market development within a rights-based framework. We are focused on a set of policy changes designed to address the specific problem of disinformation. We accomplish this by proposing both practical regulations to address clear harms and structure reform of business practices that worsen the problem over time. We have been greatly encouraged during the research and writing of this essay to see similar conclusions appear in recent reports of thought-leading policymakers.[13] In our common project of protecting democracy, the question is less what is to be done and more how to do it. The ideas offered here are intended to identify the first practical steps on a longer path towards shaping the tremendous power of the internet to serve the public interest. The consequences of inaction threaten the integrity of our democracy itself.

Transparency

An important part of the disinformation problem is driven by the opacity of its operations and the asymmetry of knowledge between the platform and the user. The starting point for reform is to rein in the abuses of political advertising. Ad-driven disinformation flourishes because of the public's limited understanding of where paid political advertising comes from, who funds it, and most critically, how it is targeted at specific users. Even the moderately effective disclosure rules that apply to traditional media do not cover digital ads. It is time for the government to close this destructive loophole and shape a robust political ad transparency policy for digital media. These reforms should accompany a broader "platform transparency" agenda that includes revisiting the viability of the traditional "notice and consent" system in this era of trillion dollar companies, exposing non-human online accounts, and developing a regime of auditing for the social impact of algorithms that affect the lives of millions with automated decisions.

Political Ad Transparency

The lowest hanging fruit for policy change to address the current crisis in digital disinformation is to increase transparency in online political advertising. Currently, the law requires that broadcast, cable and satellite media channels that carry political advertising must ensure that a disclaimer appears on the ad that indicates who paid for it.[14] Online advertisements, although they represent an increasingly large percentage of political ad spending, do not carry this requirement. A 2014 Federal Election Commission decision on this issue concluded that the physical size of digital ads was simply too small for it to be feasible to add the disclaimer.[15] And even if they had applied the rule, it would only have applied to a narrow category of paid political communications. As a result, Americans have no ability to judge accurately who is trying to influence them with digital political advertising.

The effect of this loophole in the law is malignant to democracy. The information operation conducted by a group of Russian government operatives during the 2016 election cycle made extensive use of online advertising to target American voters with deceptive communications. According to Facebook's internal analysis, these communications reached 126 million Americans with a modicum of funding.[16] In response, the Department of Justice filed criminal charges against 13 Russians early this year.[17] If the law required greater transparency into the sources of political advertising and the labeling of paid political content, these illegal efforts to influence the U.S. election could have been spotted and eliminated before they could reach their intended audiences.

But the problem is much larger than nefarious foreign actors. There are many other players in this market seeking to leverage online advertising to disrupt and undermine the integrity of democratic discourse for many different reasons. The money spent by the Russian agents was a drop in the bucket of overall online political ad spending during the 2016 election cycle. The total online ad spending for political candidates alone in the 2016 cycle was $1.4 billion, up almost 800 percent from 2012, an amount roughly the same as that candidates spent on cable television ads (which do require funding disclosures).[18] The total amount of money spent on unreported political ads (e.g. issue ads sponsored by companies, unions, advocacy organizations, or PACs that do not mention a candidate or party) is quite possibly considerably higher. Only the companies that sold the ad space could calculate the true scope of the political digital influence market, because there is no public record of these ephemeral ad placements. We simply do not know how big the problem may be.

What we do know is that none of these ads carried the level of transparency necessary for voters to have a clear understanding of who sought to influence their views and for what reason. Many online ads actively seek to cloak their origins and strategic aims. They are typically targeted at select groups of users. And unlike targeting in the television market, these messages are not publicly available—they are only visible to the target audience in the moment of ad delivery and then they disappear. (The recent introduction of ad transparency databases from Facebook and Twitter have changed this, but for most users, their experience with political ads remains similar.) And they are published on digital platforms by the millions. The special features of digital advertising that make it so popular—algorithmic targeting and content customization—make it possible to test thousands of different ad variations per day with thousands upon thousands of different configurations of audience demographics.[19] Political advertisers can very easily send very different (and even contradictory) messages to different audiences. Until very recently, they need not have feared exposure and consequent public embarrassment.

Because of these unique targeting features, the consequences of opacity in digital ads are far worse than traditional media channels. For that reason, the objective of policy reform to increase transparency in online political advertising must seek to move beyond simply achieving equality between the regulation of traditional and new media channels. Online ads require a higher standard in order to achieve the same level of public transparency and disclosure about the origins and aims of advertisers that seek to influence democratic processes. We should aim not for regulatory parity but for outcome parity.

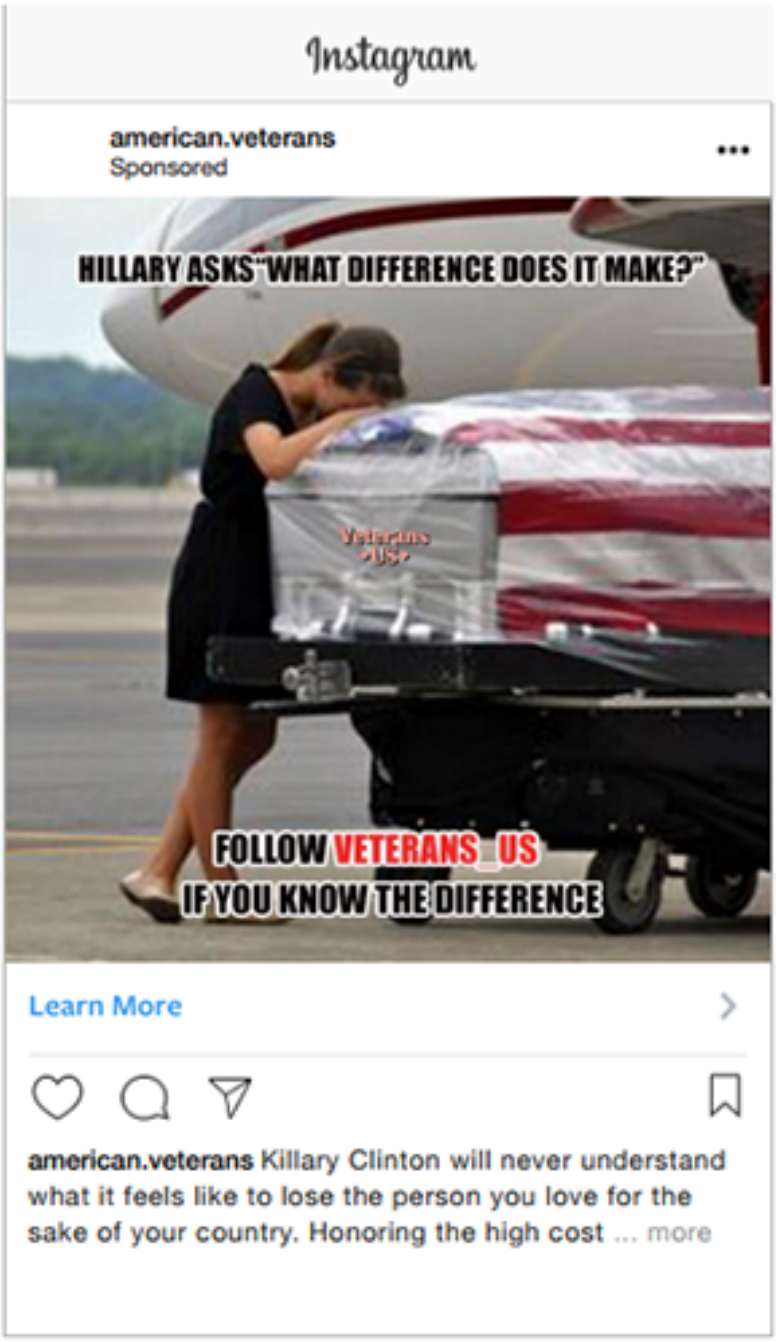
→ EXAMPLES OF RUSSIAN DISINFORMATION ON FACEBOOK AND INSTAGRAM IN THE LEAD-UP TO THE 2016 PRESIDENTIAL ELECTION

These ads were among those **released by** the House Intelligence Committee in November 2017.

Posted on: LBGT United group on Facebook
Created: March 2016
Targeted: People ages 18 to 65+ in the United States who like "LGBT United"
Results: 848 impressions, 54 clicks
Ad spend: 111.49 rubles ($1.92)

Posted on: Instagram
Created: April 2016
Targeted: People ages 13 to 65+ who are interested in the tea party or Donald Trump
Results: 108,433 impressions, 857 clicks
Ad spend: 17,306 rubles ($297)

Posted on: Facebook
Created: October 2016
Targeted: People age 18 to 65+ interested in Christianity, Jesus, God, Ron Paul and media personalities such as Laura Ingraham, Rush Limbaugh, Bill O'Reilly and Mike Savage, among other topics
Results: 71 impressions, 14 clicks
Ad spend: 64 rubles ($1.10)



Posted on: Instagram
Created: August 2016
Targeted: People ages 18 to 65+ interested in military veterans, including those from the Iraq, Afghanistan and Vietnam wars
Results: 17,654 impressions, 517 clicks
Ad spend: (3,083 rubles) $53

We applaud the efforts of congressional leaders to move a bipartisan bill—the Honest Ads Act—that would represent significant progress on this issue.[20] And we are glad to see that public pressure has reversed the initial opposition of technology companies to this legislative reform. The significant steps that Google,[21] Facebook,[22] and Twitter[23] have pledged to take in the way of self-regulation to disclose more information about advertising are important corporate policy changes. However, these efforts should be backstopped with clear rules and brought to their full potential through enforcement actions in cases of noncompliance.

Even then, the combination of self-regulation and current legislative proposals doesn't go far enough to contain the problem. None of the major platforms' transparency products -- Facebook Ad Archive, [24] Google's Political Ad Transparency Report, and Twitter's Ad Transparency Center[25] -- make available make available the full context of targeting parameters that resulted in a particular ad reaching a particular user. Google and Twitter limit transparency to a very narrow category of political ads, and both offer far less information than Facebook (though you must be logged into a Facebook account to see the Facebook data). None of this transparency is available in any market other than the United States (with the exception of Brazil, where Facebook recently implemented the ad transparency center in advance of October 2018 elections). The appearance of these ad transparency products signals an important step forward for the companies, but it also exposes the gap between what we have and what we need.

There are various methods we might use to achieve an optimal outcome for ad transparency. In our view, the ideal solution should feature five components. These are drawn from our own analysis and favorable readings of ideas suggested by various commentators and experts,[26] as well as the strong foundation of the bipartisan Honest Ads Act.

- **Clear On-Screen Designation:** All political ads that appear in social media streams should be clearly marked with a consistent designation, such as a bright red box that is labeled "Political Ad" in bold white text, or bold red text in the subtitle of a video ad. Further, there should be strict size requirements on these disclosures, for instance that they should occupy at least five to ten percent of the space of the advertisement. Too often in digital media streams, the markings on paid content are so unobtrusive that users may overlook the designation.
- **Real-Time Disclosure in the Ad**: Clear information about the ad should be pushed to the user in the payload of the ad at the same time that the ad renders (e.g. a pop-up box triggered on cursor hovers for textual and image ads, or subtitle text for video ads). It is not enough for this information to be available somewhere else on the internet, or to require

active click-through to enable access to this information. The following data points should be included:

    - *Sponsor of the ad*: The name of the organization that paid to place the ad, the total amount it spent to place the ad, and a list of its disclosed donors;
    - *Time and audience targeting parameters*: The time period over which the ad is running, the demographic characteristics selected by the advertiser for targeting of the ad, the organization whose custom target list the recipient belongs in (if applicable), and the demographic characteristics that indicate why the recipient was included in the target list (including platform-determined "look-alike" ascriptions, if applicable);
    - *Engagement metrics*: The number of user impressions for which the ad buyer has paid to reach with the present ad, and the number of active engagements by users.

- **Open API to Download Ad Data:** All of the information in the real-time disclosure for each ad should be compiled and stored by digital advertising platforms in machine readable, searchable databases available through an open application programming interface (API). If the ad mentions a candidate, political party, ballot measure or clear electoral issue, that should be logged. In addition, this database should include the complete figures on engagement metrics, including the total number of user engagements and the total number of ad impressions (paid and unpaid). This data should be available online for public review at all times and for all advertisers over a low minimum threshold of total ad spending per year.
- **Financial Accountability:** Donors for political ad spending over a minimum threshold should be reported by advertisers to election authorities, listing the provenance of funds as a form of campaign finance —including the major donors. Political advertisers should be required by advertising platforms to submit evidence of this reporting prior to a second political ad buy.
- **Advertiser Verification:** Election authorities should impose "know your customer" rules that require digital ad platforms that cross a minimum level of ad spending to verify the identity of political advertisers and take all reasonable measures to prevent foreign nationals from attempting to influence elections.

