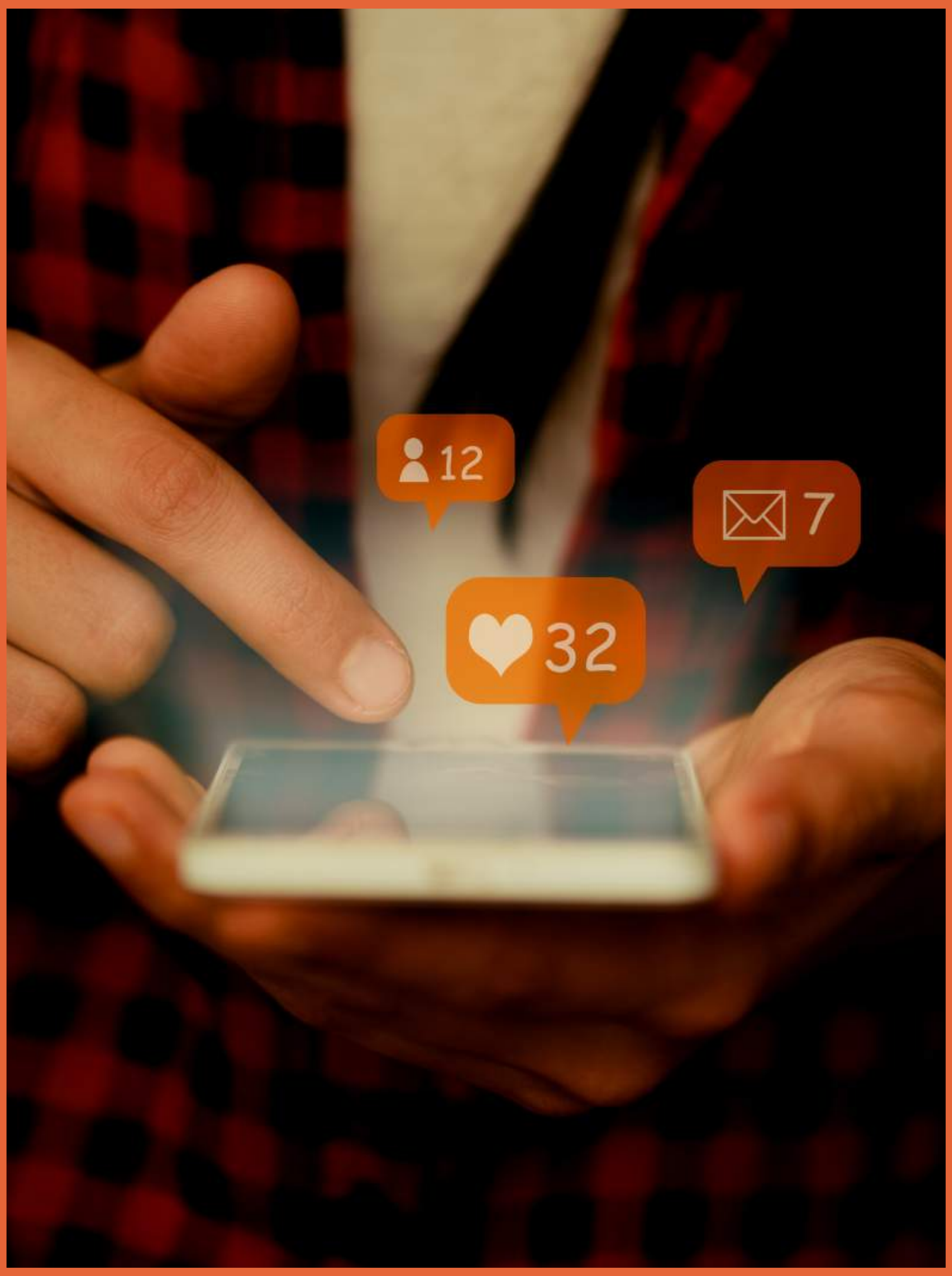
THE NEW CENTER



Policy Paper

February 2021

How Can Washington Take On Big Tech?

THE DIGITAL COMMERCE AGENCY

THE NEW CENTER

HOW CAN WASHINGTON TAKE ON BIG TECH?

THE DIGITAL COMMERCE AGENCY

Febuary 2021

AUTHOR

Olive Morris
Policy Analyst
olive@newcenter.org

RESEARCH ASSISTANCE

Tom Rollins
Policy Research Intern
tom@newcenter.org

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 vibrant center emerges with an agenda that appeals to the vast majority of the American people. This is the mission of The New Center, which aims to establish the ideas and the community to create a powerful political center in today's America.

