

THE NEW CENTER



Issue 02

Think Centered

Big Tech

Public Discourse and Privacy

ABOUT THE NEW CENTER

American politics is broken, with the far left and far right making it increasingly impossible to govern. This will not change until a viable center emerges that can create an assertive agenda that appeals to the vast majority of the American people.

This is the mission of The New Center, which aims to establish the intellectual basis for a viable political center in today's America.

We create and promote ideas that help people see common sense solutions to the problems we face.

This paper was developed with indispensable research and writing contributions from the New Center policy team: Julia Baumel, Evan Burke, Zane Heflin, Laurin Schwab and Aleksandra Srdanovic.

Big Tech

Public Discourse and Privacy

THE NEW CENTER



BIG TECH

Table of Contents

OVERVIEW 8

Introduction 10

New Center
Solutions in Brief 12

Big Tech At-a-Glance 14

THE ISSUES 18

Privacy 20

Public Discourse 28

Future Threats 36

Accountability 38

**WHERE LEFT
AND RIGHT
MIGHT COME
TOGETHER** 40

**PUBLIC
OPINION** 42

**POLICY
SOLUTIONS** 46Toward Real
Transparency 48Legislation to Protect
Privacy 50Algorithmic
Accountability 52

Congress on Tech 54

Platform Companies 55



BIG TECH

An Overview

Public Discourse and Privacy

America's leading technology companies—Apple, Facebook, Amazon, Alphabet, and Microsoft—aren't just among the biggest businesses in the world. They pervade our lives in ways that corporate behemoths of years past never did. Increasingly, they know what we're doing, where we're doing it, and with whom. As the primary news source for tens of millions of Americans, they are increasingly shaping how we think.

But we—as a country and government—have no idea what to do about it. These companies are exemplars of American innovation; leading the growth of our economy and creating jobs while connecting people in vast social networks and providing American citizens with more access to information than anyone in human history.

But the vast reach of these companies has given them tremendous influence over our public discourse and personal privacy. Washington and the tech industry has yet to settle on a sustainable or sensible framework for how

to manage these concerns. The political left obsesses over the scourge of “fake news” particularly as it relates to the 2016 election. The right fumes over allegations of censorship of conservative news and perspectives.

For its part, industry has adopted an ad hoc and mostly reactive stance, best evidenced by Facebook's pledge to double its “safety and security” staff in the wake of the Cambridge Analytica customer data breach. The big technology companies—in fits and starts—are taking customer privacy more seriously.

The left and the right are evincing concerns about real problems.

But the most important questions are too often going unasked and unanswered.

UNASKED QUESTIONS:



Are these companies really platform businesses? That is, are they impartial connectors of buyers and sellers, customers and vendors, news producers and news consumers, friends and neighbors? Or are they becoming media companies, with the power to pick and choose what we see, hear, and read?



What are technology companies really doing with our data? Is their right to make profits off what they know about us taking an unacceptable toll on our personal privacy?



Over 20 years ago, Congress gave internet companies—like social media platforms and search engines—immunity from being responsible for content posted by third parties. This protection helped nourish the growth of a fast-growing industry. But have we reached a point where these companies have too much influence without the accountability that must come with it?

DISCOURSE

PRIVACY

ACCOUNTABILITY

Beyond the noise about fake news, these are the kinds of questions our leaders—in Washington and within the big technology companies—must finally address.

1.



2.



TOWARD REAL TRANSPARENCY

Large tech companies claim they are being more transparent about how they handle your data and decide which content can exist on their platforms, but often they just provide the illusion of compliance: with long, impenetrable terms of service or standards that no one reads.

At a minimum, large tech companies should agree upon and adhere to common standards that establish a clear, standardized process for reviewing and removing material from online platforms.

FEDERAL LEGISLATION TO PROTECT ONLINE PRIVACY

Large tech companies have every incentive to collect as much personal data as possible from their consumers. Comprehensive federal privacy legislation should be enacted to give consumers more control over their personal data, and it should include:

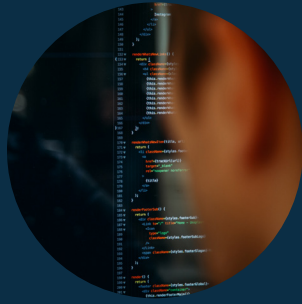
- a “right to be forgotten” online
- opt-out mechanisms for data sales and third party data use
- data collection disclosure
- a right to request all personal data collected by tech companies
- prompt data breach notifications

NEW CENTER

Solutions in Brief

FIVE CRITICAL STEPS TO PROTECT OUR PRIVACY
AND PUBLIC DISCOURSE ONLINE

3.



ALGORITHMIC ACCOUNTABILITY

Tech companies necessarily use artificial intelligence (AI) to screen the reams of content that exist and are created across their platforms. However, these AI systems are black boxes. Consumers don't understand how or why decisions are made, and the AI's decisions are often wrong. We need real standards to make AI—and the companies behind it—accountable.

4.



CONGRESS NEEDS TO GET SMART ON TECH

Recent congressional hearings featuring tech company executives have revealed that too many members of Congress don't appear to understand how big tech companies operate or the scope and scale of the problems they present. Once, Congress had a resource for objective analysis on pressing matters raised by new technologies—the Office of Technology Assessment. The OTA was shuttered in 1995, right before the advent of the modern internet. It needs to be brought back.

5.



PLATFORM COMPANIES NEED TO ACT LIKE PLATFORM COMPANIES

If large tech companies like Facebook and Google are indeed the platform companies they claim to be and not publishers, they need to act like it. That means that in deciding what can exist on their platforms, they should hew closely to the First Amendment as articulated by the U.S. Supreme Court: speech should be free unless it incites violence or promotes dangerous obscenity.

BIG TECH USERS

Numbers At-a-Glance



MONTHLY ACTIVE FACEBOOK USERS

2.23 billion +



700 million +

iPhone users as of 2017



100 million +

members on Amazon Prime, the paid subscription service that offers two-day delivery and other benefits



1.4 billion +

Microsoft Windows operating system users



3.5 billion

Google searches processed in a day. Google Search, Gmail, Google Maps, Google Chrome, Google Play, YouTube, and Android each have more than 1 billion users. Android just hit 2 billion in 2017¹

Numbers At-a-Glance

MARKET SHARE



90%
of internet search is controlled by Google²



99%
of mobile operating systems in the U.S. are made by Apple or Google³



63%
of online advertising revenue goes to Google and Facebook



94%
of social media users have a Facebook property account (e.g. Instagram, WhatsApp, etc.)⁴



75%
of ebooks are sold by Amazon



49%
of all online commerce is handled by Amazon⁵

BIG TECH MARKET DOMINANCE IS COMPARABLE TO THE LARGEST MONOPOLIES OF THE 20TH CENTURY

1904



87%

of all refined oil products were sold by Standard Oil

75%

of all digital computer installations were handled by IBM



1955



1980

75%

of local and nearly 100% of long distance phone calls were controlled by AT&T in the early 1980s⁶



1999

80%

of desktop operating systems were sold by Microsoft





BIG TECH

The Issues



Privacy

Most Americans know that large tech companies have a lot of data on them. But they don't know just how much, or how that knowledge is used.

STEP ONE

WHAT TECH COMPANIES KNOW ABOUT US

COMMUNICATION HISTORY

Google archives all emails sent and received, Facebook keeps a log of all Facebook Messenger chats, and Apple collects metadata from phone calls and text messages (not actual communication content, but who you contact and when).

WEB-SURFING ACTIVITY

Companies like Google, Facebook, and Amazon track our web page loads, even outside of their websites. In a study of 144 million page loads in 20 different countries, 64.4% were tracked by Google.⁷

LOCATION AND IP ADDRESSES

Facebook, Apple, and Google can track your location constantly, even when you are not using an app that explicitly requires location.

STEP TWO

WHAT THEY DO WITH THAT INFORMATION



USE FOR ADVERTISEMENTS

Tech companies use our personal data to enhance and customize their products, but their chief source of revenue entails using data to find better, more targeted ways to serve us advertisements. Analyzing our personal information allows companies like Facebook and Google to produce targeted advertisements and make billions of dollars even though their services are free.