An Ideal Digital Ad

Underneath all of these provisions, we need to take care to get the definitions right and to recognize the scale and complexity of the digital ad market compared to traditional media. Current transparency rules governing political ads are triggered under limited circumstances—in particular, those that mention a candidate or political party and that are transmitted within a certain time period prior to the election. These limits must be abandoned (or dramatically reconsidered) in recognition of the scope and complexity of paid digital communications, the prevalence of the issue ad versus a candidate ad,[27] and the nature of the permanent campaign that characterizes contemporary American politics. If these are the parameters, it becomes clear why all ads must be captured in a searchable, machine-readable database with an API that is accessible to researchers and journalists that have a public service mission to make sense of the influence business on digital media.

The Honest Ads Act would achieve some of these objectives.[28] The proposed legislation extends current laws requiring disclaimers on political advertising in traditional media to include digital advertising. It requires a machine readable database of digital ads that includes the content of the ad, description of the audience (targeting parameters), rate charged for the ad, name of candidate, office, or election issue mentioned in the ad and contact information of the person that bought the ad. And it requires all advertising channels (including digital) to take all reasonable efforts to prevent foreign nationals from attempting to influence elections. Even FEC bureaucrats may get in on the action with their (admittedly tepid) proposed rules to govern digital ad disclaimers.[29]

As public pressure builds in the run up to the 2018 elections, we may well see additional measures piled onto this list. Notably, a recent British Parliamentary report calls for a ban on micro-targeting political ads using Facebook's "lookalike" audiences, as well as a minimum number of individuals that all political ads must reach.[30]

The combination of self-regulation and current legislative proposals does not go far enough to contain the problem.

We favor a system that would push this kind of disclosure for political ads as quickly as possible to guard fast-approaching elections against exploitation. We acknowledge that defining "political" will always carry controversy. However, Facebook's current definition—"*Relates to any national legislative issue of public importance in any place where the ad is being run*"—is a good start.[31] They offer a list of issues[32] covered under this umbrella (though only for the United States at present). These categories could be a lot more difficult to maintain globally and over a long period of time. Consequently, we expect these measures will ultimately be extended to all ads, regardless of topic or target. This will also result in a cleaner policy for companies that do not have the resources that Facebook can bring to the problem.

But even in the potential future world of a total ad transparency policy, a method of flagging which ads fall into the category of political communications would be preferred in order to signal that voters should pay attention to the origin and aims of those ads in particular. Of course, we are mindful of the significant constitutional questions raised by these kinds of disclosure requirements. We

welcome that discussion as a means to hone the policy to the most precise tool for serving the public interest without unduly limiting individual freedoms. A full analysis of First Amendment jurisprudence is beyond the scope of this report, but we believe proposals like this will withstand judicial scrutiny.

Getting political ad transparency right in American law is not only a critical domestic priority, it is one that has global implications, because the leading internet companies will wish to extend whatever policies are applied here happens here to the rest of the world so as to maintain platform consistency. This is an incentive to get the "gold standard" right, particularly under American law that holds a high bar of protection for free expression. But it also raises questions about how we might anticipate problems that might arise in the international context. For example, there is a strong argument that advertisers that promote controversial social or political issues at a low level of total spending (indicating civic activism rather than an organized political operation) should be shielded from total transparency in order to protect them from persecution. We could contemplate a safe-harbor for certain kinds of low-spending advertisers, particularly individuals, in order to balance privacy rights against the public interest goals of transparency.

Our view is that online ad transparency is a necessary but far from sufficient condition for addressing the current crisis in digital disinformation. Transparency is only a partial solution, and we should not overstate what it can accomplish on its own. But we should try to maximize its impact by requiring transparency to be overt and real-time rather than filed in a database sometime after the fact. To put it simply, if all we get is a database of ad information somewhere on the internet that few voters ever have cause or interest to access, then we have failed. We strongly believe contextual notification is necessary—disclosure that is embedded in the ad itself that goes beyond basic labelling. And this message must include the targeting selectors that explain to the user why she got the ad. This is the digital equivalent of the now ubiquitous candidate voice-over, "I approved this ad." Armed with this data, voters will have a signal to pay critical attention, and they will have a chance to judge the origins, aims, and relevance of the ad.

Platform Transparency

Building on the principle that increased transparency translates directly into citizen and consumer empowerment, we believe a number of other proposals are worthy of serious consideration in this field. These include exposing the presence of automated accounts on digital media, developing systems to audit the social impact of algorithmic decision-making that affects the public interest, and reforming the "notice and consent" regime in terms of service that rely on the dubious assumption that consumers have understood (or have a choice in) what they have agreed to.

First, we find the so-called "Blade Runner" law a compelling idea (and not just a clever title).[33] This measure would prohibit automated channels in digital media (including Twitter handles) from presenting themselves as human users to other readers or audiences. In effect, bots would have to be labelled as bots—either by the users that create them or by the platform that hosts the accounts. A bill with this intent has been moving in the California legislature.[34] There are different ways to do this, including through a regime that applies a less onerous restriction on accounts that are human-operated but which communicate based on a transparent but automated time-table.

The Blade Runner law would give digital media audiences a much clearer picture of how many automated accounts populate online media platforms and begin to shift the norms of consumption towards more trusted content. Such transparency measures would not necessarily stigmatize all automated content. Clearly labelled bots that provide a useful service (such as a journalistic organization tweeting out breaking news alerts or a weather service indicating that a storm is approaching) would be recognized and accepted for what they are. But the nefarious activities of bot armies posing as humans would be undermined and probably these efforts would shift to some other tactic as efficacy declined. We are sensitive to the critique of this proposal as chilling to certain kinds of free expression that rely on automation. We would suggest ways that users can whitelist certain kinds of automated traffic on an opt-in basis. But the overall public benefit of transparency to defend against bot-driven media is clear and desirable.

The Blade Runner law would give digital media audiences a much clearer picture of how many automated accounts populate online media platforms and begin to shift the norms of consumption towards more trusted content.

Second, we see the increasing importance of establishing new systems for social impact oversight or auditing of algorithmic decision-making. The increasing prominence of AI and machine learning algorithms in the tracking-and-targeting data economy has raised alarm bells in the research community, in certain parts of industry, and among policymakers.[35] These technologies have enormous potential for good, including applications for healthcare diagnostics, reducing

greenhouse gas emissions, and improving transportation safety. But they may also cause and perpetuate serious public interest harms by reinforcing social inequalities, polarizing an already divisive political culture, and stigmatizing already marginalized minority communities.

It is therefore critical to apply independent auditing to automated decision-making systems that have the potential for high social impact. The research community has already begun to develop such frameworks.[36] These are particularly urgent for public sector uses of AI—not an inconsiderable practice given U.S. government R&D spending and activity.[37] And there are a few preliminary regulatory approaches to overseeing the private sector worth watching—including the GDPR provision that gives users the right to opt out of decision-making that is driven solely by automated methods.[38] These new oversight techniques would be designed to evaluate how and whether automated decisions infringe on existing rights, or should be subject to existing anti-discrimination or anti-competitive practices laws.

The idea of independent review of algorithmic social impact is not a radical proposal. There are clear precedents in U.S. oversight of large technology companies. In the FTC's consent order settled with Facebook in 2011, the agency required that Facebook submit to external auditing of its privacy policies and practices to ensure compliance with the agreement. In light of recent events that have revealed major privacy policy scandals at Facebook in spite of this oversight, many have rightly criticized the third-party audits of Facebook as ineffective. But one failure is not a reason to abandon the regulatory tool altogether; it should instead serve as an invitation to strengthen it.

Consider the possibility of a team of expert auditors (which might include at least one specialist from a federal regulatory agency working alongside contractors) regularly reviewing advanced algorithmic technologies deployed by companies that have substantial bearing on public interest outcomes. The idea here is not a simple code review; that can rarely provide much insight in the complexity of AI.[39] Rather, this type of audit should be designed with considerably more rigor, examining data used to train those algorithms and the potential for bias in the assumptions and analogies they draw upon. This would permit auditors to run controlled experiments over time to determine if the commercial algorithms subject to their review are producing unintended consequences that harm the public. These kinds of ideas are new and untested—but once upon a time, so too were the wild-eyed notions of independent testing of pharmaceuticals and the random inspection of food safety. Industry and civil society have already begun to work together in projects like the Partnership on AI to identify standards around fairness, transparency and accountability.[40]

One failure is not a reason to abandon the regulatory tool altogether; it should instead serve as an invitation to strengthen it.

Finally, as we begin to consider new rules for digital ad transparency, we should take the opportunity to revisit the larger questions about transparency between consumers and digital service providers. Our entire system of market information—which was never particularly good at keeping consumers meaningfully informed in comparison with service providers—is on the brink of total failure. As we move deeper into the age of AI and machine learning, this situation is going to get worse. The entire concept of "notice and consent" – the notion that a digital platform can tell consumers about what personal data will be collected and monetized and then receive affirmative approval—is rapidly breaking down. The intransparency in how consumer data collection informs targeted advertising, how automated accounts proliferate on digital media platforms, and how large-scale automated decisions can result in consumer harm are just the most prominent examples. As we move to tackle these urgent problems, we should be fully aware that we are addressing only one piece of a much larger puzzle. But it is a start.

Privacy

The disinformation problem is powered by the ubiquitous collection and use of sensitive personal data online. Data feeds the machine learning algorithms that create sophisticated behavioral profiles on the individual, predict consumer and political preferences, and segment the body politic into like-minded audiences. These analytics are then accessed by or sold to advertisers that target tailored political messaging at those audience segments—also known as filter bubbles—in ways used to trigger an emotional response and which drive polarization, social division, and a separation from facts and reason. Under current U.S. rules and regulations, anything goes in this arena. The starting point to contain this problem is to pop the filter bubbles. This can be done by increasing user privacy and individual control over data in ways that blunt the precision of audience segmentation and targeted communications. Current privacy law is insufficient to the task. To build a new regime, we can start by taking lessons from Obama-era legislative proposals, recent progress in the California legislature, and Europe's current regulatory framework for data protection.

The connection between privacy and the problem of disinformation in our digital information system sits at the core of the business of the digital platforms. The platforms are designed to extract as much personal information as possible from users in order to optimize the curation of organic content and the targeting of ads. The less privacy a user has from the platform, the more precisely the algorithms can target content. If that content is malignant, manipulative or merely optimized to confirm pre-existing biases, the effect (however unintended) is one that distances consumers from facts and fragments audiences into political echo chambers by feeding them more and more of the content that the algorithm predicts they prefer based on the data.

How does this work? The tracking-and-targeting data economy is based on two interrelated commodities—individual data and aggregated human attention. Companies offer popular, well-engineered products at a monetary price of zero. They log user-generated data, track user behavior on the site, mine the relationships and interactions among users, gather data on what their users do across the internet and physical world, and finally, combine it all to generate and maintain individual behavioral profiles. Each user is typically assigned a persistent identifier that allows all data collected across multiple channels, devices, and time periods to be recorded into an ever more sophisticated dossier.

Companies use these data profiles as training data for algorithms that do two things: curate content for that user that is customized to hold their attention on the platform, and sell access to profiling analytics that enable advertisers to target specific messages tailored precisely for segmented user audiences that are

likeliest to engage. These curation and targeting algorithms feed on one another to grow ever smarter over time—particularly with the forward integration of advanced algorithmic technologies, including AI. The most successful of the platform companies are natural monopolies in this space; the more data they collect, the more effective their services, the more money they make, the more customers they acquire, and the more difficult it is for competitors to emerge.

The starting point to contain this problem is to pop the filter bubbles.

Meanwhile, most users have very little visibility into or understanding of the nature of the data-for-service transactional quality of the consumer internet, or for the breathtaking scope of the tracking-and-targeting economy. A 2015 Pew survey reported that 47 percent of Americans polled said they were not confident they understood how their data might be used, and that "many of these people felt confused, discouraged or impatient when trying to make decisions about sharing their personal information with companies."[41] And even if they do become aware of the asymmetry of information between buyers and sellers, once the market power plateau is reached with an essential service (such as internet search or social networking), there is little in the way of meaningful consumer choice to provide any competitive pressure.

Perhaps this lack of awareness is responsible for the persistent lack of public demand for meaningful privacy regulation in the United States. Anecdotal accounts suggest that many consumers seem not to care about protecting their privacy. At the same time, though, we know from the fallout of the Cambridge Analytica incident and prior academic studies that consumers do in fact place some value on the privacy of their information.[42] Perhaps the lesson to draw from this is that people typically don't care about their privacy until and unless they have experienced a harm from the unauthorized access or use of their personal information. Or, more simply, they care, but they are resigned to the fact that they have no real control over how their data is used if they want to continue to have essential services. This explains the fact that, even in the aftermath of the Cambridge Analytica incident, the #DeleteFacebook movement has apparently proved inconsequential.[43]

It is not only Facebook, Google, Twitter, and other internet companies that engage or plan to engage in tracking and targeting practices. So do the owners of physical networks—known as broadband internet access service (BIAS)

providers. BIAS providers, situated as the consumer's route to the internet as they are, necessarily gain access to a universe of sensitive personal data including any internet domains and unencrypted URLs the consumer may have visited—which can readily be used to infer the consumer's interests and preferences.[44] These firms, the wireline leaders among them in United States being AT&T, Comcast, and Verizon, enjoy tremendous market power in the regions in which they operate. Meanwhile, they are increasingly investing in the digital advertising ecosystem because they see synergies between their data collection practices and the core resources needed to succeed in digital advertising.