THE NEW CENTER

1808 I Street NW, Fl. 5
Washington, D.C. 20006
www.newcenter.org

INTRODUCTION

On January 8, 2021, Twitter suspended President Donald Trump's account after he called on his supporters to march towards the U.S. Capitol building while Congress attempted to certify Joe Biden as the winner of the 2020 presidential election.

Soon after, other social media outlets suspended Trump from their platforms—even ones that the President didn't appear to have an account on—including Youtube, Snapchat, Reddit, Twitch, Shopify, and TikTok. Google then suspended the popular-with-conservatives, pro-free speech blogging website Parler from its app store, citing its failure to provide "robust moderation" of posts inciting violence.

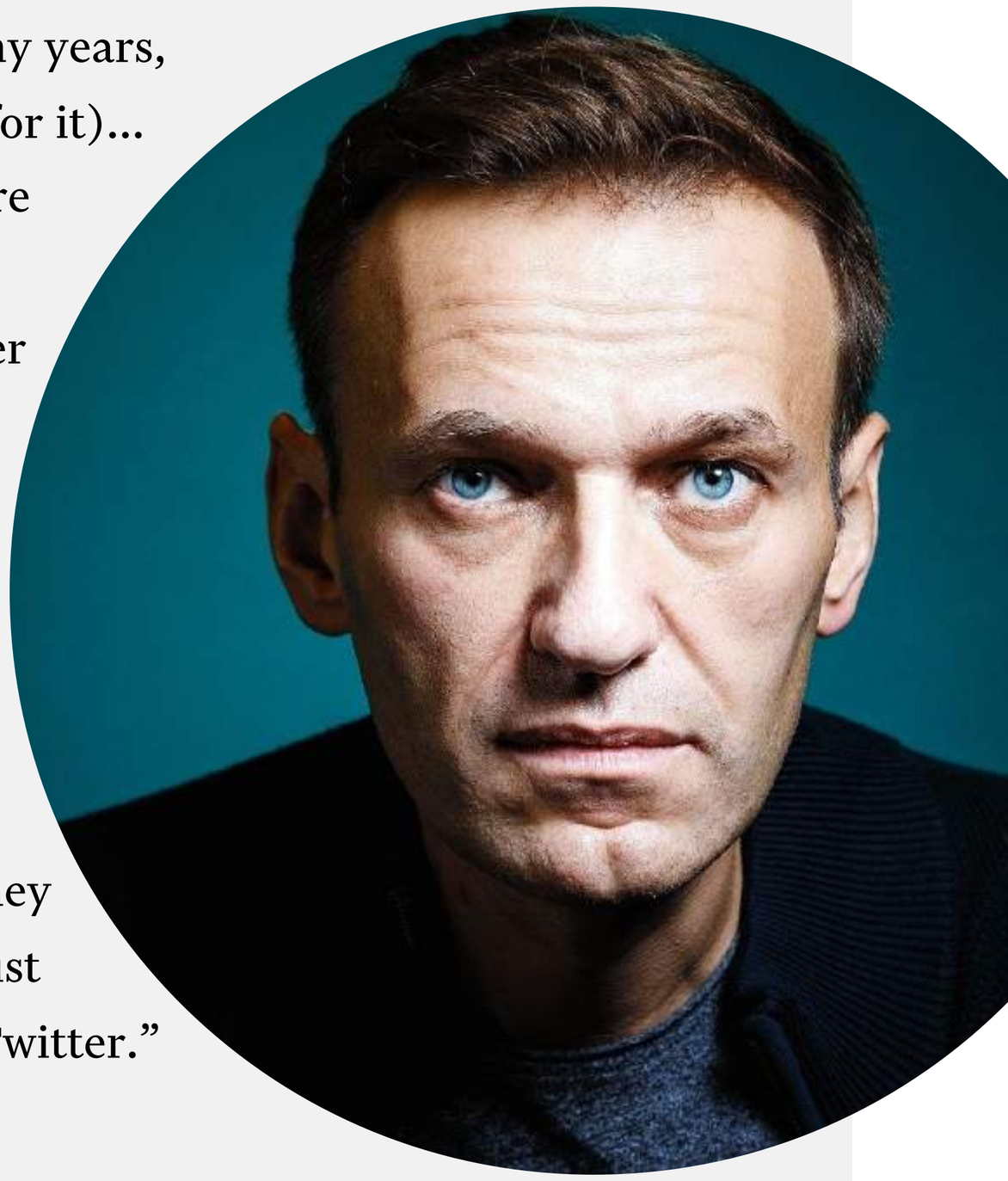
In some corners of the media, these steps were applauded as critical in the fight against hate and misinformation. But at what cost? These moves reveal a world in which a few private companies—which are not accountable to voters—increasingly have the power to decide what the American people can hear and say.

It sets a dangerous precedent when a company like Twitter can unilaterally shut down the main communication channel of the President of the United States. In fact, many global leaders—even those with a publicly contentious relationship with President Trump—are raising alarms about the lack of judicial and democratic oversight for Big Tech and the declining space for free expression.