SELL OUR DATA

While the major tech companies do not sell user data, 70% of the apps on iOS and Android smartphones share personal data with third party tracking companies. Several of the major cell phone carriers sell our location data to aggregation firms.⁸

PRIVACY

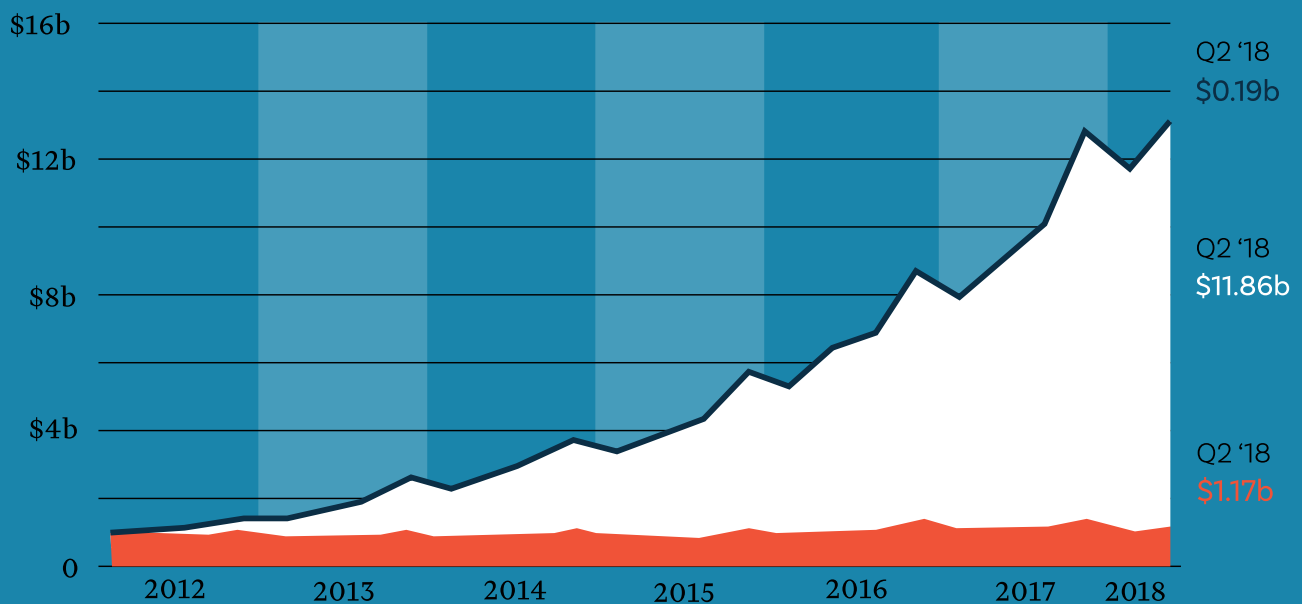
How Big Tech Benefits

ADVERTISEMENTS

Facebook's Growth is Fueled by Mobile Ads⁹

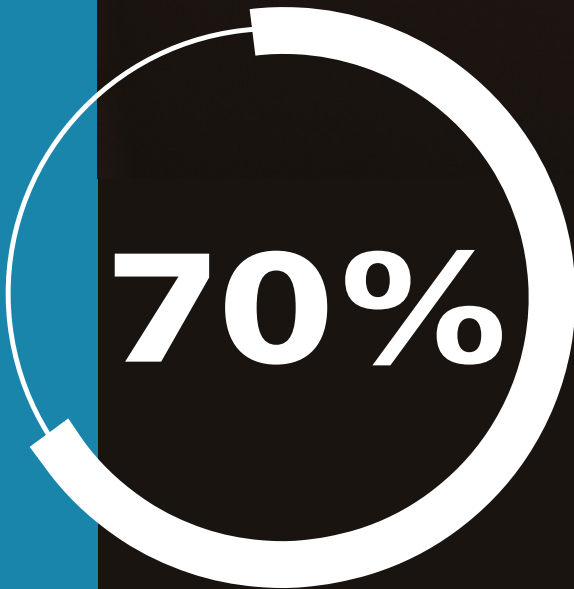
Facebook's quarterly revenue by segment

● Desktop Advertising ● Mobile Advertising ● Payments (In-App, e.g. Online Games)



Source: Facebook
StatistaCharts

SELLING DATA



of the apps on iOS and Android smartphones share personal data with third party tracking companies¹⁰

Who Regulates Your Data?



IN THE UNITED STATES

Privacy laws protect personal health and financial data, but personal online data is largely unregulated.

Various state laws attempt to regulate internet privacy, but tech companies have used lobbying power to prevent the passage of many of them. Additionally, many of the laws that have been passed are inconsistent with one another.

For example, while many states have enacted legislation related to online security breaches, some are preventative while others are reactive. California law mandates notification of a security breach to all affected customers. Other states, like Massachusetts, require preventative measures against security breaches but their laws do not specify what should be done if a breach actually occurs.¹¹



IN THE EUROPEAN UNION

The General Data Protection Regulation (GDPR) requires websites to disclose to their users which types of information they collect and how they use it.

Additionally, it requires companies to both obtain consent before collecting sensitive personal information and to delete information if a consumer wishes to be “forgotten.”

Obstacles to Protecting Your Data

For many websites, privacy is not the default. To protect information online, consumers must dig through confusing privacy settings.

Although sites like Facebook now feature pop-ups encouraging us to review our privacy settings, the choices can be overwhelming, and it is often easier and faster to skip through them.

Tech companies actively try to discourage us from protecting our personal information. Instead of allowing us to disable all data collection with one click, we must disable each type of data collection individually. Sometimes it takes more than one change to keep a single type of data private, and the options are not always intuitive.

EXAMPLE ONE: GOOGLE

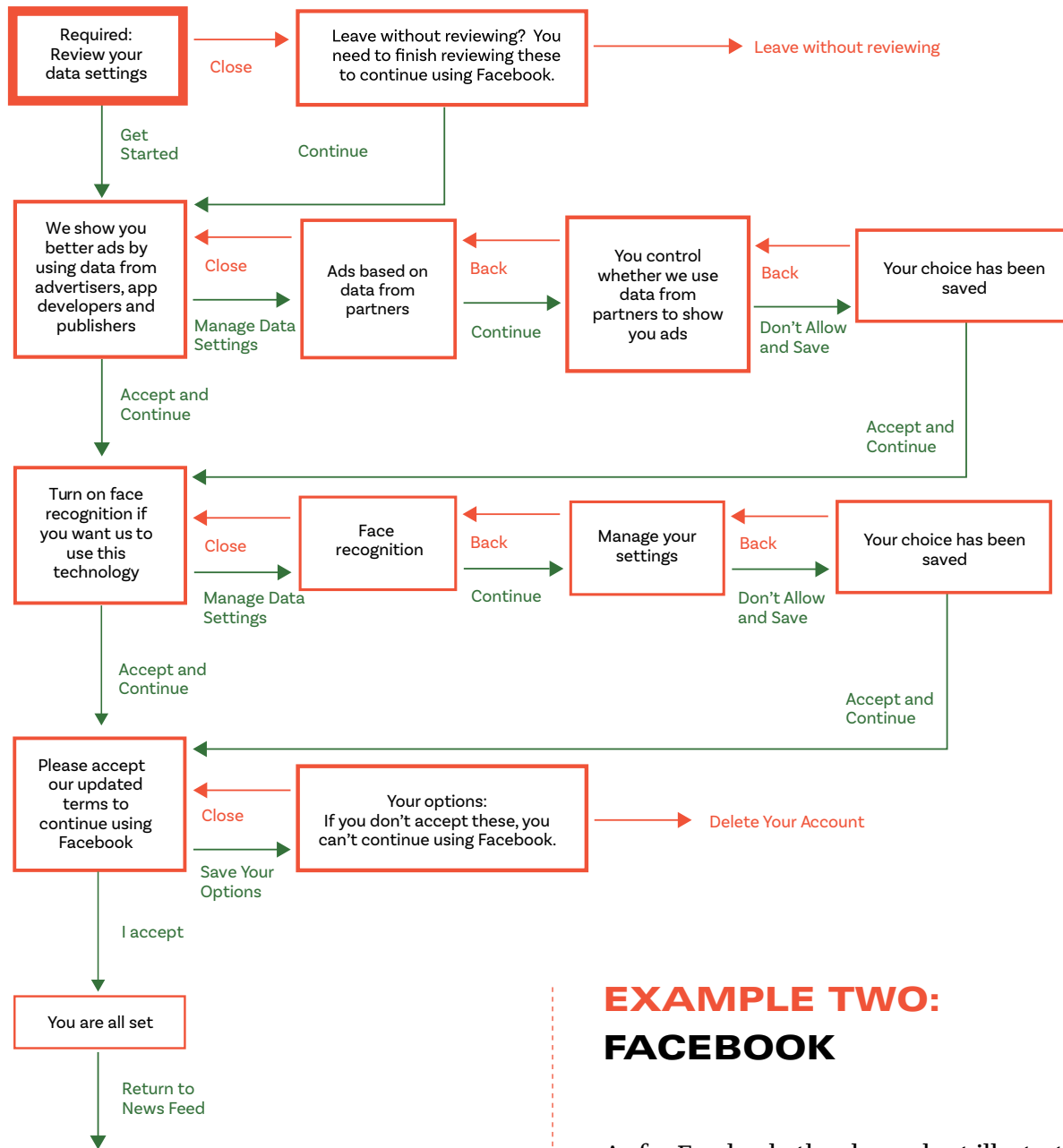


Google allows us to keep our location data private, but its privacy settings are misleading. Disabling the “location history” setting is not enough; another hidden setting, “web and app activity,” must also be disabled to prevent Google from tracking location.