People typically don't care about their privacy until and unless they have experienced a harm from the unauthorized access or use of their personal information.

Comcast, for example, owns subsidiaries Freewheel, an industry-standard video ad management platform, and Comcast Spotlight, which enables advertising clients to place targeted digital advertisements. Meanwhile, Verizon owns Oath, which may possess the most sophisticated full-service digital advertising technology stack outside of Google and Facebook. Each also owns significant consumer media properties—for instance, NBC, Telemundo, and Universal Pictures; and AOL, Yahoo!, and HuffPost respectively. And of course, both Verizon and Comcast serve as BIAS providers as well, possessing regional market power in providing internet service throughout the United States.

This is a dangerous vertical integration; it allows these corporations to provide consumers internet service, maintain large stores of consumer data in-house, generate behavioral profiles on consumers using that data, provide them with digital content over their television networks and internet media properties, and target ads at them over those digital platforms. And because these firms are not compelled to reveal their management practices concerning consumer data, it is difficult for the public to know if and how they use broadband subscribers' web browsing and activity data in the advertising ecosystem. But under current FCC regulations, there alarmingly are few restrictions if any against its use. To resolve this glaring problem, the Obama FCC promulgated rules that would have established data privacy regulations on BIAS providers for the first time—recognizing the potential harms of a network operator leveraging total access to internet communications in and out of a household in order to collect and

monetize data. Unfortunately, Congress nullified these rules soon after Trump took office, leaving consumers with no protection against potential abuses.[45]

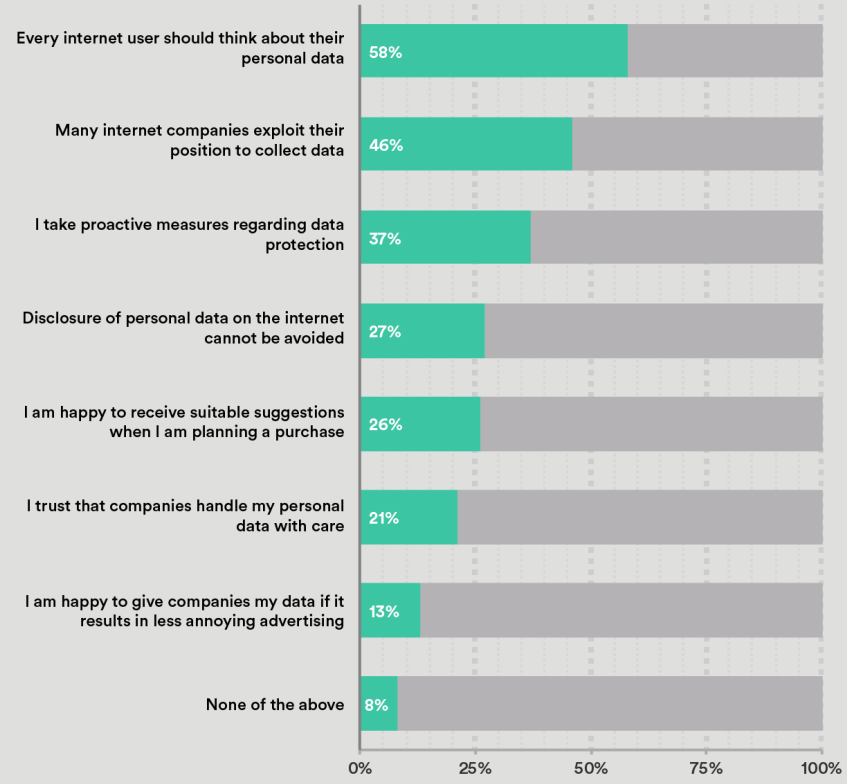
The tracking-and-targeting regime pursued by these industries results in a persistent commercial tension that pits the profits of an oligopoly of network owners and internet companies against the privacy interests of the individual. Without the oversight of regulators, the consumer has no chance in this contest. The appropriate policy response to contain and redress the negative externalities of the data tracking-and-targeting business must begin with an earnest treatment of privacy policy. But the U.S. government currently possesses no clear way of placing checks on the business practices relating to personal data. While narrow, sectoral laws exist for particular practices—among them, the Children's Online Privacy Protection Act (COPPA), the Electronic Communications Privacy Act (ECPA), the Gramm-Leach-Bliley Act (GLBA), and the Health Information Portability and Accountability Act (HIPAA)—none of these independently or collectively address the harms (including political disinformation) wrought by the internet's core tracking-and-targeting economy.

Without the oversight of regulators, the consumer has no chance.

Internet companies and broadband network operators exist under a regulatory regime that is largely overseen at the national level by the Federal Trade Commission (FTC). Industry commitments to consumers are enforced principally through Section 5 of the Federal Trade Commission Act of 1914, which prohibits "unfair or deceptive acts or practices."[46] This regime allows the FTC to hold companies accountable to voluntary policy commitments—including privacy policies, terms of service and public statements—that they make to their users. So if a firm chooses to be silent about certain practices, or proactively says in fine text that it reserves the right to sell all of the subject's data to the highest bidder, then it has, in effect, made it extraordinarily difficult for the FTC to bring an enforcement action against it for those practices since it could be argued that the firm has not deceived the consumer.[47]

The additional fact that the FTC largely lacks the ability to promulgate new regulations from fundamental principles—known as "rulemaking authority"—suggests that consumers face a losing battle against industry practices.

Share of Internet Users in U.S. Who Agree With Selected Statements About Online and Data Privacy as of May 2017



Source: *Statista*, https://www.statista.com/statistics/713869/us-internet-user-opinion-digital-privacy/

NEW AMERICA

The FTC is only empowered to punish firms for past abuses under Section 5, including failures to comply with voluntary commitments—producing a light-touch regime that cannot proactively protect consumers. The outcome is that the industries that fall under its jurisdiction—including internet firms and the broader digital advertising ecosystem—are for the most part responsible for policing themselves.

The resulting self-regulatory mode of regulation established by the internet and digital advertising industries companies in consultation with other stakeholders is relatively favorable to the industry—providing it the leverage to negotiate policies on its own terms. Industry experts can essentially define the terms of frameworks like the Network Advertising Initiative's Self-Regulatory Code of Conduct, and while stakeholders including government and consumer advocates

can attempt to influence the terms of such codes, there is nothing compelling the industry to listen.[48] This is in part why we now have a digital ecosystem in which personal data is largely out of the person's control and rather in the corporation's. This is not to say that the FTC staff and commissioners do not act earnestly, but rather that the agency as a whole requires far greater resources and authority to effectively protect consumers of the firms for which the FTC is the principal regulator, including internet-based services.

Industries that fall under the FTC's jurisdiction are for the most part responsible for policing themselves.

It is worth noting that on occasion, an FTC with political will can find ways to corner companies that have made major missteps that deviate from the privacy guarantees made to consumers in the terms of service. The FTC intervenes to discipline companies by compelling them to agree to broad public-interest settlements called consent orders. Facebook, Snapchat, and Google have all entered such arrangements with the agency. These consent orders typically require that the firm follow certain stipulated practices to the letter, and keep agency staff informed of their compliance with those requirements.

Notably, though, the FTC lacks the resources to hold the companies that are under consent orders accountable, or to develop consent orders with all bad actors. For instance, in the case of Facebook, which was compelled by a 2011 FTC consent order to have its privacy practices externally audited by PricewaterhouseCoopers, the auditors missed for years the fact that those with access to Facebook's developer platform could siphon social graph data from an entire friend network just by persuading a single user to agree to the terms of the application.[49] PricewaterhouseCoopers found nothing wrong, even in its 2017 report, despite the December 2015 reports about the connections between Cambridge Analytica and Sen. Ted Cruz.

The current system is broken. What we need now is a completely new legal framework that establishes a baseline privacy law.

The Legacy of the Obama Administration's Efforts

As we consider how to structure an American baseline privacy law to treat problems like filter-bubble-driven political disinformation, policymakers need not start from zero. There have been several attempts to legislate baseline commercial privacy in the past, the most comprehensive of which was the "Consumer Privacy Bill of Rights" discussion draft published by the Obama administration in early 2015.[50]

Throughout President Barack Obama's first term, the technology industry made exciting predictions about the potential of applying sophisticated algorithms to the processing of big data to generate new economic growth. Vast sums of investment capital poured into the markets to develop new tools and create new firms. Very little industry attention was paid to the privacy implications of this data gold rush. The Obama administration accordingly predicted that the industry's trend toward more expansive data collection meant that a baseline privacy law—legislation that could apply across industries and to most kinds of personal data collected by companies—was necessary to protect consumer privacy in the future.

What we need now is a completely new legal framework that establishes a baseline privacy law.

In 2015, the Obama White House and U.S. Department of Commerce jointly developed and released a legislative proposal that put forth a comprehensive approach to regulating privacy called the Consumer Privacy Bill of Rights Act of 2015. It was informed by more than two years of market research and policy analysis, and amplified by the public outcry over data privacy that accompanied the Snowden revelations in 2013. The wide-ranging proposal attempted to encapsulate the key lessons—including from a corresponding 2012 report titled the Consumer Privacy Bill of Rights, as well as policy efforts that came before like the Clinton administration's Electronic Privacy Bill of Rights and various European approaches—into a legislative draft that the U.S. Congress could take forward.[51]

The hope was that Congress could work atop the legislative language shared by the White House and send revised language back to the President's desk. But the

draft got very little traction. With the proposal opposed by industry as too regulatory and by privacy advocates as too permissive, Congress never attempted to legislate.

Looking back now, it appears the Consumer Privacy Bill of Rights Act of 2015 was ahead of its time. We begin our analysis by revisiting these ideas in light of today's market context and newfound political will.

Control

The clear and persistent public harms resulting from the tracking and targeting data economy make quite clear that consumers have lost meaningful control over how their data is collected, shared, sold, and used. Therefore, the starting point for new digital privacy regulations must be the ability for consumers to control how data collected by service providers is used, shared and sold. The ideas expressed in the proposed Consumer Privacy Bill of Rights Act represent a good starting point for deliberation in the way forward.

First and foremost is the proposed bill's definition of personal data. It sets the boundaries for what kinds of information pertaining to the individual is protected under the bill. The discussion draft takes a broad approach and includes the individual's name, contact information, and unique persistent identifiers, but also "any data that are collected, created, processed, used, disclosed, stored, or otherwise maintained and linked, or as a practical matter linkable by the covered entity, to any of the foregoing."

Atop this framework, the draft proposes commanding and expansive rights for the consumer. Data collectors "shall provide individuals with reasonable means to control the processing of personal data about them in proportion to the privacy risk to the individual and consistent with context." Additionally, consumers would be afforded the capacity for easy access to control their data in ways that the data collector would have to to clearly explain. Consumers would also have the right to withdraw consent at any time. These elements should be part of future legislative and regulatory frameworks.

With these elements in place—a broad definition of personal data, and an affordance of consumer control over what data is collected and how it is used to a degree adjusted for various commercial contexts—the effectiveness of online disinformation operations could be substantially reduced. This is because these new protections would immediately blunt the precision of targeting algorithms as service providers would be permitted to store and apply only the information that the individual elects can be used. It would also begin to put limits on the now ubiquitous data gathering practices in the industry that too often result in non-purpose specific collection and data leakage to ill-intended actors.

What do internet companies and ISPs know about me?

Location

Companies in the digital sector can know your location in real time through a number of means including through direct or indirect access to cell tower triangulation information, SIM-based radio measurements, address-specific GPS data, or Wi-Fi positioning data. Compiled over time, precise historical location data can reveal an individual's behaviors, preferences and beliefs.

Search history

An individual's search history is gathered by internet search providers like Google, Bing and Yahoo. Search history reveals a user's intent -- industry lingo for your propensity to make a purchase or be convinced by an idea -- better than any other source of information.

Browsing history

Web browsing history is accessible to firms that provide browsers like Google (Chrome), Microsoft (Internet Explorer and Edge), Mozilla (Firefox), and Apple (Safari). It is also available to internet service providers like AT&T and Sprint, which can access unencrypted data downloaded by a subscriber, as well as a list of domains visited even if downloaded data is encrypted. Like search history, browsing history can be used to infer one's behaviors, preferences and beliefs.

App use

Internet companies and cellular network providers -- not to mention mobile operating systems like iOS and Android themselves -- often monitor which apps you use on your smartphone. They may be able to access this information by monitoring plug-ins you enable for their services, studying internet connections you make over your phone, or through engaging in general OS management.

Email tracking

Commercial email providers often monitor the metadata and content of the emails sent and received so that they can know who you're communicating with, what you're saying, and what you're reading. This analysis can reveal your relationship network as well as your interests and preferences. Additionally, entities that send you emails might insert email cookies into the email, which can be used to signal to them whether and when you opened the email they sent you.

