

PRIVACY: Shorenstein/New America report says big tech business model is broken, untrustworthy over handling of user data

<https://www.wsj.com/articles/big-techs-business-model-is-broken-report-says-1537826407>

The report is called "Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet" <https://www.newamerica.org/public-interest-technology/reports/digital-deceit-ii/executive-summary/>

PRINTABLE VERSION OF FULL REPORT:

[https://s3.amazonaws.com/newamericadotorg/documents/Digital Deceit 2 Final.pdf](https://s3.amazonaws.com/newamericadotorg/documents/Digital_Deceit_2_Final.pdf)

WSJ: Big Tech's Business Model Is Broken, Report Says

Industry giants deserve tougher regulation, including scrutiny of deals that let them suck up more data

By

Deepa Seetharaman

THE WALL STREET JOURNAL

Sept. 24, 2018 6:00 p.m. ET

Silicon Valley tech giants can't be trusted to police themselves and should be subject to tougher regulation, including around their pattern of acquiring competitors to accumulate ever-larger stores of user data, according to a critical new report released Monday.

The business models powering digital advertising platforms like Facebook Inc. and Alphabet Inc.'s Google still undermine user privacy and incentivize disinformation campaigns despite recent efforts by tech companies to prevent abuse, says the report from Harvard's Shorenstein Center on Media, Politics and Public Policy and New America, a left-leaning Washington-based think tank.

"We need to completely reorganize the way that industry works," said Dipayan Ghosh, who previously worked on privacy and policy issues at Facebook and is now a fellow at the Shorenstein Center.

The [report lands](#) amid a broad discussion in the industry and in Washington, D.C., about how aggressively lawmakers should move on Silicon Valley's biggest firms, and comes just days before the [Senate Commerce Committee is due to hold a high-profile hearing](#) on the privacy practices of several large tech companies. Google, Amazon.com Inc., Twitter Inc. and Apple Inc. will all send privacy executives to testify at the Senate hearing, along with

telecommunications firms AT&T Inc. and Charter Communications Inc. A Facebook representative isn't scheduled to attend.

The authors argue that the federal government should take the lead on regulations rather than states like California, which recently passed a tough new privacy law that the industry broadly opposes. Most big tech companies have said they are open to sensible regulation as long as it doesn't overly curtail their ability to offer personalized products and services to consumers.

Mr. Ghosh and his co-author, Ben Scott, a director of policy and advocacy at the Omidyar Network, argue that protecting user data will require a combination of stronger privacy laws and limits on how much data the tech companies can gobble up. They add that tech companies also need to provide additional disclosure about how their information is used to serve them ads, far beyond what is currently shared.

Over the course of the year, the tech companies have announced changes to their privacy practices and have tried to take steps to shore up user trust. But those changes don't go far enough to address the deeper problems of the platforms, which are still reliant on maintaining user attention, according to Messrs. Ghosh and Scott, who wrote a separate report in January critical of the big tech companies.

"I think we both felt at the beginning of the year, there was potential to talk to the industry," said Mr. Ghosh, who previously served as a White House technology adviser under President Barack Obama. "We are increasingly disillusioned now."

Among the specific recommendations is for tougher restrictions on tech-related mergers and acquisitions, particularly on those that allow the biggest companies to add to their vast stores of data about consumers. "If data is a source of primary value in the modern economy, then it should be a significant focus of merger review," the authors write.

They also call for more aggressive third-party auditing of algorithms underpinning these systems.

Write to Deepa Seetharaman at Deepa.Seetharaman@wsj.com

Appeared in the September 25, 2018, print edition as 'Report: Big Tech Needs Fixes.'

***WHAT FOLLOWS IS AN EXCERPT FROM THE
SHORENSTEIN / NEW AMERICA REPORT – THE SECTION
ADDRESSING PRIVACY.***

EXCERPT: Digital Deceit II

A Policy Agenda to Fight Disinformation on the Internet

Authors

[Dipayan Ghosh](https://www.newamerica.org/our-people/dipayan-ghosh/) | <https://www.newamerica.org/our-people/dipayan-ghosh/>
Pozen Fellow, Shorenstein Center on Media, Politics and Public Policy

A computer scientist and privacy engineer by training, Ghosh joined New America from Facebook, where he was a privacy & public policy advisor. Prior to his time at Facebook, Ghosh was a technology policy advisor at the White House during the Obama Administration.