To make your Google account completely private, you must disable the following settings:

- Web & App Activity
- Location History
- Device Information
- Voice & Audio Activity
- Youtube Search History
- Youtube Watch History
- Ad Personalization

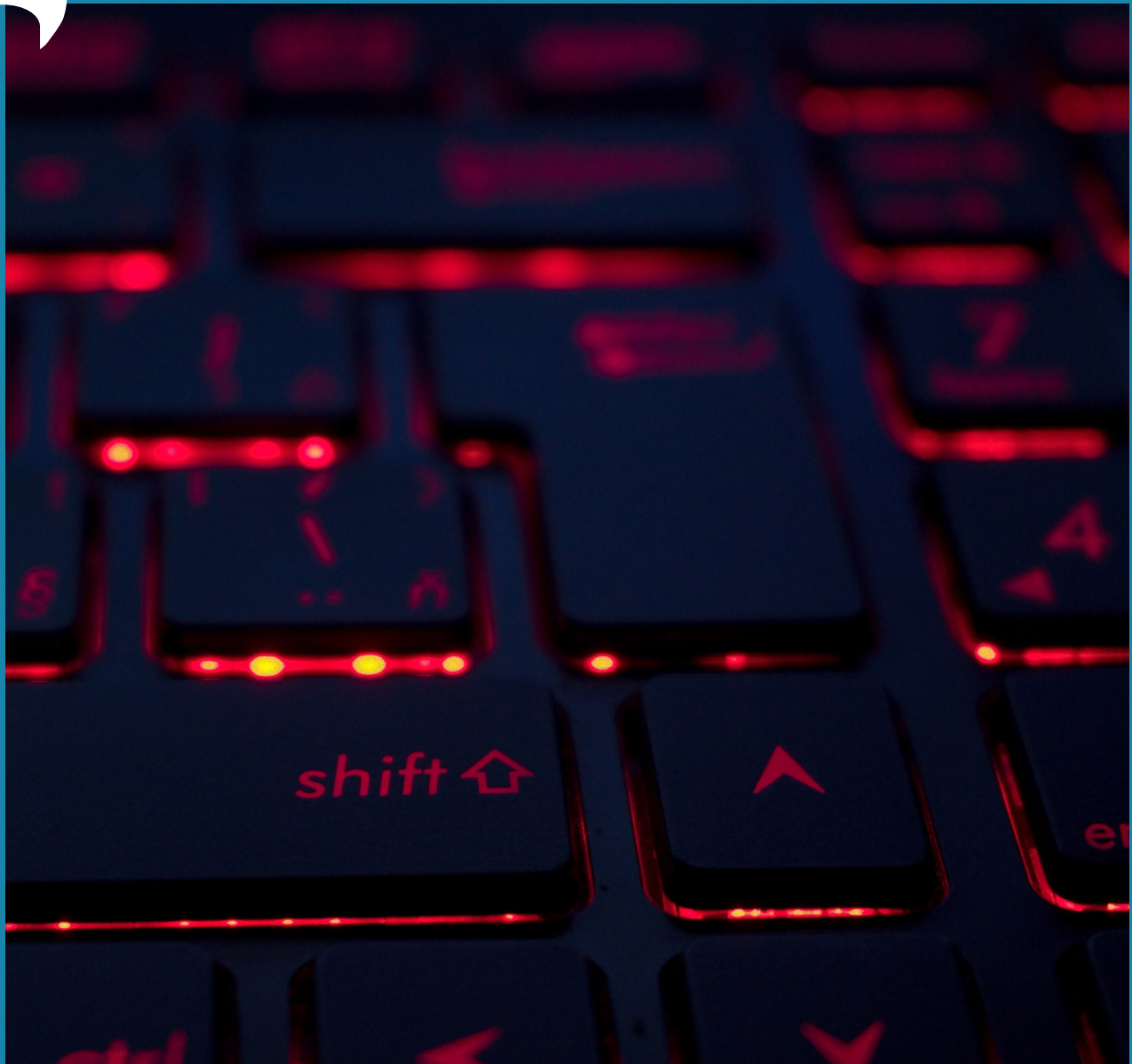
Steps to Review Facebook Privacy Settings¹²



EXAMPLE TWO: FACEBOOK



As for Facebook, the above chart illustrates the many steps involved in reviewing your Facebook privacy settings. If you choose to allow every type of data collection, it takes five clicks to return to the news feed and continue using Facebook. **If you choose to manage your data settings and deny access at each step, it takes eight additional clicks to return to Facebook.**



Public Discourse

FOR MOST OF OUR HISTORY, our public discourse has been governed by two clear guardrails.

GOVERNMENT

The First Amendment allows you say anything you want so long as you don't directly incite violence or promote dangerous obscenity. If you do, the government can arrest you.

THE PUBLIC

Private citizens can't stop you from saying something unless you defame or libel them. Then they can sue you.

BUT NOW, large technology companies are playing a more active role in promoting and policing the speech that happens between these two guardrails of our public discourse.

Some advocates encourage these companies to take greater action in monitoring their content, and to act as the gatekeepers of public discourse that restrict speech between the guardrails.

However, social media companies are not subject to the same rules and regulations as more traditional gatekeepers, like television and radio companies.

Social Media Is a News Destination

Social media platforms face pressure from both the left and right to do more to regulate their platforms in light of growing concerns about their potential to influence the American public. While their efforts to clean up their sites are undoubtedly well-intentioned, there are real challenges and problems involved in such an undertaking.

67%

of U.S. adults get news from social media, including 78% of those ages 18-49.¹³



45%

of U.S. adults get news on Facebook, making it the dominant social media platform for news consumption.

18%

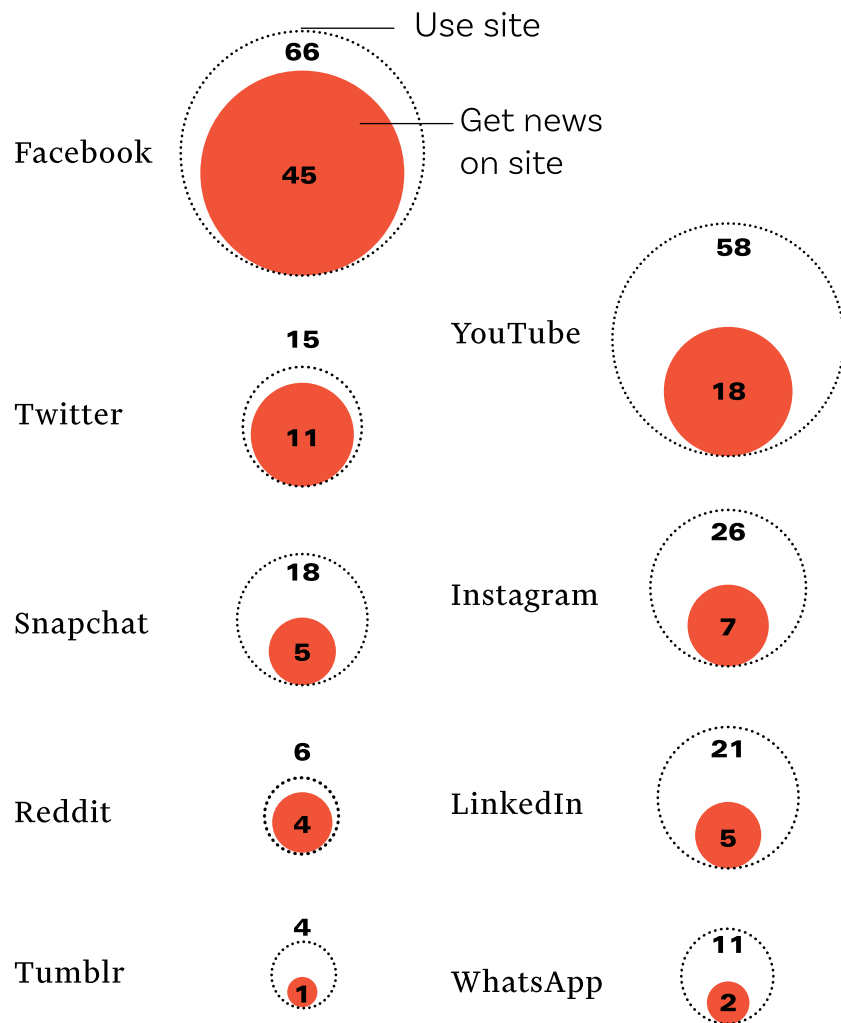
of adults use YouTube for news, making it the second largest platform.¹⁴