Behavioral profiles

Underlying the collection of raw data is the ongoing compilation of a behavioral tracking profile on you by many different kinds of firms, whether ISPs, internet companies, data brokers, or others. They typically use persistent identifiers to track you across platforms and devices, amalgamating any and all data of interest into your profile so as to maintain a real-time repository with which your up-to-date interests, preferences, beliefs can behaviors can be inferred, usually for forward commercial use.

NEW AMERICA

Trust and transparency in data use

The tracking-and-targeting data economy has gone off the rails in large part because it operates out of sight of the consumer. No Facebook user would have knowingly consented to have their data shipped to Cambridge Analytica or to sell access to their profile to target ads sent by foreign agents to disrupt elections. Because the problem of distortion in our political culture is exacerbated by the scale of data collection that shape filter bubbles in digital media, the damage can be limited by instituting the requirement that data be used only for transparent and agreed-upon purposes as specified with the individual. There is no reason to deny the individual consumer full knowledge of why and how data is collected, particularly when it can so readily be used to abet the goals of nefarious actors. But the problem remains that they are simply unaware of how their data is used, and there is little they can do about that.

The Consumer Privacy Bill of Rights attempted to solve for exactly this predicament by requiring that companies be transparent with users about what kinds of data they collect and how they use it. This was accomplished in the legislative draft through clever implementation of two core concepts that have long been central to protective privacy policymaking: purpose specification and use limitation.

Purpose specification—the general concept that before an individual's data is collected, the data-collecting entity (say, a BIAS provider)—should inform the individual (in this case, a subscriber to broadband services) of what data is collected and why it is collected. For instance, a BIAS provider needs to maintain data on the subscriber's identity and internet protocol (IP) address; the provider also needs to receive and transmit the subscriber's input signals as well as the information routed back to the subscriber after server calls—in other words, the subscriber's broadband activity data. This information is needed by the BIAS provider so that it can serve the subscriber with broadband internet services. A BIAS provider that properly engages in purpose specification will note to the subscriber the data streams it will collect to provide broadband services; commit to the subscriber not to use the data for any other purpose; and enforce that policy with rigor, or risk facing regulatory enforcement should it fail to do so.

There is no reason to deny the individual consumer full knowledge of why and how data is collected.

Use limitation, meanwhile, is the idea that data collected on the individual will not be utilized by the data-collecting entity outside the realm of reasonability. Extrapolating the example of the BIAS provider, it is more than reasonable to expect that they will need to take the user's input data (say, the subscriber's navigation to the URL "www.reddit.com") in order to feed the subscriber that data over the broadband connection. But perhaps less reasonable, at least considering the average subscriber's expectations, would be the forward use of that sensitive broadband activity data—including URLs visited and time spent exploring different domains—to infer the subscriber's behavioral patterns and consumer preferences to inform digital ad-targeting. This is the sentiment captured in the principle of use limitation: that the data-collecting entity will refrain from using the subject's data for any reason outside of providing that subject with a technically functional service offered to the degree and level of service expected by the user. Stated differently, a policy regime that upholds use limitation as a priority should use the minimum amount of personal data required to uphold the technical functionality of its service.

These two principles—purpose specification and use limitation—are regularly overlooked by the leading internet firms. This negligence has eroded the public's trust over time. Restoring them to the core of a new set of consumer privacy rights will limit many of the harms we see today at the intersection of data privacy and disinformation. For example, applied effectively, these rights would restrict the practices of invisible audience segmentation and content-routing that are exploited by disinformation operators. These rules would apply not only to the internet companies; but also to the data broker industry, which exists primarily to hoover up data from such sources as credit agencies, carmakers and brick-and-mortar retailers in order to apply that data for purposes unrelated to those for which it was given.

Drawing Lessons from the European Approach

The European Union, over the past several years, has developed its General Data Protection Regulation (GDPR), a broad set of new laws that applies restrictions to the general collection and use of personal data in commercial contexts. The much-anticipated regulatory framework went into effect on May 25, 2018. The regulation, which is technically enforced by the data protection authorities in each of the 28 member states of the European Union, includes novel and stringent limitations that will likely force significant changes to the operations of the major internet firms that serve European consumers. Many of its provisions mark important building blocks for any future American privacy law. Indeed, many were transposed into the newly passed data privacy law in California, which will go into effect in 2020.[52] Further, the principles of purpose specification and use limitation encapsulated in the Consumer Privacy Bill of Rights come to life vividly in the GDPR.

While the present industry landscape has encouraged an information asymmetry, the GDPR will offer consumers more power in the face of powerful internet companies. Among the GDPR's constraints are the following.

- **Consent and control**: The GDPR requires that consent to data collection and use must be "freely given, specific, informed and unambiguous." Further, the subject's consent must be collected for each type of processing of the subject's data, and consent can be withdrawn at any time in a manner easily available to and understandable by the subject. The GDPR explicitly requires meaningful consent by regulating against the opposite, as well; it bans opt-out data-collection consent frameworks in forbidding the use of silent or passive regimes that have so often been used by internet companies to collect consent in the past, particularly for web cookies.

- **Individual rights**: The GDPR stipulates that data collectors offer a number of unassailable rights to data subjects. One is the general requirement that data collectors communicate their practices and the individual's options "in a concise, transparent, intelligible and easily accessible form, using clear and plain language." Moving forward, such requirements will be vital in providing consumers with the in-context information needed to make thoughtful decisions about their personal data. Equally important is the right to erasure of personal data held by a data controller and to the portability of personal data, shareable with the individual in machine-readable format. This latter provision, which we will touch on further in the following section on competition policy, is critical in the balance of power between individuals and corporates. In addition, data subjects are afforded the rights to access their data, rectify erroneous information about them, restrict the processing of their data, and object to the collection and processing of their data.

- **Protections from automated processing**: Perhaps the GDPR's most novel set of restrictions are those it institutes in regard to the automated processing and profiling of individuals. The core problem that the GDPR attempts to address is that companies—especially internet companies—analyze personal data to draw out certain inferences about us without our knowledge. It is not raw data that allows internet companies to most effectively curate ads and content; it is the inferences that these companies are able to make about us—about our personalities, interests, behaviors, character traits, and beliefs. But we know very little about this kind of secret processing. The GDPR, for the first time, institutes hard checks against this sort of practice, first by giving the individual the right to object to "profiling to the extent it is related to direct marketing." Alongside this, the GDPR gives individuals the ability to request that firms

cease the processing of their data and avoid making non-transparent decisions about them that have been powered by profiling. Finally, the regulation also establishes an important protection from algorithmic bias by disallowing firms from making discriminatory decisions "against natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status, or sexual orientation." This set of new protections in the face of the industry's use of opaque algorithms is a critical step in the right direction.

- **Explicit regulations on sensitive personal data**: Regulations instituted by the GDPR include requirements that firms obtain explicit consent for the collection of especially sensitive data, including data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs," as well as the stipulation that enforcement operators can block the collection of certain forms of personal data even if the individual consents to its collection. This provision is a critical bulwark for consumer privacy to guard against disinformation because this is the kind of data that enables the sort of audience segmentation that catalyzes filter bubbles and the distortion of the public sphere. The GDPR's restrictions over sensitive data could afford individuals substantially more protection from malicious uses of their data.

- **Strong enforcement**: A stunning feature of the GDPR is its establishment of harsh penalties for firms that violate the regulations. Enforcement authorities can levy fines of up to either 20 million Euros or 4 percent of global turnover. These are penalties that will force the industry into productive negotiations with both Brussels and the 28-nation enforcement authorities.

This menu of regulatory powers afforded to the European regulatory community is the start to establishing a strong privacy regime that will offer European citizens far greater power in the face of the industry than they historically have had. But how effective the regime instituted by GDPR will be determined in large part by the nature of enforcement. An important consideration for national policymakers in the United States will be whether we can accept a bifurcated regime of data regulation that affords certain classes of individuals—Europeans among them—one set of rights in the face of the industry, while Americans continue to have lesser rights.

Another critical point for review in the U.S. policymaking community is the usability challenge of GDPR. There is no doubt that the European regulations have given EU citizens tremendous new rights against commercial practices, but these rights have also come at an explicit cost to the individual consumer: The internet-based services that have complied with GDPR have instituted a bevy of compliance measures that add to the clutter of already-confusing privacy

disclosures made by firms. Some of the apparent impacts include expanded fine print in privacy policies, waves of email notifications, and increased just-in-time consent mechanisms (e.g., to accept cookies). In addition, some services have found the new regulations so challenging to comply with that they have indefinitely ceased serving the EU—among them the Pinterest-owned service called Instapaper,[53] the email unsubscribing service Unroll.me,[54] and the digital versions of the *Los Angeles Times* and *Chicago Tribune*.[55] This clear trade-off with usability imposed by GDPR is something that regulatory policymakers and the industry should address together.

A Way Forward for an American Baseline on Privacy

The disinformation problem is directly catalyzed by the phenomenon of the filter bubble and the consequential polarization of the American electorate. These echo chambers are begotten by the industry's expansive data collection, consumer profiling, and content targeting that altogether exploit personal information to segment audiences. Meaningful privacy regulation has the potential to blunt the capacity for nefarious audience segmenting and algorithmic targeting, which can thereby reverse the atomization of the polity and restore social dialogue and engagement among communities with differing views.

A baseline privacy law for the United States must begin by empowering the consumer. We propose that the United States renew its efforts to pass a comprehensive consumer privacy law that provides the following rights to the individual, drawing on precedents from legislative analysis in the Obama White House as well as legal frameworks in the EU and now in California.

- **Control**: Consumers require control of their data. This means that they should have to give direct and meaningful consent to the collection of their data by companies. It additionally means that they should have the ability to withdraw the company's access to it or delete it outright at any time, and to object to the processing of their data, including in digital advertising contexts, if they so choose. These controls should all be easy to find and communicated plainly to consumers. And finally, the data over which consumers have control should be the comprehensive set. As such, legislators should define personal information broadly to include any and all information pertaining to the individual, including the inferences that the corporate makes about the individual. This is critical. It is upon those inferences, whether drawn from first-party or third-party data, that internet companies and other corporates truly premise their commercial decisions.

- **Transparency**: As important, a baseline privacy law should enforce a strong commitment to maintaining transparency with the user. Most users

are likely completely unaware of the extent of the data collected about them by internet companies and other firms in the digital ecosystem. Even if they understand that companies like Facebook collect information about them through their use of the company's leading platforms, the layperson is likely unaware of the use of such off-platform tracking technologies as web cookies, email cookies, location beacons, and more. And the fact is that companies like Facebook and Google are far from being alone in using these technologies to maintain behavioral profiles. The entire industry must be more transparent, and this can only be enforced through federal legislation that appropriately codifies the privacy concepts of purpose specification and use limitation.

- **Enforcement**: A critical failing of federal privacy and security policy enforcement is that the enforcement is shockingly lax. Much of the problem lies in the fact that the independent regulatory agencies—the government entities that are meant to protect the public from corporate abuse—are terribly resourced. Agencies that are charged to police the digital sector including the FCC and FTC lack the funding and staff necessary to give the industry the scrutiny it deserves. More staff and funding can alleviate a number of tensions, among them the need to begin new investigations, understand modern and evolving technology, maintain closer ongoing dialogues with industry and civil society, and reduce the harm wrought by regulatory capture. Legislators should assure more resource goes to these two agencies in particular. Should Congress be unable to adequately resolve these consistent issues plaguing the regulatory agencies, legislators should afford consumers a private right of action so that they can sue firms in the industry directly.

Recent developments in California—particularly with the passage of Assembly Bill 375 as the new California Consumer Privacy Act of 2018—deserve recognition as the starting point for a path forward at the national level. This law is now the most protective privacy standard anywhere in the United States. We saw even greater promise in the ballot initiative that was originally proposed, and which prompted the serious consideration of A.B. 375; it was more robust and would have afforded individuals many novel protections in the face of digital disinformation. However, the California Consumer Privacy Act—which was watered down after interest lobbying—still represents progress from which the rest of the nation should build.[56]

A baseline privacy law for the United States must begin by empowering the consumer.

The new law affords California residents important new data rights vis-a-vis businesses that collect their personal data. But among the new law's less redeeming qualities are its lack of a private action for the individual for any violations of the law besides those encapsulated in its data breach regime, and a general reliance on attorney general enforcement in its stead; its lax definition of personally identifiable information, which is borrowed from California's existing data breach statute, which fails to include most kinds of modern data collected by internet companies among others; the fact that the rights to data-related requests about oneself are premised on that restrictive definition of personal information; and the fact that the right to be forgotten only applies to data that is directly provided by the user.

Our hope is that California's new law can trigger a much-needed discussion amongst policymakers at the national level—and renewed calls for the sort of meaningful federal legislation that we discuss above.

Competition

The relationship between market power, competition policy, and the problem of disinformation in our political culture is structural and indirect. The digital platform companies that aggregate and publish media content from channels across the internet have enormous influence over public discourse as de facto editors that determine the content we see. While there is some logic in applying regulations to monopolies as "one stop shops" to address immediate public harms, the long terms solution must involve a more robust competitive landscape to put market forces to work diversifying the digital media landscape. More to the point, competition policy affords opportunities to restore user control over data through portability and to provide individuals with the leverage they need to shape digital media products that do not devolve to the logic of data driven attention capture.