[Ben Scott](#)

Director of Policy & Advocacy, Omidyar Network | <https://www.newamerica.org/our-people/ben-scott/>

Ben Scott was Senior Advisor to the Open Technology Institute at New America and director of the European Digital Agenda program at the Stiftung Neue Verantwortung in Berlin. He is Director of Policy & Advocacy at the Omidyar Network. Previously, he was Policy Adviser for Innovation at the US Department of State. Prior to joining the State Department, for six years he led the Washington office for Free Press. 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.

BELOW EXCERPTED FROM:

<https://www.newamerica.org/public-interest-technology/reports/digital-deceit-ii/executive-summary/>

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

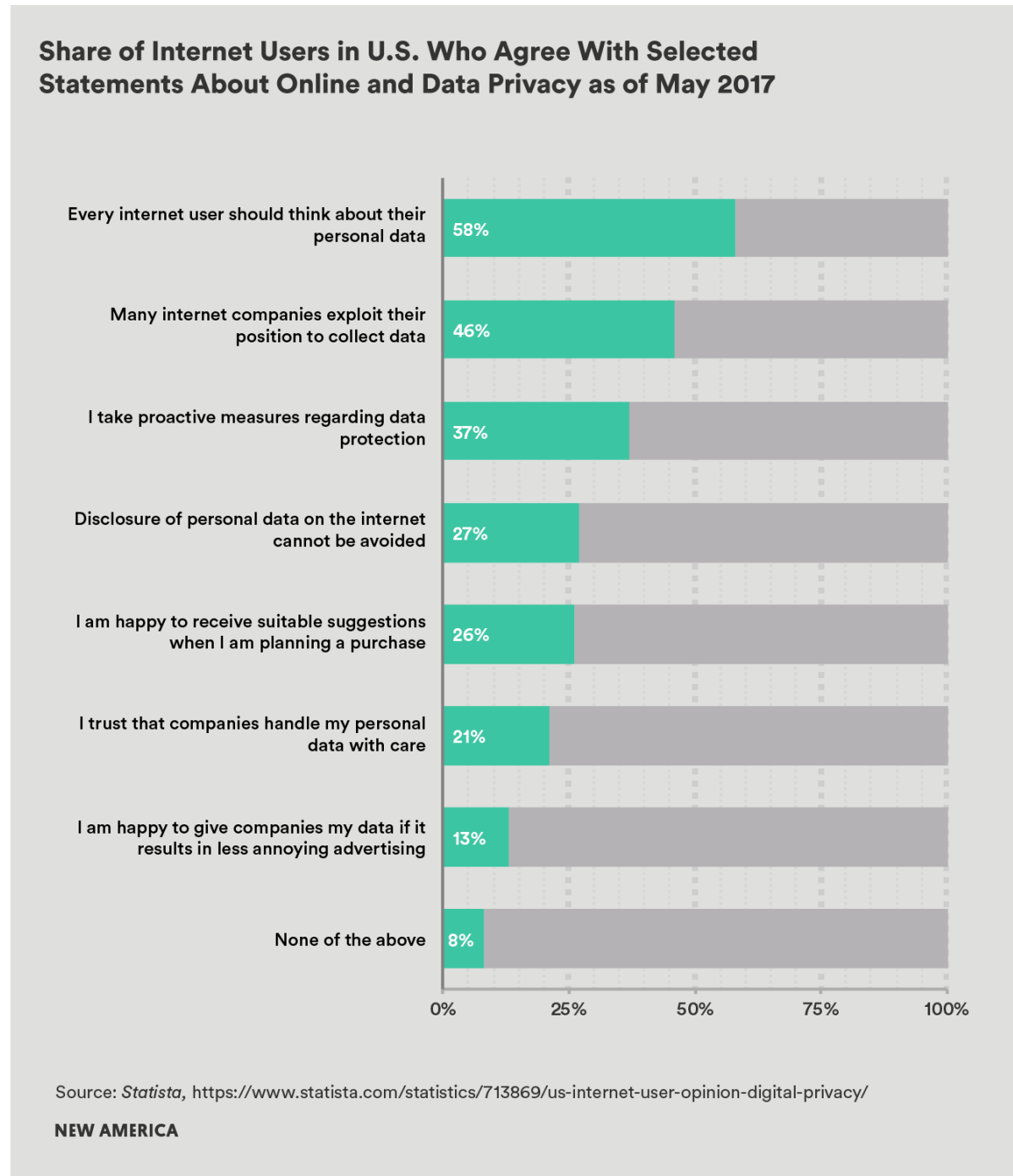
It is not only Facebook, Google, Twitter, and other internet companies that engage or plan to engage in tracking and targeting practices. So do the owners of physical networks—known as broadband internet access service (BIAS) providers. BIAS providers, situated as the consumer’s route to the internet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

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 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.