20%

of Americans reported they often get their news from social media.¹⁵ That number is comparable to print news (18%) and radio (25%), and while it still lags behind TV (50%), it forms a large part of a growing community of Americans often getting their news online in general (43%).¹⁶

Social media sites as pathways to news¹⁷

% of U.S. adults who use each social media site and % of U.S. adults who get news from each site



Source: Survey conducted Aug. 8-21, 2017
"News Use Across Social Media Platforms 2017"
Pew Research Center

PUBLIC DISCOURSE



20,000
MODERATORS

Regulating Huge Networks

YouTube has 1.8 billion monthly active users.¹⁸ Facebook is even larger at 2.23 billion,¹⁹ which includes 210 million in the United States.²⁰ These users generate massive amounts of content. Between 2015 and 2017, people in the United States saw more than 11 trillion posts from pages on Facebook.²¹ Even with the 20,000 content moderators that Facebook pledged to have on staff by the end of the year, it would be impossible to police its network with humans alone.

Big tech is turning to artificial intelligence for help. Facebook, Google, and other big tech companies are using AI systems to detect and flag content violations that aren't reported by

users or found by human moderators. Facebook reported that it took action on 837 million pieces of spam content from January-March 2018 alone.²² AI found and flagged nearly 100% of this content before it was reported by users.

While big tech companies currently employ AI in tandem with humans as back-ups, they aim to develop more advanced AI systems that in the future will have greater control over determining acceptable limits of speech among users.²³ Though AI undoubtedly has great potential, there are significant limitations on what it can monitor—and questions about what it should.



vs. **2.23**
BILLION
USERS

The Role of AI

AI systems cannot reliably evaluate meaning in human language.

They struggle to understand context, cultural norms, and regional slang, and make mistakes by flagging and removing content that humans wouldn't.²⁴ Some of these errors are innocuous; for example, in July, Facebook AI flagged and temporarily blocked a post for hate speech that contained part of the Declaration of Independence.²⁵ Some, however, are more concerning. Posts bringing attention to racist behavior²⁶ and humanitarian disasters have been taken down on Facebook and YouTube because AI systems detected hate speech and graphic violence.²⁷


AI can be gamed.

Algorithms trying to make sense of human language rely on key words and patterns, and as a result can be gamed by bad actors who, over time, figure out words to avoid or masking patterns to include to escape detection.²⁸

AI can become biased, and we're only beginning to understand how.

Algorithms that learn from biased trends in data will retain such bias, often in ways that developers don't predict—including adopting racist or sexist tendencies.²⁹ Bias in an AI moderator presents the danger of over-censoring certain communities, groups, and viewpoints.





No Clear Code of Conduct

Social media lacks clear and consistent standards for online behavior. Despite the efforts they've made to clean up their platforms, some big tech companies struggle to enforce those standards consistently and transparently. Notably, Facebook expanded its community standards in April 2018 to definitively outlaw hate speech, yet months later over a thousand anti-Rohingya posts from Myanmar that violated those standards for hate speech were still found on the site.³⁰

Questions about accountability remain.

What happens when Facebook or another big tech company gets it wrong and fails to uphold its own standards? What oversight is there to make sure company standards are appropriate and don't result in over-censorship? To both questions, the answer is: not much. Internet companies are largely protected in this sphere by a provision called Section 230, which is part of legislation passed in 1996. See page 39 for more details.

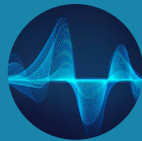


Threats on the Horizon

America is having a tough time navigating the current challenges at the intersection of technology, privacy, and public discourse. But future challenges are even more daunting.

Big tech companies are constantly introducing innovative new products and services that can impact society deeply in a matter of months. As a result, the consequences of innovation should continuously be evaluated. Recent technological innovations that should be monitored include fake audio and video, hacking threats to cybersecurity, facial recognition tech, and anonymous encrypted communication.

FAKE AUDIO & VIDEO



DeepFake is a technology that can create artificial but strikingly realistic videos of individuals performing compromising actions or saying things they never actually did.³¹ AI bots can use sophisticated voice technology to mimic existing human voices³² or create entirely new ones, fooling people into thinking they're real.³³ In the hands of bad actors, these technologies are the future of fake news.

FACIAL RECOGNITION



In recent years, several of the major tech companies have developed their own facial recognition technologies to identify individuals. They have also shared the software with other parties, such as law enforcement agencies. While facial recognition is useful for cataloging faces on social media and identifying criminals, advances in the technology and expansion of its use across many sectors could lead to civil liberties concerns.

CYBERSECURITY

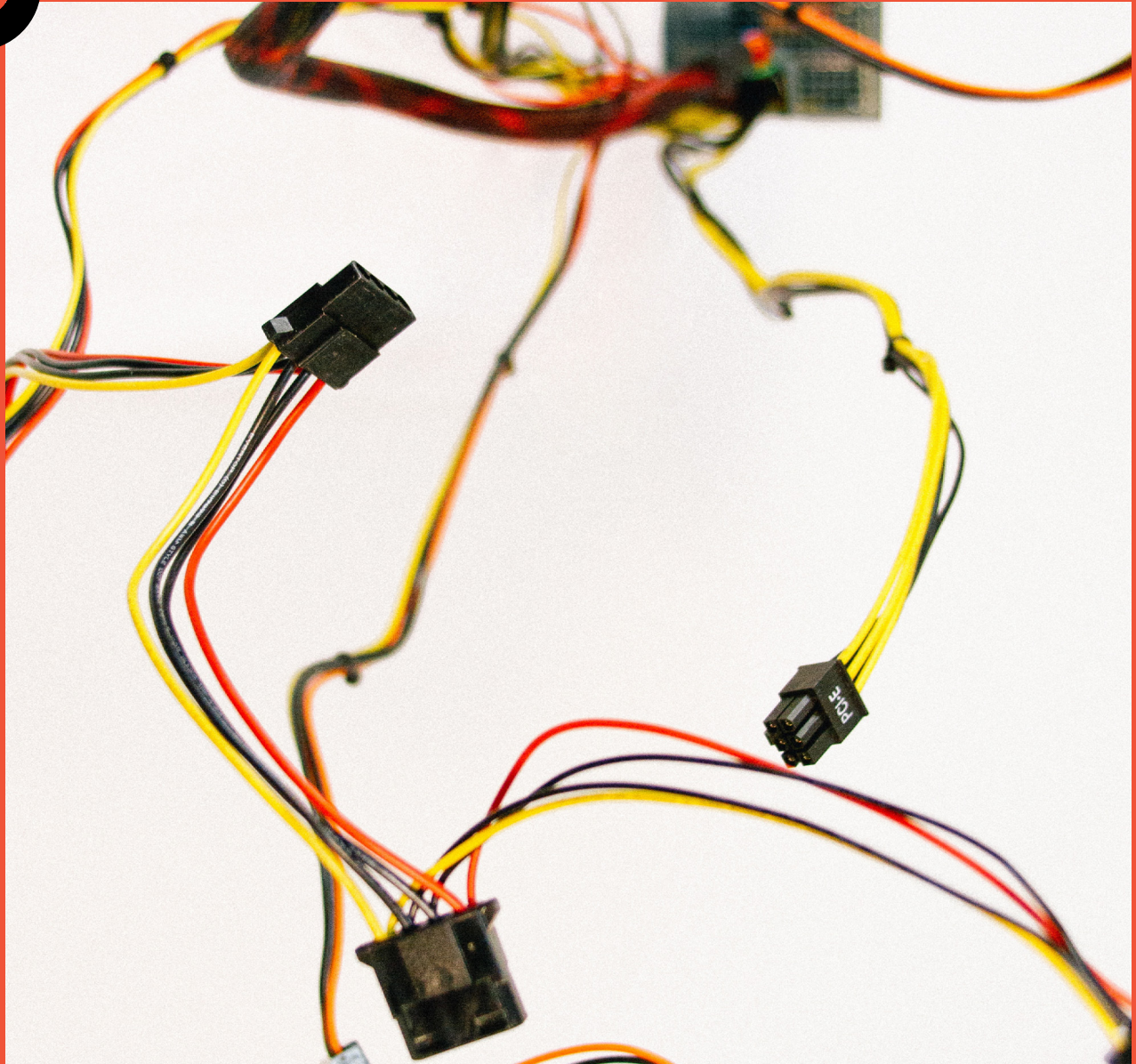


As the amount of user data collected by big tech companies increases, the threat of a data breach does too. The recent Cambridge Analytica scandal gave a third party access to 87 million Facebook users' data without their explicit consent.