People are gradually losing track of the distinction between credible and questionable sources of news on the internet. "I saw it on Facebook" encapsulates the problem underlying the nation's broken media system. Facebook, of course, is not a publisher. It is both a media company and a technology platform that distributes the publications of others, whose brands meanwhile fade into the background of the medium.

The same is true (in slightly different ways) of Google search, YouTube, Twitter, and other internet platforms that aggregate content. And although these companies cannot be considered news editors in the traditional sense, they do perform one key editing task: selecting which content their audience will see. In so doing, they choose not to select content based on a set of judgements related to the democratic role of public service journalism (i.e. out of a principled commitment to inform the public). Instead, they make selections based on what will keep the user on the platform longer, thus enabling the display of more ads and the collection of more user data.

"I saw it on Facebook" encapsulates the problem underlying the nation's broken media system.

To be sure, this raw commercial logic was always a part of the media business, too. But on digital platforms, it has become the entire business. For modern

internet platforms, gone is the notion that the media entity should cultivate a set of top stories that meet the needs of an informed citizen. The criteria for selection here are derived from algorithmic processing of the voluminous data that these companies keep about each user. From the data, they determine what users will find relevant, attractive, outrageous, provocative, or reassuring—a personalized editorial practice designed not to journalistically inform citizens, but rather to grab and hold every user's attention. The precision and sophistication of the preference-matching grows with the improvement of the technology and the quantity of data. And the algorithm is indifferent as to whether it leads the user to towards facts and reasoned debate or towards conspiracy and nonsense.

When the attention-maximizing algorithms that serve as the editors of our political culture generate negative externalities for the public—such as filter bubbles that amplify disinformation and atomize the polity into opposed clusters—it is the role of government to act on behalf of society to reverse or contain the damage. This can happen in a variety of ways. We can make the criteria of the content selection—the aforementioned editing function—more visible to the user by stipulating that the platform's algorithms be made transparent to the public. We can also limit the amount of data the companies may process in order to blunt the precision of those filtering algorithms and protect people from being segmented into self-reinforcing, misinformed audiences by requiring more stringent privacy policies. (We have covered these approaches in the previous two sections)

As a third option, we can promote market competition by giving people more control over their data and generating alternative ways for people to find the information they seek. The theory of change behind this potential measure is that by destabilizing the monopoly markets for digital media aggregation, curation, and distribution, we will foster new market structures that better serve public interest outcomes.

What is the starting point for new competition policy that can better reflect the changes wrought by the digital ecosystem? For years, there has been public debate about whether the major technology platforms—Google, Facebook, Amazon, and Apple, in particular—are monopolies and whether they should justifiably be broken up or regulated as utilities. The phenomenal growth, profitability, and market share enjoyed by these firms heightens the urgency of the issue.

Without question, there is tremendous concentration of wealth and market power in the technology sector. And many segments of the digital economy bear the hallmarks of a "winner-take-all" market.[57] The top companies have gained dominance through a combination of data, algorithms and infrastructure that organically creates network effects and inhibits competitors. Put simply, once a network-based business reaches a certain scale, it is nearly impossible for

competitors to catch up. The size of its physical infrastructure, the sophistication of its data processing algorithms (including AI and machine learning), and the quantity of data served on its infrastructure and feeding its algorithms (constantly making them smarter) constitutes an unassailable market advantage that leads inexorably to natural monopoly.[58]

The top companies have gained dominance through a combination of data, algorithms and infrastructure that organically creates network effects and inhibits competitors.

For example, there is simply no economically viable method for any company to match Google's capability in the search market or Facebook's capacity in social networking. That is not to say these companies are eternal. But it does mean that until there is a major shift in technology or consumer demand, they will dominate in the winner-take-all market. It is also worth raising the caveat that we must be mindful that a regulatory regime across a variety of issues that requires extensive resources to implement could perversely add to this market dominance—as the existing oligopoly might be the only market players able to fully comply. That said, this is not a reason to shy away from addressing the competition problem head-on; and there are ways to tier regulatory requirements to match proportional impact of different kinds of firms.

Digital policy expert Peter Swire offers a useful rubric to evaluate whether a company has achieved monopoly-scale market power.[59] He offers four criteria: market share, essentiality of services, natural monopoly characteristics, and high consumer costs for exiting the market. In each of these categories, the tech platforms have met the standard. One company controls more than 91 percent of the global market in internet search,[60] two companies control 73 percent of the digital advertising market,[61] and one company operates the world's two most popular internet-based, non-SMS text messaging applications.[62] And to exit these markets, consumers pay a high price, particularly if they are long time users of the service.

This last point on the high cost of market exit—or switching costs, if there even exists a competitor that could offer a substitutable service—bears further consideration because it is directly related to the topic of the previous section on privacy. In these markets, most products are "free" in the sense that consumers

need not pay in hard currency for access to the service. But instead, they must pay by trading their personal information for services; in other words, they pay a "privacy price." Because there is little competition in these markets, and therefore little consumer choice, there is no option when a consumer becomes sensitive to rising privacy prices. These privacy prices are perfectly inelastic. No matter how much data Google or Facebook extract from users, no matter how that data is monetized, and no matter what level of transparency accompanies the user agreement, there is very little change in the user's demand for the service.

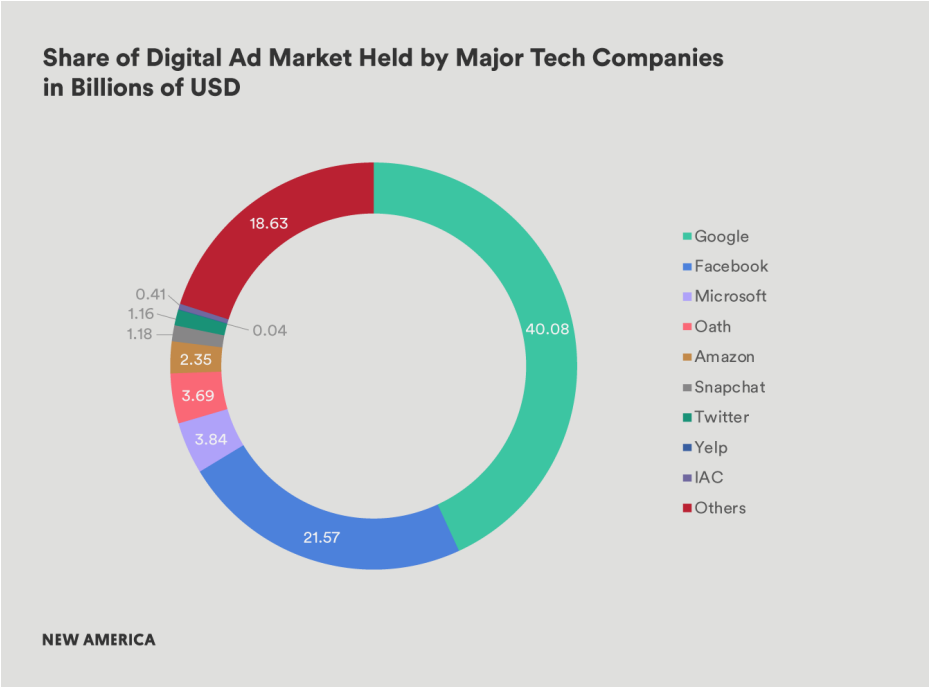
The leading digital platform companies have mastered this basic microeconomic dynamic. This is why a failure to agree to the terms of service results in only one option for consumers: to not use the service at all. Following Swire's logic, if the service is essential and the exit costs are high, then there is no choice at all. Consequently, the argument that the absence of consumer flight from the product is a market signal indicating satisfaction or indifference is an extraordinarily misleading fallacy. And placing the disinformation lens over this conundrum suggests the unsettling notion that to participate on the major internet platforms, consumers will necessarily be forced accept that political falsehoods shall be targeted at them.

No matter how much data Google or Facebook extract from users, no matter how that data is monetized, and no matter what level of transparency accompanies the user agreement, there is very little change in the user's demand for the service.

Europeans have begun pressing the point that privacy and competition policy converge when a company with market power makes unreasonable demands for data-sharing in its terms of service. The German antitrust authority opened an investigation of Facebook's practices last year, making precisely this case.[63] Similarly, the GDPR provision that requires companies to offer meaningful, nondiscriminatory options for opting out of data sharing service agreements intends to address this reality as well.[64] Indeed, one of the most high-profile lawsuits filed against the major technology companies in the wake of GDPR

enforcement points to the failure of Facebook to provide meaningful alternatives to accepting all terms and conditions of use.[65]

Regardless of whether these companies are defined as monopolies, their market position justifies an increase in regulation and oversight to protect consumer welfare, especially on data privacy. There have to be meaningful options for privacy other than the binary choice of accepting whatever terms are offered by monopolies for essential services or exiting the market altogether, particularly given the obscure, misleading, or hard-to-find privacy options currently offered by some of the companies leading this sector.[66] The policy ramifications implicate the need for both strong privacy policy enforcement as well as new forms of competition policy.



In light of this market and policy analysis, we see an urgent need to rethink competition policy as it applies to the technology sector. We believe the following measures, profiled in ascending order of ambition given current technological and political constraints, are necessary and promising opportunities for progress that demand further inquiry and examination in Washington and beyond. Most critically, we hope that these proposed measures can spark more robust discussion, research, and policy analysis.

Restrictions on Mergers and Acquisitions

There is an entire ecosystem of technology start-up companies that are built by their founders in hopes of being acquired for tidy sums by the dominant technology firms. And more visibly, the major technology firms have been overt in their strategy to acquire any competitive entrant that appears to gain market momentum (e.g. Instagram, WhatsApp, DoubleClick, YouTube, and Waze). This practice of acquiring competitors should be monitored and restricted. Looking back, it is clear that regulators should have been far more careful in assessing the potential of past mergers to result in market power and consumer harms. Any mergers that are permitted should be scrutinized and conditioned to restrict data-sharing between affiliates.[67]

Top 10 Acquisitions Over Past 10 Years for the 4 Major Internet Companies

Alphabet

Company name	Price	Type	Date
Motorola Mobility	$12,500,000,000	Device manufacturer	August 2011
Nest Labs	$3,200,000,000	Automation	January 2014
DoubleClick	$3,100,000,000	Digital advertising	April 2007
YouTube	$1,650,000,000	Video social media	October 2006
HTC properties	$1,100,000,000	Intellectual property	September 2017
Waze	$966,000,000	GPS navigation	June 2013
AdMob	$750,000,000	Digital advertising	November 2009
ITA Software	$676,000,000	Travel technology	April 2011

Company name	Price	Type	Date
Postini	$625,000,000	Communications security	July 2007
DeepMind Technologies	$625,000,000	Artificial intelligence	January 2014

Amazon

Company name	Price	Type	Date
Whole Foods Market	$13,700,000,000	Supermarket chain	June 2017
Zappos	$1,200,000,000	E-commerce	July 2009
Pillpack	$1,000,000,000	E-commerce	June 2018
Ring	$1,000,000,000	Security technology	February 2018
Twitch	$970,000,000	Streaming video	August 2014
Kiva Systems	$775,000,000	Robotics	March 2012
Souq.com	$580,000,000	E-commerce	March 2017
Quidsi	$545,000,000	E-commerce	November 2010
Elemental Technologies	$500,000,000	Video technology	September 2015
Annapurna Labs	$370,000,000	Microelectronics	Jan-15

Apple

Company name	Price	Type	Date
Beats Electronics	$3,000,000,000	Electronics and music streaming	August 2014
NeXT	$404,000,000	Hardware and software	February 1997
Anobit	$390,000,000	Flash memory	December 2011
AuthenTec	$356,000,000	Security	July 2012
PrimeSense	$345,000,000	Scanners	November 2013
P.A. Semi	$278,000,000	Semiconductor technology	April 2008
Quattro Wireless	$275,000,000	Digital advertising	January 2010
C3 Technologies	$267,000,000	Mapping	August 2011
Turi	$200,000,000	Machine learning	July 2009
Lattice Data	$200,000,000	Artificial intelligence	May 2017

Facebook

Company name	Price	Type	Date
WhatsApp	$19,000,000,000	Mobiel messaging	February 2014
Oculus VR	$2,000,000,000	Virtual reality	March 2014

Company name	Price	Type	Date
Instagram	$1,000,000,000	Social media	April 2012
LiveRail	$400m-500,000,000	Digital monetization platform	August 2014
Face.com	$100,000,000	Facial recognition	June 2012
Atlas Solutions	<$100,000,000	Digital advertising	February 2013
Parse	$85,000,000	Application development tools	April 2013
Snaptu	$70,000,000	Mobile application	March 2011
Pebbles	$60,000,000	Augmented reality	July 2015
FriendFeed	$47,500,000	Social networking	August 2009

Moreover, merger review should explicitly consider not only the concentration of horizontal market power but also the concentration of data that enables competitive advantage in multiple adjacent market segments. For example, in the case of Facebook's acquisition of Instagram, a case can be made that these services address different markets. However, the user data they collect that informs ad-targeting decisions is firmly in the same market, and more importantly, it is the market where most of the revenues are generated.