FAKE NEWS ON ENCRYPTED APPS



WhatsApp, a Facebook-owned instant messaging platform with 450 million users worldwide, allows for encrypted communication that only the sender and the receiver can read. It is being used to stoke religious, ethnic, and racial tensions through rumors that spread via group messages to wide audiences.³⁴ The encryption can protect perpetrators from detection by moderators and shield them from government prosecution for inciting violence.



Accountability

The Rosetta Stone of Internet Regulation

The most consequential regulation governing the activities of big tech companies is arguably Section 230 of the 1996 Communications Decency Act. But what is it?

Section 230 gives broad protections to ‘interactive computer services’—including social media sites and search engines—from liability for content posted by third parties.³⁵ Essentially, the law states that because websites aren't publishers, they aren't legally responsible for the content of their users. For example, if a customer posts a negative restaurant review on a website like Yelp, the restaurant cannot sue Yelp for damages.

However, just because websites aren't liable for their users' content doesn't mean they can't regulate it. Section 230 also gives online platforms the power to engage in content moderation however they see fit, as long as it is in “good faith.”³⁶ This good faith protection is broad; it invests authority in the individual websites to make judgments about which content is or isn't acceptable—even content protected under the First Amendment.

Section 230 has been hugely important in shaping the modern internet. Social media platforms like Facebook, online streaming services like YouTube, and collaborative review forums like Yelp would have struggled to develop if they were liable to be sued for each and every one of their users' posts.

In public, big tech companies like Facebook have historically maintained that they are “platforms”—i.e. interactive computer services hosting third party content—rather than “publishers.” This is key to the protection they receive from the law. However, lawyers for Facebook recently made a contradictory claim: that the company is in fact a “publisher” whose editorial decisions are protected by the First Amendment.³⁷ If Facebook is indeed a publisher of original content, then it could become legally responsible for the content on its platform.

Where the Left and Right Might Actually Be Able to Come Together



Many issues in U.S. politics have created seemingly unbridgeable divisions between the left and right.

But the concentrated power of technology companies—and their influence on Americans’ public discourse and privacy—is an exception. Both sides are concerned, even if for different reasons.

In the wake of the 2016 election, both political parties have voiced concerns about the management of tech platforms.³⁸ While the left demands accountability³⁹ for fake news, the right rails against what they believe to be anti-conservative censorship.⁴⁰

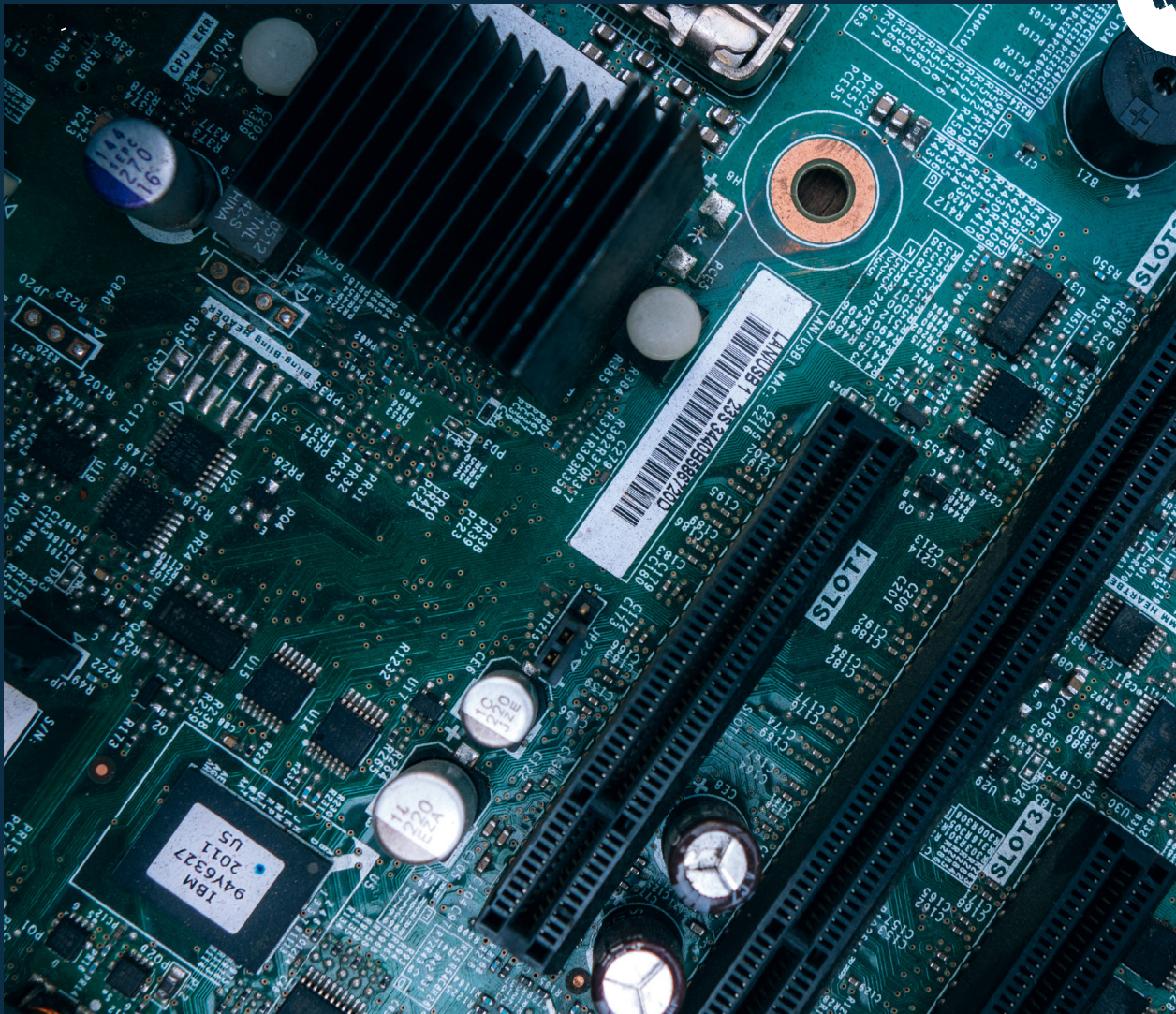
Bipartisan concern about the practices of tech companies has created openings for cooperation in Congress, including the recent passage of the Stop Enabling Sex Traffickers Act (SESTA) and the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA). These make it illegal to knowingly assist, facilitate, or support sex trafficking, and they revise the legal protection of Section 230 by making tech companies liable if third parties place ads for prostitution on their platforms. But even this step forward poses unintended consequences; digital advocacy groups have criticized the bill for increasing tech companies’ liability for user content, creating potential for broader online censorship.

Congress is making a greater effort to hold tech companies accountable, as evidenced by invitations to executives from Amazon, Apple, Google, and Facebook to testify before various committees. Still, Washington has unquestionably fallen behind in tackling some of the thorniest

issues. To cite just one example, over 80 countries and independent territories around the world exercise a federal framework of data privacy legislation. The United States is not one of them.

In short, Congress must show purpose and unity by pushing tech companies to develop a more sustainable and consistent framework for the challenges posed to our privacy and public discourse. If tech companies aren’t up to the challenge, then Congress may need to take more decisive regulatory action.





Public Opinion on Big Tech

The public generally believes big tech companies have a positive impact on society and the economy, but these views vary by company, and net favorability is declining for each company surveyed.

GOOD FOR THE WORLD?

58%

believed that Google is good for the world.

32% of respondents believed Facebook is good for the world, and 20% of respondents believed that Twitter is good for the world.⁴¹

Harvard-Harris Poll, August 2018

DECREASE IN FAVORABILITY

In a poll conducted by Axios between October 2017 and March 2018, the net changes in favorability for major tech companies were found to have decreased significantly.

- Facebook fell 28% (from +33 to +5),
 - Amazon fell 13% (from +72 to +59),
 - Google fell 12% (from +76 to +64),
 - Apple fell 10% (from +50 to +40),
 - Microsoft fell 3% (from +62 to +59)⁴²
-

ETHICAL?

69% of Americans said tech companies are no more or less ethical than companies in other industries.

PERSONAL VS. SOCIETAL

Additionally, they found that 74% of Americans said major tech companies and their products and services have had more of a positive than a negative impact on their own lives, whereas 63% of Americans said major tech companies and their products and services have had more of a positive than a negative impact on society as a whole.⁴³

The Pew Research Center, June 2018

PUBLIC OPINION



DATA PRIVACY

In light of revelations surrounding the data collection practices of big tech companies, public concern has grown as to whether these firms can keep user data private. According to a June 2018 poll from Pew Research Center, 75% of the public thought major tech firms weren't doing enough to protect the personal data of their users.⁴⁴ Of all the major tech companies surveyed, the public believed Facebook was the least trustworthy. An April 2017 Morning Consult survey found that 61% of responders didn't trust Facebook to keep their personal information private.⁴⁵



DATA MISUSE

In addition to concerns over the privacy of personal information, Americans are increasingly worried about the ways in which their data can be used—or misused—by tech companies. This is particularly true for data sold to third parties.

77% of respondents to a Morning Consult poll from April 2017 were uncomfortable with tech companies selling personal data to third parties for advertising purposes, 61% were against tech companies using personal data to advertise themselves, and 57% were against the use of personal data for research purposes.⁴⁶

Interestingly, fear of personal data misuse appears to vary by company.

PUBLIC OPINION



75%

of the public thought major tech firms weren't doing enough to protect the personal data of their users.

Pew Research Center, June 2018

61%

of responders didn't trust Facebook to keep their personal information private.

Morning Consult survey, April 2017

56%

of respondents identified Facebook as the company they trusted the least with their personal information. The second most popular choice was Google at 5%.⁴⁷

Recode survey, April 2018



POLITICAL BIAS AND CENSORSHIP

Big tech's influence over public internet discourse has sparked a debate in the American public over bias, censorship, and how much of a role the government should have in policing big tech's policies on internet speech. A majority of Americans (53%) were concerned with online censorship by humans and AI bots, according to the August 2018 Harvard-Harris poll.⁴⁸ Pew Research reported that 72% of the public thought it likely that social media platforms were actively censoring political views that those companies found objectionable.⁴⁹ 63% of Americans believed tech was doing more to justify these biased decisions than to remove bias from the decision-making process.⁵⁰

The American public appears to be in favor of specifying the types of content that tech companies can remove. 55% of responders to the August 2018 Harvard-Harris poll believed that tech and social media companies should only take down material that violates the First Amendment by advocating imminent lawless action and social violence, or material that falls outside community standards of decency.⁵¹ 69% of respondents favored a constitutional amendment that would guarantee free speech online.⁵²



55%

of the public believed tech companies have too much power and influence.

The Pew Research Center, June 2018

Big tech companies have quickly become integral to the U.S. economy since the creation of the internet, and they have benefited from relaxed government regulatory standards safeguarding the new industry. The importance of these companies in our everyday lives and their failure to self-regulate have led to a debate about the proper amount of regulation needed to keep public discourse civil and privacy protected.

In a HarrisX poll conducted in April of 2018, 84% of respondents thought that technology companies should be held legally responsible for the content on their systems, while 83% of respondents thought there should be tougher regulations and penalties for breaches of data privacy. In the same poll, there was overwhelming support for the major online privacy and security legislation currently being considered in the U.S. and Europe (67% in support of the Consent Act, 67% in support of the EU's General Data Protection Regulation).⁵³

In a Pew Research Center poll conducted in June of 2018, 51% of the public (44% of right-leaning, 57% of left-leaning individuals) believed that major tech companies should be regulated more than they are now.⁵⁴ In the more recent August 2018 poll from Harvard-Harris, 64% of respondents believed that tech companies should be held legally accountable for the content posted on their sites through libel and other laws.⁵⁵



Policy Solutions

Despite the significant threats that large tech companies increasingly pose to American privacy and public discourse, Washington needs to be smart about how it implements expansive new federal regulations—if it chooses to do so.

For starters, innovation in the tech space is accelerating, and the regulations Congress might implement today could be ill-equipped to address the problems the public will face tomorrow (such as the rise of artificial intelligence).

Washington must also be mindful that American tech companies are the crown jewels of American innovation, fueling economic growth, investment, and job creation. Ill-advised regulation could fail to preserve privacy, do little to improve public discourse, and hurt American tech companies—providing an opportunity for foreign firms, like those in China, to out-compete them.

Finally, many key decision-makers in Congress still don't seem to grasp the complexities of how the tech industry or the internet works. At Mark Zuckerberg's Senate committee hearing in early 2018, at least one senator did not appear to understand how the company made money.

Are these the people we want micromanaging the future of the tech industry in America? Probably not.

But self-regulation doesn't always work, and the federal government does have a "hammer" available to force the tech industry to do the right thing. This could include revoking liability protection under Section 230 of the Communications Decency Act as well as pursuing more aggressive anti-trust enforcement.

A government crack-down on tech companies is an outcome we should hope to avoid. But these firms owe it to their customers and to the public to do more, now, to protect our privacy and safeguard our discourse from censorship.

PUBLIC OPINION



64%

believed that tech companies should be held legally accountable for the content posted on their sites through libel and other laws.

Harvard-Harris Poll, August 2018

1.

Toward Real Transparency

**PUBLIC
OPINION**



53%

were concerned with censorship
online by humans and bots.

72%

of the public thought it likely
that social media platforms
actively censor political views
that those companies find
objectionable.

Pew Research Center, June 2018



Large tech companies claim they are being more transparent with respect to how they handle our data and decide which content can exist on their platforms. But often, they just provide the illusion of compliance with long, impenetrable terms of service and standards that no one reads.

At minimum, large tech companies should agree upon and adhere to common standards that establish a clear, standardized process of review for the material they remove.

THIS WOULD INCLUDE:

■ Meaningful Notice

Anyone whose content is removed from an online platform should be provided:

- A notice from the platform about the community standard violated
- A copy of the specific language violating the standard
- A characterization of who reported the post; i.e. whether it was a government, fellow user, or automated system

■ Appeal

Users should have the recourse to appeal any content takedown, and that appeal should be examined by a human or panel of humans who weren't involved in the original decision.

■ Regular Reports

Tech platforms should make regular reports available to the public that detail the amount and types of content were removed, which community standards were violated, and whether content was flagged by a user, human moderator, or bot.

■ Pay the People Who Are Harmed

Tech companies often have to pay fines to the government for misbehavior, but customers never see any of it. Customers who have their content taken down suffer real harm, and they should be compensated for it. If tech companies agreed to pay a small fine to each customer for each day their content was unjustifiably taken down, they might just do it less often.

*Note: A number of these recommendations are drawn from the Santa Clara Principles on Transparency and Accountability in Content Moderation, developed by technology policy academics and nonprofit organizations including the ACLU, the Electronic Frontier Foundation, and the Center for Democracy and Technology.⁵⁶

2.

Legislation to Protect Online Data Privacy



**PUBLIC
OPINION**



75%

of the public believed major tech firms were not doing enough to protect the personal data of their users.

Pew Research Center, June 2018

Large tech companies have every incentive to collect as much personal data as possible from their consumers. Comprehensive federal privacy legislation should be enacted to give consumers more control over their personal data.

Legislation should grant rule-making and enforcement authority to the FTC so that regulations can be updated as necessary without a complete legal overhaul.

THE LAW SHOULD INCLUDE THE FOLLOWING PROVISIONS:

■ The “Right to Be Forgotten”

The option to remove your personal data from an online platform’s database should be available for users who want to keep their personal data from being further disseminated to and accessed by third parties.

■ Opt-Out Mechanisms for Data Sales and Third-Party Data Use

Customers should have the option to withdraw consent and prevent internet companies from selling their information or using it for targeted advertising.

■ Data Collection Disclosure

Internet companies should be required to explicitly disclose to consumers information about the types of personal data they collect, how they use that data, and the types of third parties with whom they may share the data.

■ Right to Access Personal Data

Consumers should have the ability to request from an internet company a copy of all personal data collected by that company, and the company should be required to provide that information via a file download.

■ Prompt Data Breach Notification

Internet companies should be required to notify all affected consumers in the case of a data breach within 72 hours (identical to the data breach notification provision in the GDPR) so that further harm can be mitigated.