The most effective route for a Silicon Valley firm to profile individual users is to collect as much data as possible from as many sources as possible to create a comprehensive store of data that takes advantage of inferential redundancies to affirm the individual's behavioral preferences with greatest confidence and also eliminate any inaccuracies raised by misleading outlier activity data. If data is a source of primary value in the modern economy, then it should be a significant focus of merger review.

In addition, we would suggest an inquiry focused on the vertical integration of tracking and targeting services. The largest abuses of market power that appear to drive privacy violations, political polarization, cultural radicalization, and

social fragmentation are rooted in the combination of data tracking and audience targeting within a single business. This is particularly true for companies that possess tremendous amounts of data collected through the primary service (i.e., "on-platform" collection) but generate substantial marginal value atop that by aggregating data collected outside the service and buying it from third party vendors (i.e., "off-platform" collection).

If data is a source of primary value in the modern economy, then it should be a significant focus of merger review.

To conduct this analysis and regulatory review effectively, it is likely necessary to put a value or price on personal data. It is clear that the industry makes these calculations (as do their investors) when they review an acquisition or merger proposal. Regulators must also do so in order to generate relevant standards of review. One way to test this theory would be for regulators to study mergers approved in years past that received limited scrutiny and have since resulted in apparent increases in market power. These might include Facebook-Instagram, Facebook-Whatsapp, Google-DoubleClick, and Google-YouTube. Experts can look at changes in the market post-merger to determine the effect on price, market share, and consumer choice. By applying a standard of review pegged to the concentration of value in data and aggregated consumer attention that national regulators previously missed in these cases, we may discover ways to build a generally applicable rule that better protects consumers from anticompetitive commercial behaviors for the future.

Antitrust regulators can also specifically look to apply heightened privacy and security restrictions on certain firms. For mergers and acquisitions made in particular sectors, as in the case of BIAS providers acquiring media properties or advertising technology firms, there could be tailored restrictions that treat the problem of privacy in this especially sensitive context. For instance, BIAS providers seeking to close such acquisitions could be required to abide by tailored regimes to protect consumer privacy and security like the broadband privacy rules promulgated by the Obama FCC. In a similar example, firms that participate in the digital advertising ecosystem could be required not to link any shared or acquired data with any persistent identifiers.

The underlying goal here is to make space for competitive service providers to challenge the market dominance of the large platforms by offering new products —including those that privilege truly protective consumer privacy as a feature.

Antitrust Reform

From its origins, this country has been governed with strong anti-monopoly views; as far back as 1641, the legislature of the Colony of Massachusetts decreed: "There shall be no monopolies granted or allowed among us but of such new inventions as are profitable to the country, and that for a short time."[68] The primary mode of antitrust regulation in the United States correspondingly became rooted in maintaining competition in the market, and it is the underlying theory of structural economics that significantly influenced what came to be known as the Harvard School of antitrust, which held that a market tending toward monopoly or oligopoly could result in societal harm because such concentration in the market would afford firms excessive power over other societal entities.[69]

In short, concentrated markets could lead to anticompetitive behavior, collusion, barriers to market entry, and consumer harm, such as raising prices, lowering quality of products and services, limiting the variety of offerings, and lowering capacity for innovation. Corporate power could also lead to predatory pricing schemes and the diminishing of competitive forces in the market more generally. The harms to the public would then include lower wages, the creation of fewer novel enterprises and innovations, and increased political clout among the monopolistic class in a way that might threaten democracy. The Harvard School's goal was thus to premise regulation and enforcement on the structure of a market to protect competition and public welfare.

The influence of the Harvard School's theory of antitrust, dominant for most of American history, has waned in the last few decades. In its place has risen the Chicago School of antitrust enforcement.[70] It does not premise antitrust enforcement on the idea that the accumulation of market power allows the firm to engage in anticompetitive behaviors and that if it does, then the firm should be scrutinized. The new school of thought argues that enforcement should only come into consideration if a clear harm to consumer welfare can be established. In the Chicago School, that means basically only one thing: increased prices. The support for this new style of approach from all corners of the federal government, in part on the basis of Robert Bork's well-known writings on antitrust reform,[71] established it as the framework of choice for regulators throughout the 1970s and 1980s.

As many scholars have documented, this regime, still largely in place today,[72] is broken.[73] It creates arbitrary boundaries for regulatory jurisdiction. A firm that

limits choices for consumers can be just as (or more) harmful to the consumer as another that hikes prices; both practices diminish the consumer's value for money. To require that antitrust enforcement officials premise their decision-making primarily on whether or not consumer welfare has been harmed on the sole basis of price increases is to miss the point that a firm's presence and activity in the market is expressed through many variables, not exclusively consumer prices, and that the consumer suffers if any of these variables works against the interest of the consumer.

And indeed, it is clear now that the United States has missed the point. The near-required premise that antitrust regulators must establish harm to consumer welfare as evidenced by price hikes has apparently failed as the national economy has undergone the influences of rapid globalization. And when we consider the case of internet platforms in particular, it becomes quite difficult to find a way to address any anticompetitive behaviors in which they engage since many of them do not charge prices for their services or undercut the alternatives.

As a result, the march to market power in the tech industry has been largely unimpeded. These firms have become so large and valuable that they resist conventional instruments of oversight. Even in cases when regulators take aggressive action against anticompetitive practices (such as tying arrangements), it does not appear to create a disciplinary impact on the market. Consider the EU's recent announcement of a record fine against Google—$5 billion on top of last year's $2.7 billion fine—for violating competition standards in Europe. Despite these setbacks, Alphabet's stock price continues to rise as investors seem to shrug this off as a cost of doing business.[74]

It becomes difficult to find a way to address any anticompetitive behaviors in which internet platforms engage since many of them do not charge prices for their services or undercut the alternatives.

But are the leading internet brands causing consumers harm in any way? To see one of the most important and devastating examples of this harm, we need only connect back to the topic of digital disinformation and its distortion of the public sphere. For all of the reasons we have documented here (and elsewhere),[75] the concentration of market power in digital advertising and information distribution has catalyzed polarization and irrationality in our political culture. But the

problem is not simply about the elevation of low quality information, it is also about the decline in high quality information. To put it mildly, the public service news industry did not adapt well to the disruption of the internet, the displacement of print media as a profitable service, and the rise of platforms as aggregated distributors of digital content. With some notable exceptions (e.g. *The Economist*), the rising fortunes of Google and Facebook have coincided with a catastrophe for traditional news businesses.

A full account of why this happened and who bears ultimately responsibility is a beyond the scope of this essay. The point we want to make is straightforward: The accumulation of market power in the aggregation of news content in search and social media (for a zero price) together with the domination of the digital ad market (and the vast disparity of digital ad prices compared to print) has left the news industry with no path back to the profit models they enjoyed for nearly a century.

Whether we choose to read this history of the present as negative market externalities that accompanied a technological paradigm shift or the predatory pricing of digital platform monopolies, the public harm is clear as day: There are fewer journalists working today and less quality news in distribution than there once was—and as a society already in political tumult, we could not afford any decline at all. While it would not be fair to lay all of the blame on Silicon Valley's largest firms, it would be equally foolish to ignore the role they have played in weakening the 4th Estate and the responsibility they carry to help address this public problem. Hearkening back to the Harvard School, it is the role of antitrust regulators to protect the public from both the direct and the indirect harms of concentrated market power.

The rising fortunes of Google and Facebook have coincided with a catastrophe for traditional news businesses.

What do those harms look like exactly? Traditional journalistic organizations all over the United States, including major outlets such as the *Seattle Post-Intelligencer*, *San Francisco Chronicle*, and *Detroit Free Press*, have all drastically reduced their services in recent years. The news hole they have vacated is not empty, it is filled with all manner of content that Facebook and Google algorithms deem to be the most relevant. But relevance is not the same as quality. Nor does it begin to replace the social contract established in the commercial

news industry a century ago that sought (however imperfectly) to balance commerce with public service—a commitment from which consumers continue to benefit every time they pick up the newspaper, watch a television journalist, or visit a news website. On platforms like Facebook and Google, meanwhile, money rules over all else, expressed through the sale of aggregated attention to the end showing the consumer a relevant ad. This reality has engendered the dangerous forms of disinformation which now pervade over these platforms.

National policymakers and the public will require far more open scholarship on these matters to determine what the appropriate direction and dosage of regulatory or legislative action should be. But we must begin with a more thorough economic analysis of the current market structure in this information ecosystem. We see two areas of significant potential for competition enforcement officials as they consider the market power of internet platforms: to subject them to stricter antitrust reviews, and to apply stricter regulations on their business practices. Both sets of measures may be appropriate and necessary to adequately replace power in the hands of the individual consumer.

In regard to stricter antitrust reviews, we see great promise in empowering regulators to pursue enforcement against the industry on the basis of predatory pricing.[76] While the leading internet firms' style of predatory pricing—in offering zero-cost services or intellectual offerings at cut prices on the strength of the backing of the institutional investment community—carries a starkly different flavor from the schemes of the past in more traditional industries, it is predatory nonetheless and likely diminishes competition. And as the major platform companies offer a zero-price service, a clear externality is their indifference (and abdication of editorial responsibility) to maintaining a commitment to the veracity of the content shared on their platforms. This meanwhile contributes to an information ecosystem that is plagued by vastly decreased journalistic capacities at a time when the public requires far better access to the truth.

Scholars and critics have furthermore contested that antitrust officials can and should pursue vertical integrations of firms in the digital ecosystem.[77] We agree with this perspective. As discussed above, the business model emerging amongst firms that have for the most part been thought of as internet service providers—among them Verizon, Comcast, and AT&T—is progressively gravitating toward the dissemination of new media content and digital advertising. This combination of business practices at successive regions of the value chain presents a difficult challenge to the individual consumer's autonomy and privacy from the industry, and is one that requires further investigation, particularly in an era where the federal regulatory agencies largely lack a foothold to pursue these types of integration.

On platforms like Facebook and Google, meanwhile, money rules over all else, expressed through the sale of aggregated attention to the end showing the consumer a relevant ad.

We are similarly concerned about the accumulation and cultivation of personal data pursued by the leading internet firms as well, Facebook and Google among them. Both of these firms have sought to purchase other internet properties, thus closing horizontal mergers with brands like Waze and WhatsApp, and subsequently share consumer data collected throughout their universe of apps so as to compile behavioral profiles on individuals across their services. This carries with it certain privacy risks; consumers are often not aware that their YouTube viewing data could be shared with Waze to inform ad-targeting on the navigation service.

But perhaps even more critically, this ongoing accumulation and amalgamation of data—which is done purely for Google's commercial purposes—places Google in a position of power; its surveillance operation, powered by Alphabet's incredible wealth, reach and market power, can allow it to identify gaps in the market sooner than anyone else and pursue them in an anticompetitive manner. This is indeed among the concerns that were raised when Google infamously announced in 2012 that it would be reformulating its user privacy commitments into a single policy that would apply across the majority of its services.[78] Intimations that Facebook was exploring data-sharing arrangements with its subsidiary WhatsApp, which have variously since been confirmed[79] and may have led to the departure of WhatsApp's founders,[80] show that this sort of combination of data profiles from different services is a problem that is not restricted only to Google.

As antitrust regulators consider the case of internet firms, there is a menu of regulatory mechanisms (beyond the merger and acquisition measures discussed in the previous section) that can be pursued in contexts such as reviews of monopoly power, vertical integrations, acquisition proposals, or others to restrict the potential for harmful anticompetitive behaviors in the industry. Some of these include the following, presented here in no particular order.

- **Maintain commitments to past policies, including privacy restrictions**: Firms could be required to abide by all privacy policies,

terms of service, and other publicly disclosed commitments to users if they wish to acquire smaller entities and broaden their reach in a horizontal market. Such a measure, if applied in the case of a merger or acquisition, can obviate situations where a firm like Google extracts data from the acquired firm like DoubleClick to further strengthen its dominance in a given market.

- **Require transparency in data management practices:** As we argue elsewhere, transparency is not an antidote to consumer concerns like privacy, but it is a feature that can nonetheless have great impact if influencers come to understand the inner workings of the industry. To that end, antitrust officials could require certain monopolistic, vertically integrated, or merging entities to disclose any and all data management practices to the public or to the regulatory agency. If such a requirement is difficult to impose, antitrust officials could at a minimum require that only certain data sharing arrangements taking place within the firm's silos in particularly concerning ways be disclosed to regulatory bodies. Such conditions can enable agencies like the Antitrust Division to monitor the firm's data practices and determine whether or not it is impeding third-party access to its platform services such as advertising networks or media properties in an anticompetitive manner.