PUBLIC OPINION



67%

of respondents supported the European Union’s GDPR, which includes the right to be forgotten as a major provision.

HarrisX Poll, April 2018

61%

were uncomfortable with tech companies using personal data for their own advertising purposes.

77%

were uncomfortable with tech companies selling their data to third parties for their advertising purposes.

Morning Consult Poll, April 2017

83%

of Americans thought we need tougher regulations and penalties for breaches of data privacy.

Harris X Poll, April 2018

3. Algorithmic Accountability

Tech companies are using artificial intelligence (AI) to screen reams of content across their platforms. However, these systems too often make wrong decisions, and tech companies, given their market dominance, are giving their users little to no choice to accept or refuse them. AI should be subject to regulation, and big tech should be legally obligated to minimize any injury their algorithms could cause users. AI is not a person but a collection of code, and tech companies should be required to disclose life and death decision-making rationales and whether bots are programmed to sell products or have consumers' best interests at heart.

The Center for Data Innovation recently unveiled a legal framework for the regulation of AI systems on the principle of 'Algorithmic Accountability'.⁵⁷ The FTC could draw on this framework to enact a system of standards for the use of AI in moderating online public discourse.



SUCH A SYSTEM COULD REQUIRE:

■ Legal Responsibility for the Operator

Liability for a faulty algorithm should not lie with individual developers, who cannot reasonably be expected to predict with complete accuracy the behavior of an algorithm that interacts with billions of users. Instead, the companies using the algorithm should bear legal responsibility, and firms should implement checks and standards to ensure the algorithm functions as intended.

■ Liability For Consumer Injury

The FTC could consider cases of unnecessary censorship of users by algorithms on the existing basis of consumer injury through unfair business practices. In particular, the FTC should focus on cases of demonstrable negligence of tech companies to ensure algorithms are working as intended, to maintain transparency with respect to their AI operations, and to identify and redress instances of improper censorship.

■ High Standards

AI systems in development should be able to demonstrate low degrees of error before their use, and should be recalled and reevaluated if they can't continue to meet these standards. Confidence intervals should also be used in cases in which algorithms make decisions independent of human supervision.

- For example, a Facebook bot should not remove content unless it is at least 95% sure that content is in violation of a community standard.

■ Transparency

When introducing new AI technologies, companies should conduct impact assessments similar to those outlined by New York University's AI Now Institute.⁵⁸

- These assessments should test algorithms for bias, logical errors, and discrimination on the basis of race, gender, ethnicity, or political belief.
- These impact assessments should happen before

launch and in regular intervals after launch, and the results of these assessments should be made available to the public for review.

■ Audits

Tech companies should make algorithms and training data available for third-party teams of experts to audit for bias or flawed decision-making upon a request granted by the FTC.

- A safeguard system should be enacted to prevent the leak of classified intellectual property.

■ Due Process

Users should be notified if their content has been flagged by AI, and should be entitled to an explanation of the AI's decision. An option to appeal biased or otherwise unfair decisions should be available to users.

■ Clarity in Design

Some deep-learning algorithms are so complicated that even the engineers who built them cannot understand their decision-making process. This should never be the case for automated systems deciding the limits of acceptable online public discourse; if the operator of an AI bot cannot explain why the bot censored a user's content, that content should be re-instated immediately and the operator subject to penalty.

■ Penalties for Not Fixing Bad Outcomes

Tech companies should be able to demonstrate to regulators that incorrect decisions from AI systems are remedied as quickly as possible. Larger patterns of error should be investigated in a timely manner. Failure to do so should result in a significant fine.

4.

Congress Needs to Get Smart on Tech



In 1995, the new Republican House majority eliminated the congressional Office of Technology Assessment, which was supposed to provide unbiased information about science and technology to Congressional leadership. Considering the 115th Congress only had one PhD scientist and a major lack of tech and science understanding, this office should be reopened in the next Congress. When and if Congress needs to pass new tech regulation, it should get up to speed on what's really happening.

5.

Platform Companies Need to Act Like Platform Companies



If large tech companies like Facebook and Google are indeed platform companies and not publishers, as they claim, then they need to act like it. That means that in developing content policies for what can exist on their platforms, they should hew closely to the First Amendment as articulated by the U.S. Supreme Court: speech should be free unless inciting violence or promoting dangerous obscenity.

BIG TECH

PUBLIC OPINION



64%

of Americans supported regulating Facebook like a traditional media company if it continued to distribute news.

HarrisX Poll, April 2018

55%

of respondents to the August Harvard-Harris poll believed tech and social media companies should only take down material that violates the First Amendment by advocating imminent lawless action and social violence, or material that is outside community standards of decency.

69%

favored a constitutional amendment that would guarantee free speech online.

Harvard-Harris Poll, August 2018

Sources

Sources

- 1 Popper, B. (2017, 17 May). "Google Announces over 2 Billion Monthly Active Devices on Android." Retrieved from <https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users>
- 2 Statcounter (2018). "Search Engine Market Share Worldwide". Retrieved from <http://gs.statcounter.com/search-engine-market-share>
- 3 Statista (2018). "Subscriber share held by smartphone operating systems in the United States from 2012 to 2018." Retrieved from <https://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/>
- 4 Ip, G. (2018, 16 January). "The Antitrust Case Against Facebook, Google, and Amazon." Retrieved from <https://www.wsj.com/articles/the-antitrust-case-against-facebook-google-amazon-and-apple-1516121561>
- 5 Lunden, I. (2018, 13 July). "Amazon's Share of the US E-commerce Market Is Now 49%, or 5% of All Retail Spend". Retrieved from <https://techcrunch.com/2018/07/13/amazons-share-of-the-us-e-commerce-market-is-now-49-or-5-of-all-retail-spend/>
- 6 Federal Communications Commission, Common Carrier Bureau, Industry Analysis Division (2001, August). "Trends in Telephone Service". Retrieved from https://transition.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/trend801.pdf
- 7 Richter, F. (2017, 12 December). "They Know What You Clicked Last Summer." Retrieved from <https://www.statista.com/chart/12236/reach-of-companies-tracking-online-behavior/>
- 8 Barrett, B. (2018, 19 May). "A Location-Sharing Disaster Shows How Exposed You Really Are." Retrieved from <https://www.wired.com/story/locationsmart-securus-location-data-privacy/>
- 9 Richter, F. (2018, 26 March). "Facebook's Growing Stature in the Online Ad Market". Retrieved from <https://www.statista.com/chart/13348/facebook-share-of-global-online-ad-revenue/>
- 10 Vallina-Rodriguez, N. and Sundaresan, S. (2017, 29 May). "7 in 10 Smartphone Apps Share Your Data With Third Party Services." Retrieved from <https://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404>.
- 11 Jolly, I. (2017, 1 July). "Data Protection in the United States: Overview." Retrieved from [https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=\(sc.Default\)&transitionType=Default&firstPage=true&bhcp=1](https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1)
- 12 Forbrukerrådet, (2018, 27 June). "Deceived by Design: How Tech Companies use Dark Patterns to Discourage us from Exercising our Rights to Privacy." Retrieved from <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>
- 13 Gottfried, J. and Shearer, E. (2017, 7 Sept.). "News Use Across Social Media Platforms 2017". Retrieved from <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/>
- 14 Gottfried, J. and Shearer, E. (2017, 7 Sept.). "News Use Across Social Media Platforms 2017". Retrieved from <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/>
- 15 Gottfried, J. and Shearer, E. (2017, 7 Sept.). "News Use Across Social Media Platforms 2017". Retrieved from <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/>
- 16 Gottfried, J. and Shearer, E. (2017, 7 Sept.). "Americans' Online News Use is Closing in on TV News Use". Retrieved from <http://www.pewresearch.org/fact-tank/2017/09/07/americans-online-news-use-vs-tv-news-use/>
- 17 Gottfried, J. and Shearer, E. (2017, 7 Sept.). "News Use Across Social Media Platforms 2017". Retrieved from <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/>
- 18 Gilbert, B. (2018, 4 May). "YouTube Now Has 1.8 Billion Users Every Month, Within Spitting Distance of Facebook's 2