- **Assure government rights to review, investigate, and enforce**: Antitrust officials can establish conditions whereby if a firm presents particularly concerning challenges to market competition, or they permit a merger or acquisition to close, they will reserve the right to review the entity's compliance with all rules and regulations it is subject to. Additionally, officials can demand that they be afforded the right to access any relevant proprietary information and interview any key personnel should they wish to understand more about the merged firm's business practices.

- **Require support of a public media trust fund**: The government could organize—and antitrust officials could require subject firms' support of—a public media trust fund that redistributes contributions to journalistic organizations. The idea, raised by various scholars, can go a long way in restoring the strength of failing businesses that have a public interest quality to them including local journalistic outfits.

- **Examine utility-style regulation to counterweight market abuses**: The idea scholars have proposed that the leading internet platforms should be regulated in a manner similar to public utilities deserves serious attention. This sort of measure would require as a premise an evidentiary finding that the internet companies that should fall under such scrutiny are indeed monopolies or form a part of a tight oligopoly in particular

> market segments. Such a development could impart immense benefits to the modern information ecosystem if some kinds of nondiscrimination requirements were applied with circumspect rigor. Given the dominance that companies like Google and Facebook enjoy in the market for information consumption, the public may well benefit from implementation of new rules that notionally require that the platforms limit the ways they give preferential treatment to their own products and services. The EU's challenge of Google's promotion of its own shopping services serves as an example of the type of impact such a mode of regulation could have.

As difficult as it may be to achieve such reforms of our antitrust regime given the current political environment, pursuing this level of scrutiny to maintain sound competition policies can significantly blunt the capacity for anticompetitive behaviors in the industry, and as a result, enable and, in time, assure heightened stability and health of the electorate's information ecosystem.

Robust Data Portability

The market for digital media is premised on gathering personal data, building detailed behavioral profiles on individuals, and extracting value by selling advertisers targeted access to those users. There are very limited consumer choices in this market and high barriers to competitive entry for alternative service providers. These circumstances offer a clear case for policies that mandate data mobility or portability. This is true for many adjacent markets in e-commerce as well. According to the logic of "winner-take-all" network effects in the data economy, we should expect to see more of this trend. In this market, consumers trade data for services (or give data in addition to money), but they reap only a marginal reward for the value of that data (e.g. more relevant ads). The lion's share of the value from the data stays with the large data controllers. Consequently, when we consider structural solutions to the problem of data-driven filter bubbles, we are led logically to engage the question of how to distribute the value in the data economy more equitably.

The starting point here is data portability, an idea enshrined in the EU's GDPR as well as California's new data privacy law.[84] At the minimum, consumers should be able to have a copy of all data stored about them by a service provider. But critically, we would add that consumers should have access not only to user-generated content, but to the data that is generated about them by that company (which is often more valuable than user-generated content because it is combinatorial data linked to a wide variety of tracked user behaviors and interactions with other users). This is not about data ownership; it is about how individuals can exercise rights to control their digital identities; that is, to direct and protect their own personal information and benefit from the economic value

generated from it, thus affording them the capacity to shape their digital personalities in the ways they wish to shape them.

The lion's share of the value from the data stays with the large data controllers.

This is also not solely about privacy. It is about the distribution of value in the digital and data economy. If the future marketplace is dominated by machine learning algorithms that rely on the "labor" of personal data to turn the engine of pattern recognition, knowledge generation and value creation, then it follows that individuals should be empowered to have as much control as possible over the data that matters to them, that defines their identities to other parties, and which powers these facets of the modern economy.[85]

Today, data portability offered by leading internet companies has extremely limited value because the data that these firms choose to make available is largely incomplete and not usefully formatted. Further, there are few if any competitors that might even try to use it, either because they do not have the capability to do so or because they do not see the economic value. Notably, there are some (perhaps counterintuitive) signs within the companies that this could change. The recent announcement of the Data Transfer Project (DTP)[86] is very interesting. It is a project that brings Google, Facebook, Twitter, and Microsoft in a partnership to create a common API that permits users to move data between these service providers. So far, the project has limitations. It is in a very early stage and not yet ready for wide scale use. Exactly what data is given for transfer isn't clear. And the way the project is described suggests the creators weren't thinking about data portability as a hallmark feature of digital consumer behavior, but rather as an infrequent but important need to switch service providers.[87] Nonetheless, the appearance of the DTP shows that a more decentralized model of data management is not impossible under the current system, and element sof it might even be embraced by the large platforms.

What we propose here goes considerably beyond what DTP imagines. If we established a general right to robust data portability, expanded the concept of API-based inter-firm data exchange in the DTP with global technical standards, and built on that idea to fundamentally restructure the market, the resultant positive change for consumers would be inordinate.

Data portability offered by leading internet companies has extremely limited value because the data that these firms choose to make available is largely incomplete and not usefully formatted

Consider the potential for competitive market entrants if users were able to move to alternative service providers carrying the full value of their data, including the analytical inferences generated about them based on that data. Consider the value (in services and compensation) that users might unlock if they could reassemble data from every company that tracks, collects or stores data about them or for them into a user-controlled data management service. Consider the rebalancing of asymmetrical market power if these data management services could act on behalf of users to engage automatically with data controllers of all kinds to ensure data usage limits are held to a pre-chosen standard rather than the defaults offered in user agreements. Consider the possibilities that might emerge if users on one platform could reach users on a competitive service through a common application programming interface. Consider how users could choose to pool data with others (of their own volition) and create collective value that might be transferred to different platforms for new services or monetized for mutual gain. There are significant technical and data privacy challenges to making this a reality—in part because some of the value of one individual's data lies in the ways in which it is combined with another's data—but it has enormous potential.

As a thought experiment to explore new ideas and policy proposals, we offer the provocative proposal for data portability that follows. We believe some approximation of this concept would create substantial competitive pressure in the market with myriad potential benefits. But specific to the focus of this analysis, a change in market structure of this type would act to curb the negative externalities of data markets that are driving the proliferation of disinformation. Here is how it might work.

- **Define the Market**: Establish a legal definition for data controllers or data brokers—commercial firms of a certain size that collect, process, and commercialize personal information as a direct or indirect part of their business.

- **Establish Individual Data Rights**: These rights would include full transparency about the nature and scope of personal data collected, processed, shared or sold by the data controller. It would include access to the personal data given by the individual to a data controller as well as the data generated by the data controller about the individual. It would include the right to view, delete, or revise this data. And it would permit all individuals to set the conditions for the type of data collected, the uses to which it may be put, the terms of sharing and commercialization, and the frequency of consent required. (These rights map to the standards described in the previous section.)

- **Portability**: All data controllers would be required to make it possible for users (upon request) to access, copy, and port their data through a simple API. The format of ported data should be standardized so that ported data can be aggregated by the individual into a digital "data wallet" that should be machine-readable so that other data collectors can process the data should the individual wish to share personal data with them.

- **Data Management Service Marketplace**: Because it is unreasonable to expect that all consumers will have the capacity and capability to manage all of the data that they might copy and port to their data wallets from all of the dozens of data controllers with whom they interact, it will be necessary to establish a market for Data Management Services (DMS) that have regulated standards for security, privacy and interoperability. Similar to the way robo-advisors use software to manage investment portfolios based on a set of user-defined preferences (taking on the burden of interfacing with complex financial service markets), a DMS will manage data assets for individuals. The DMS will have a set of defaults for data rights in accordance with the law and will permit users to adjust those settings to match their preferences for data sharing. The DMS will automatically interface with the complex terms of service provided by data controllers and manage opt-in/opt-out settings (or reject service altogether) in accordance with the individual's pre-set preferences. In order to ensure that all individuals can exercise their data rights, it may be worthwhile to consider a lightweight "public option" DMS to which all citizens are automatically enrolled. Notably, such a system could also offer substantial efficiencies for streamlining and digitizing government services.

- **Intermediary DMS Marketplace**: On top of the public DMS system will be a secondary commercial market. This market will have access through an API to the underlying DMS service. It will permit private sector companies to offer innumerable commercial applications and services that individuals may choose in real time or through their pre-set preferences. Some will help users monetize their own data. Others may

> seek to group consenting users into aggregate data sets that optimize value. Others may permit easy switching between competitive service providers. Some may sell enhanced privacy protection or anonymity. The core concept is to leverage competition to put the user rather than the data controller in a position of greater control.

This imaginative scenario contains a variety of assertions and leaps of political will, policy change, technical development, market cultivation, and user acclimation. There are also some questions we purposely leave on the table for discussion regarding privacy protection, cybersecurity, and administration.

We are keenly aware that a new data management market that assembles personal data into easily accessible, decentralized packages raises serious questions about vulnerability. Yet, as blockchain scholars and various other security researchers have ably demonstrated, the decentralization of personal data from Silicon Valley to the individual need not mean it is insecure. Further, the intent here is not to present this concept as a fully developed proposal, but rather to spark a debate about competing ideas to redistribute the value of individual data more equitably in our society and in the process to generate competitive pressures that will limit the negative externalities of the current market that are weakening democracy.

We are experiencing the greatest concentration of wealth in capitalism in a century, and it is built on the value of aggregated personal data. We need bold proposals for change. And we need proposals that reduce inequalities without choking technological innovation or losing the utility of data analytics and network effects. The policy architecture presented here is a provocation to open that discussion to a wide range of possibilities. We plan to pursue this idea further in subsequent research to explore more precisely how it might work, what nascent industry efforts align with this concept, and the ways in which market forces like these could facilitate public benefit.

Conclusion: A New Social Contract for Digital Rights

The problem of disinformation that plagues modern democracy is rooted in the broader political economy of digital media markets that interact with structural changes in our societies. Network communications technologies have triggered a paradigm shift in how citizens access and process news and information. In the resulting creative disruption, we have gained enormous public benefits, not least of which is instant access for anyone with a smartphone to the vast store of human knowledge available over the internet.

But we have also undermined the traditional market for public service journalism and weakened the strength of democratic institutions that require the integrity of robust public debate. We have permitted technologies that deliver information based on relevance and the desire to maximize attention capture to replace the normative function of editors and newsrooms. Further, we have overlooked for too long the ways in which these technologies—and the tracking and targeting data economy they power—have contributed to the gradual fragmentation and radicalization of political communications.

For two decades, public policy has taken a hands-off approach to these new markets, believing that regulation might blunt innovation before these technologies reached maturity. Now, we have dominant market players that have built the most valuable companies in the world, and yet they still operate largely without the oversight of public government. The steady increase in negative externalities these new tech monopolies generate for democracy has been building for years. In recent months, these developments have suddenly hit the vertical section of an S-curve of socio-political change, and we are feeling the consequences.

We have permitted technologies that deliver information based on relevance and the desire to maximize attention capture to replace the normative function of editors and newsrooms.

For these reasons, it is time to design a public policy response to rebalance the scales between technological development and public welfare through a digital

social contract. This report provides a textured analysis of what this agenda should look like. It is extremely challenging because there are no single-solution tools that are likely to meaningfully change outcomes. Only a combination of policies—all of which are necessary and none of which are sufficient by themselves—will begin to show results over time. We believe that building this package of policies around core principles of transparency, privacy and competition is the right approach. And we look forward to others producing parallel analyses, challenging our conclusions, or building on our work.

Despite the scope of the problem we face, there is reason for optimism. Silicon Valley giants have begun to come to the table with policymakers and civil society leaders in an earnest attempt to take some responsibility. Gone are the flippant dismissals that technology markets have nothing to do with the outcomes of democratic processes or the integrity of public institutions. And governments are motivated to take action. Europeans have led on data privacy and competition policy. Meanwhile, a variety of countries are focused on transparency and election security. The research community is getting organized and producing promising new studies. And the public service news industry is highly attuned to the problem, dedicating resources to fact-checking and showing signs of a resurgent commitment to the public service ethos that has long animated its role in democracy (if not always in functional practice).

Most importantly, the sleeping dragon of the general public is finally waking up. For the first time, people are asking questions about whether constant engagement with digital media is healthy for democracy. They are developing more critical instincts about false information online and demanding accountability from companies that play fast and loose with personal data and stand aside as organized disinformation operators seek to disrupt democracy. It is impossible to predict how the path of reform will lead us to restoring the strength of democratic institutions and public confidence in them. But we can at least see the starting point.

Notes

1 David Streitfeld, Natasha Singer and Steven Erlanger, "How Calls for Privacy May Upend Business for Facebook and Google", New York Times, March 24, 2018.

2 Jane Wakefield, "Facebook and Google need ad-free options says Jaron Lanier", BBC, April 11, 2018.

3 George Soros, "The Social Media Threat to Society and Security", Project Syndicate, February 14, 2018.

4 Taylor Hatmaker, "Facebook's latest privacy debacle stirs up more regulatory interest from lawmakers" , Tech Crunch, March 18, 2018.

5 Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election", Journal of Economic Perspectives, 2017 Spring.

6 Alicia Parlapiano and Jasmine C. Lee, "The Propaganda Tools Used by Russians to Influence the 2016 Election", New York Times, February 16, 2018.

7 Carole Cadwalladr, "The Cambridge Analytica Files –– 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower," The Guardian, March 18, 2018.

8 Scott Shane, "How Unwitting Americans Encountered Russian Operatives Online," The New York Times, February 18, 2018.

9 Jillian D'Onfro, "How YouTube search pushes people toward conspiracy theories and extreme content," CNBC, March 12, 2018.

10 James Vincent, "Why AI isn't going to solve Facebook's fake news problem," The Verge, April 5, 2018.

11 Amy Gesenhues, "Facebook's new rules for political & issue ads start today", Marketing Land, May 25, 2018.

12 See, e.g. Seth Fiegerman, "Facebook and Twitter face uncertain road ahead," CNN, July 27, 2018.

13 Esp., U.S. Senator Mark Warner, White Paper, "Potential Policy Proposals for Regulation of Social Media and Technology Firms," July 30, 2018; and UK House of Commons, Digital, Culture, Media, and Sport Committee, "Disinformation and 'fake news': Interim Report," July 24, 2018.

14 Ellen L. Weintraub, "Draft internet communications disclaimers NPRM," Memorandum to the Commission Secretary, Federal Election Commission, Agenda Document No. 18-10-A, February 15, 2018.

15 "Statement of Reasons of Chairman Lee. E. Goodman and Commissioners Caroline C. Hunter and Matthew S. Petersen, In the Matter of Checks and Balances for Economic Growth, Federal Election Commission, MUR 6729, October 24, 2014.

16 Mike Isaac, "Russian Influence Reached 126 Million Through Facebook Alone", New York Times, October 30, 2017.

17 See, United States of America vs. Internet Research Agency, February 16, 2018.

18 Kate Kaye, "Data-Driven Targeting Creates Huge 2016 Political Ad Shift: Broadcast TV Down 20%, Cable and Digital Way Up", Ad Age, January 3, 2017.

19 Lauren Johnson, "How 4 Agencies Are Using Artificial Intelligence as Part of the Creative Process", Ad Week, March 22, 2017.

20 "Honest Ads Act"

21 Kent Walker, "Supporting election integrity through greater advertising transparency", Google, May 4, 2018.

22 "Hard Questions: What is Facebook Doing to Protect Election Security?", Facebook, March 29, 2018.

23 Bruce Falck, “New Transparency For Ads on Twitter”, Twitter, October 24, 2017.

24 See the Facebook Ad Archive.

25 See the Twitter Ad Transparency Center.

26 Aaron Rieke and Miranda Bogen, “Leveling the Platform: Real Transparency for Paid Messages on Facebook”, Team Upturn, May 2018; Young Mie Kim, “Report: Closing the Digital Loopholes that Pave the Way for Foreign Interference in U.S. Elections”, Campa ign Legal Center, April 16, 2018.

27 Laws governing political ad transparency are often limited to ads that mention a candidate, a political party, or a specific race for an elected office. Yet a great many ads intended to influence voters mention none of these things, but they instead focus on a political issue that is clearly identified with one party or another. Hence, reform advocates have argued that the scope of political ad transparency must be extended to reach all ads that address a political issue rather than the narrower category of ads reference candidates or political parties.

28 Sen. Amy Klobuchar, S. 1989: “Honest Ads”, U.S. Congress, October 19th, 2017

29 “REG 2011-02 Internet Communication Disclaimers”

30 See UK report, Conclusions, Paragraph 36

31 Facebook’s political advertising policy was announced in May 2018. In addition to this catch-all category, it also includes specific reference to candidate ads and election-related ads.

32 See, Facebook’s list of “national issues facing the public.”

33 Many have proposed versions of this idea—but it was popularized by Tim Wu’s New York Times opinion piece,Tim Wu, “Please Prove You’re Not a Robot”, New York Times, July 15, 2017.

34 Senator Hertzberg, Assembly Members Chu and Friedman, “SB-1001 Bots: Disclosure”, California Senate, June 26, 2018.

35 Julia Powles, “New York City’s Bold, Flawed Attempt to Make Algorithms Accountable”, New Yorker, December 20, 2017; Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights, Executive Office of the President, May 2016

36 Dillon Reisman, Jason Schultz, Kate Crawford and Meredith Whittaker, “Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability”, AI Now, April 2018; Aaron Rieke, Miranda Bogen, David Robinson, and Martin Tisne, “Public Scrutiny of Automated Decisions,” Upturn and Omidyar Network, February 28, 2018.

37 See, e.g. The National Artificial Intelligence Research and Development Strategic Plan, Networking and Information Technology Research and Development Subcommittee, National Science and Technology Council, October 2016; and “Broad Agency Announcement, Explainable Artificial Intelligence (XAI),” Defense Advanced Research Projects Agency, DARPA-BAA-16-53, August 10, 2016.

38 European Commission, GDPR Articles: 4(4), 12, 22 , Official Journal of the European Union, April 27, 2017.

39 See, e.g., Will Knight, “The Dark Secret at the Heart of AI,” MIT Tech Review, April 11, 2017.

40 “Tenets,” The Partnership on AI.

41 Lee Rainie, “The state of privacy in post-Snowden America”, Pew Research Center, September 26, 2016.

42 Federico Morando, Raimondo Iemma, and Emilio Raiteri, Privacy evaluation: what empirical research on users’ valuation of personal data tells us, Internet Policy Review, Vol. 3, Iss. 2, 20 May 2014.

43 Jessica Guynn, Delete Facebook? It's a lot more complicated than that, USA Today, March 28, 2018.

44 An interesting note on this matter is that BIAS providers have, in the recent past, made the argument that they should to be able to use the consumer's browsing history—known as broadband activity data —to develop behavioral profiles so that they can compete with internet companies in the market digital advertising. This is an unfortunate and misleading argument. BIAS providers—like retail banks or insurance companies—collect data on the consumer to provide a critical service to the consumer for which the consumer is forced to pay additional fees. This is namely access to the internet. That BIAS providers argue that they should be able to use their privileged place in the market to take data collected for one purpose (provision of internet services) and use it for another is misplaced; we would hold a similar position with the banking and insurance industries as well. And while BIAS providers may choose to further argue that they are different from these other types of firms since internet service providers are part of the digital ecosystem along with internet firms like Facebook and Google, this too is a misleading argument since this is an arbitrarily chosen market boundary. The only conclusion, independent of any current politics, is that broadband activity data should have special protection from commercial use for tertiary purposes.

45 Brian Fung, "Trump has signed repeal of the FCC privacy rules. Here's what happens next.", Washington Post, April 4, 2017.

46 A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, Federal Trade Commission, July 2008.

47 Comment of Terrell McSweeny, Commissioner, Federal Trade Commission, In the Matter of Restoring Internet Freedom, WC Docket No. 17-108, July 17, 2017.

48 "The NAI Code of Conduct", Network Advertising Initiative.

49 Nitasha Tiku, "Facebook's Privacy Audit Didn't Catch Cambridge Analytica", WIRED, April 19, 2018.

50 Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, The White House, February 2015.; Note that privacy legislation, like the Electronic Privacy Bill of Rights championed by Vice President Al Gore in 1998, has been advocated by past administrations. But none were as comprehensive as the Obama Administration's effort.

51 Office of the Press Secretary, "We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online," The White House, February 23, 2012.

52 Ed Chau, "AB-375 Privacy: personal information: businesses.", California State Legislature, June 28, 2018.

53 Nick Statt, Instapaper is temporarily shutting off access for European users due to GDPR, The Verge, May 23, 2018.

54 Natasha Lomas, Unroll.me to close to EU users saying it can't comply with GDPR, TechCrunch, May 5, 2018.

55 Alanna Petroff, LA Times takes down website in Europe as privacy rules bite, CNN, May 25, 2018.

56 We also wish to note that we see quality in a number of legislative proposals that, while not as broad or comprehensive as the approach taken in the Consumer Privacy Bill of Rights or the California Consumer Privacy Act, would represent real progress in narrower aspects for consumers. Some of these legislative proposals that have been introduced at the federal level include, among others, the SAFE KIDS Act introduced by U.S. Senators Richard Blumenthal and Steve Daines, the CONSENT Act introduced by U.S. Senators Edward Markey and Richard Blumenthal, and the Data Broker Accountability and Transparency Act introduced by U.S. Senators Richard Blumenthal, Edward Markey,Sheldon Whitehouse, and Al Franken.

57 Om Malik, "In Silicon Valley Now, It's Almost Always Winner Takes All", New Yorker, December 30, 2015.

58 This summation of network effects and the so-called "winner take all" market phenomenon is common to most scholarship and commentary about the contemporary tech oligopoly. It is nicely portrayed in Patrick Barwise, "Why tech markets are winner take all," LSE Business Review, June 16, 2018.

59 Peter Swire, "Should Leading Online Tech Companies be Regulated Public Utilities", Lawfare Blog, August 2, 2017.

60 "StatCounter: Global Stats", Statcounter, July 2018.

61 Jillian D'Onfro, "Google and Facebook extend their lead in online ads, and that's reason for investors to be cautious," CNBC, December 20, 2017.

62 "Most popular global mobile messenger apps as of July 2018, based on number of monthly active users (in millions)", Statista, 2018.

63 Bundeskartelamt "Preliminary Assessment in Facebook Proceeding," December 19, 2017.

64 See, e.g. EU General Data Protection Regulation, Articles 5, 6, 7, 9, 12 & 15 as well as Recitals 63 & 64.

65 See, Complaint of NOYB against Facebook, May 25, 2018.

66 "Facebook and Google use 'dark patterns' around privacy settings, report says", BBC, June 28, 2018.

67 This call for deeper scrutiny of acquisitions has been treated at length by other sources, see, e.g. Tim Cowen and Phillip Blond, "'TECHNOPOLY' and what to do about it: Reform, Redress and Regulation", Respu blica, June 2018.

68 William Letwin, Law and Economic Policy in America: The Evolution of the Sherman Antitrust Act, University of Chicago Press, 1956.

69 Robert D. Atkinson and David B. Audretsch, "Economic Doctrines and Approaches to Antitrust," Information Technology & Innovation Foundation, January 2011.

70 Richard Posner, "The Chicago School of Antitrust Analysis," University of Pennsylvania Law Review, Vol. 127, No. 4, April 1979.

71 Robert Bork, The Antitrust Paradox, Free Press, 1993.

72 This, for the most part, is true, though the U.S. regulatory community has variously shown an interest in other means of enforcement, including in the Federal Trade Commission's Horizontal Merger Guidelines released in 2010.

73 E.g., Lina Khan, Amazon's Antitrust Paradox, Yale Law Journal, Vol. 126, No. 3, January 2017; Franklin Foer, World Without Mind: The Existential Threat of Big Tech, Penguin Press, 2017.

74 Hayley Tsukayama, Alphabet shares soar despite hit to profit from Google's European Union fine, The Washington Post, July 23, 2018.

75 Dipayan Ghosh and Ben Scott, "Digital Deceit, The Technologies Behind Precision Propaganda on the Internet," New America and the Shorenstein Center for Media, Politics and Public Policy, Harvard Kennedy School, January 2018.

76 Nitasha Tiku, How to Curb Silicon Valley Power—Even With Weak Antitrust Laws, WIRED, January 5, 2018.

77 See, e.g., "Should regulators block CVS from buying Aetna?," The Economist, November 7, 2017; William A. Galston and Clara Hendrickson, "What the Future of U.S. Antitrust Should Look Like," Harvard Business Review, January 9, 2018.

78 Jon Brodkin, Google's new privacy policy: what has changed and what you can do about it, Ars Technica, March 1, 2012.

79 Chris Merriman, WhatsApp and Facebook are sharing user data after all and it's legal, The Inquirer, May 24, 2018.

80 Nick Statt, WhatsApp co-founder Jan Koum is leaving Facebook after clashing over data privacy, The Verge, April 30, 2018.

81 Esp. Victor Pickard, Break Facebook's Power and Renew Journalism, The Nation, April 18, 2018.

82 See, e.g., Richard Eskow, "Let's nationalize Amazon and Google: Publicly funded technology built Big Tech," Salon, July 8, 2014; Jonathan Taplin, "Is It Time to Break Up Google?," The New York Times, April 22, 2017; and "'A Web of Totalitarian Control': George Soros Adds to Davos's Demand for Tech Regulation," F ortune, January 26, 2018.

83 Karen Gilchrist, EU hits Google with a record antitrust fine of $2.7 billion, CNBC, June 27, 2017.

84 European Commission, "GDPR Article: 20", Officia l Journal of the European Union, April 27, 2017.

85 For more on this concept, see, e.g. Pedro Dominguez, The Master Algorithm.

86 https://datatransferproject.dev/

87 See DTP White Paper, https://datatransferproject.dev/dtp-overview.pdf. The paper recommends against federating data from multiple service providers into a Personal Information Management System (for sensible reasons of cyber-security), but this also indicates that the DTP only contemplates a portion of the concept proposed here.

88 See Tom Wheeler, "How to Monitor Fake News," The New York Times, February 20, 2018; Wael Ghonim and Jake Rashbass, "It's time to end the secrecy and opacity of social media," The Washington Post, October 31, 2017.

NEW AMERICA