- Billion.” Retrieved from <https://www.businessinsider.com/youtube-user-statistics-2018-5>
- 19 Statista. (2018). "Number of Monthly Facebook Users Worldwide as of 2nd Quarter 2018 (in Millions)." Retrieved from <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>
- 20 Statista (2018). “Leading Countries Based on Number of Facebook Users As Of July 2018”. Retrieved from <https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/>
- 21 Isaac, M. And Wakabayashi, D. (2017, 30 Oct.) “Russian Influence Reached 126 Million Through Facebook Alone.” Retrieved from <https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html>
- 22 Facebook. (2018). "Community Standards Enforcement Preliminary Report." Retrieved from <https://transparency.facebook.com/community-standards-enforcement>
- 23 Harwell, D. (2018, 11 April). "AI Will Solve Facebook’s Most Vexing Problems, Mark Zuckerberg Says. Just Don’t Ask When or How.” Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/ai-will-solve-facebooks-most-vexing-problems-mark-zuckerberg-says-just-dont-ask-when-or-how/?utm_term=.dd445a97a440
- 24 Harwell, D. (2018, 11 April). "AI Will Solve Facebook’s Most Vexing Problems, Mark Zuckerberg Says. Just Don’t Ask When or How.” Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/ai-will-solve-facebooks-most-vexing-problems-mark-zuckerberg-says-just-dont-ask-when-or-how/?utm_term=.dd445a97a440
- 25 Sandler, R. (2018, 5 July). "Facebook has Apologized for Flagging Parts of the Declaration of Independence as Hate Speech.” Retrieved from https://www.businessinsider.com/facebook-declaration-of-independence-hate-speech-2018-7?utm_content=buffer962af&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer-bi
- 26 Guynn, J. (2017, 3 Aug.). "Facebook Apologizes to Black Activist who was Censored for Calling out Racism.” Retrieved from <https://www.usatoday.com/story/tech/2017/08/03/facebook-ijeoma-oluo-hate-speech/537682001/>
- 27 Asher-Schapiro, A. (2017, 2 Nov.). "YouTube and Facebook are Removing Evidence of Atrocities, Jeopardizing Cases against War Criminals.” Retrieved from <https://theintercept.com/2017/11/02/war-crimes-youtube-facebook-syria-rohingya/>
- 28 Harmon, E. and Gillula, J. (2017, 13 Sept.). "Stop SESTA: Whose Voices will SESTA Silence?” Retrieved from <https://www.eff.org/deeplinks/2017/09/stop-sesta-whose-voices-will-sesta-silence>
- 29 Buranyi, S. (2017, 8 Aug.). "Rise of the Racist Robots - how AI is Learning all our Worst Impulses.” Retrieved from <https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses>
- 30 Stecklow, S. (2018, 15 Aug.). "Why Facebook is Losing the War on Hate Speech in Myanmar.” Retrieved from <https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/>
- 31 Dvorsky, G. (2018, 12 June). "Deepfake Videos are Getting Impossibly Good.” Retrieved from <https://gizmodo.com/deepfake-videos-are-getting-impossibly-good-1826759848>
- 32 Lomas, N. (2017, 25 April). "Lyrebird is a Voice Mimic for the Fake News Era.” Retrieved from <https://techcrunch.com/2017/04/25/lyrebird-is-a-voice-mimic-for-the-fake-news-era/>
- 33 Leviathan, Y. and Matias, Y. (2018, 8 May). “Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone.” Retrieved from <https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html>
- 34 The Economist, (2018, 26 July), "WhatsApp Suggests a Cure for Virality”, Retrieved from <https://www.economist.com/leaders/2018/07/26/whatsapp-suggests-a-cure-for-virality>
- 35 Legal Information Institute. “47 U.S. Code 230 - Protection for private blocking and screening of offensive material.” Retrieved from <https://www.law.cornell.edu/uscode/text/47/230>
- 36 Legal Information Institute. “47 U.S. Code 230 - Protection for private blocking and screening of offensive material.” Retrieved from <https://www.law.cornell.edu/uscode/text/47/230>
- 37 Levin, S. (2018, 3 July). "Is Facebook a Publisher? In Public it Says No, but in Court it Says Yes.” Retrieved from <https://www.theguardian.com/technology/2018/jul/02/facebook-mark-zuckerberg-platform-publisher-lawsuit>

- 38 Samuels, B. (2017, 1 Nov.). "Feinstein to Tech Execs: 'I Don't Think You Get It.'" Retrieved from <http://thehill.com/business-a-lobbying/358232-feinstein-to-tech-cos-i-dont-think-you-get-it>
- 39 McCabe, D. (2018, 30 July). "Warner Suggests 20 Ways Democrats Could Crack Down On Big Tech". Retrieved from <https://www.axios.com/mark-warner-google-facebook-regulation-policy-paper-023d4a52-2b25-4e44-a87c-945e73c637fa.html>
- 40 Gold, A. (2018, 8 July). "GOP Thinks Bashing Big Tech Companies Will Rally Base". Retrieved from <https://www.politico.com/story/2018/07/08/republicans-midterm-social-media-bias-strategy-659634>
- 41 Harvard CAPS & The Harris Poll. (2017, Oct.) "Crosstabs, Monthly Harvard-Harris Poll: October 2017." Retrieved from https://harvardharrispoll.com/wp-content/uploads/2017/11/HCAPS-October_Topline-Memo_with-banners_Registered-Voters-Social-Media.pdf
- 42 Hart, K. and Fried, I. (2018, 26 March). "Exclusive Poll: Facebook Favorability Plunges." Retrieved from <https://www.axios.com/exclusive-poll-facebook-favorability-plunges-1522057235-b1fa31db-e646-4413-a273-95d3387da4f2.html>.
- 43 Smith, A. (2018, 28 June). "Public Attitudes Toward Technology Companies." Retrieved from <http://www.pewinternet.org/2018/06/28/public-attitudes-toward-technology-companies/>.
- 44 Ibid.
- 45 Nasr, A. (2017, 10 April). "Poll: Little Trust that Tech Giants Will Keep Personal Data Private." Retrieved from <https://morningconsult.com/2017/04/10/poll-little-trust-tech-giants-will-keep-personal-data-private/>.
- 46 Ibid.
- 47 Molla, R. (2017, 10 April). "Facebook is the Least-Trusted Major Tech Company." Retrieved from <https://www.recode.net/2018/4/10/17220060/facebook-trust-major-tech-company>.
- 48 Harvard CAPS & The Harris Poll (2018, Aug.). "Crosstabs, Monthly Harvard-Harris Poll: August 2018". Retrieved from: https://harvardharrispoll.com/wp-content/uploads/2018/08/Final_HHP_Aug2018_RegisteredVoters_Crosstabs_Memo.pdf
- 49 Smith, A. (2018, 28 June). "Public Attitudes Toward Technology Companies". Retrieved from: <http://www.pewinternet.org/2018/06/28/public-attitudes-toward-technology-companies/>
- 50 Bellstrom, K. (2018, 20 July). "70% of Americans Think Technology Increases People's Bias". Retrieved from: <http://fortune.com/2018/07/20/technology-inherent-bias/>
- 51 Harvard CAPS & The Harris Poll (2018, Aug.). "Crosstabs, Monthly Harvard-Harris Poll: August 2018". Retrieved from: https://harvardharrispoll.com/wp-content/uploads/2018/08/Final_HHP_Aug2018_RegisteredVoters_Crosstabs_Memo.pdf
- 52 Ibid.
- 53 HarrisX (2018, April). "Inaugural Tech Media Telecom Pulse Survey 2018". Retrieved from http://harrisx.com/wp-content/uploads/2018/04/Inaugural-TMT-Pulse-Survey_-20-Apr-Final.pdf
- 54 Smith, A. (2018, 28 June). "Public Attitudes Toward Technology Companies". Retrieved from: <http://www.pewinternet.org/2018/06/28/public-attitudes-toward-technology-companies/>
- 55 Harvard CAPS & The Harris Poll (2018, Aug.). "Crosstabs, Monthly Harvard-Harris Poll: August 2018". Retrieved from: https://harvardharrispoll.com/wp-content/uploads/2018/08/Final_HHP_Aug2018_RegisteredVoters_Crosstabs_Memo.pdf
- 56 Raicu, R., Suzor, N., Roberts, S., West, S. M., ACLU Foundation of Northern California, Electronic Frontier Foundation. Center for Democracy & Technology. (2018, 7 May.). "The Santa Clara Principles on Transparency and Accountability in Content Moderation". Retrieved from <http://www2.datainnovation.org/2018-algorithmic-accountability.pdf>
- 57 New, J. and Castro, D. (2018, 21 May). "How Policymakers Can Foster Algorithmic Accountability". Retrieved from: <http://www2.datainnovation.org/2018-algorithmic-accountability.pdf>
- 58 Reisman, D., Schultz, J., Crawford, K., & Whittaker, M. (2018, 9 April). "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability". Retrieved from: <https://ainowinstitute.org/aiareport2018.pdf>

THE NEW CENTER

THINK CENTERED