Notable world leaders who opposed Twitter and Facebook's actions include Mexico's president Andrés Manuel López Obrador, France's economy minister Bruno Le Maire, and British Prime Minister Boris Johnson. The spokesman for German Chancellor Angela Merkel said that "the right to freedom of opinion is of fundamental importance. Given that, the chancellor considers it problematic that the president's accounts have been permanently suspended."

Russian opposition leader Alexey Navalny, a prominent critic of Vladimir Putin, called the Trump Twitter ban, "an unacceptable act of censorship...based on emotions and personal political preferences." Navalny was poisoned and then arrested amid his investigation into high-level government corruption, which U.S. intelligence services are calling an act of political retribution by the state.

“Don't tell me he [Trump] was banned for violating Twitter rules. I get death threats here every day for many years, and Twitter doesn't ban anyone (not that I ask for it)... Among the people who have Twitter accounts are cold-blooded murderers (Putin or Maduro) and liars and thieves (Medvedev)...Of course, Twitter is a private company, but we have seen many examples in Russian [sic] and China of such private companies becoming the state's best friends and the enablers when it comes to censorship...This precedent will be exploited by the enemies of freedom of speech around the world. In Russia as well. Every time when they need to silence someone, they will say: 'this is just common practice, even Trump got blocked on Twitter.”



Russian Opposition Leader Alexey Navalny, January, 9, 2021, via Twitter

The Trump Twitter ban is but one small facet of an increasingly serious problem—the immense and concentrated influence of major tech companies. The growing dominance of these tech companies is imposing real costs that are suddenly not so hidden—including threats to privacy, free speech and expression, and monopolistic practices that are potentially limiting competition and distorting markets. Though both Democrats and Republicans in Washington have been increasingly spotlighting these problems, they have not yet developed a response commensurate with the challenge.

In this paper, the New Center explores the problems posed by social media and platform companies and explains how Washington could solve them by reaching into the past. Just as Congress once created the Federal Communications Commission to oversee the rapidly growing radio and TV industries, it is time to create a new Digital Commerce Agency that could protect consumers, competition, and democracy.

THE MYTH OF FREE SERVICE

Platform-centric companies like Facebook and Google rely on advertisements to billions of users as their primary source of revenue. The companies are able to more precisely target the ads because of the reams of information they gather about their users, like the things they read, watch, click, and like. It's this model that has made these businesses so profitable: In 2019, Facebook generated $69.7 billion from advertising and Google's parent company Alphabet earned $162 billion.

Many commentators have deemed personal data "the new oil"—a highly valuable commodity that powers the world's largest companies. In 2019, Facebook had 2.38 billion monthly active users and made an average of $29 per user. And that's the going rate for Facebook alone—the average person had 8.6 social media accounts in 2020.

Despite data being a linchpin of the global economy, many consumers are confused about who is collecting their data and why it's so valuable. According to a 2019 Pew Research Poll, 81% of Americans reported they had "very little/no control over the data companies collect" and 59% of Americans have "very little/no understanding" of what is done with that data.

Most Americans accept this trade-off because these companies provide them with avenues to interact with friends, watch videos, and shop and start small businesses—at no cost to the user. However, Christopher Mims writes in The Wall Street Journal, "In reality, these services are anything but free. We just don't pay for them in the way we're used to." These supposedly free business models rely on progressively compelling users to hand over their personal data, creating three distinct harms to consumers.

Firstly, instead of using money, people are paying for these services with their privacy and attention. To keep users on their platforms, social media companies employ a series of techniques to maintain people's attention and gather more of their data.

To keep someone on LinkedIn, for example, the site will send an email to the user about a message they received on the platform, but they'll need to visit the website to read it. On Instagram, the app frequently pings users to turn on more notifications, but never to turn them off. With this constant nagging, it's unsurprising that the average user spent 2 hours and 24 minutes per day on social media in 2020.

Secondly, social media companies' "free" business models compel them to prioritize advertising over privacy, public health, and social good. One of the most notable examples is Facebook allowing advertisers on their platform to collect users' friends' data, precipitating the infamous Cambridge Analytica scandal.

In 2016, the political advertising firm Cambridge Analytica used a third-party app to clandestinely obtain data on millions of Facebook users without their permission in an attempt to influence the U.S. presidential campaign. Thousands of Facebook users downloaded an app called "This Is Your Digital Life," which eventually provided the data of users and all their Facebook friends to Cambridge Analytica, which used it to promote the campaigns of Senator Ted Cruz and President Donald Trump.

What Google Knows

Google compiles enough data to build comprehensive portfolios of most users–who they are, where they go and what they do–and the information is all available at google.com/dashboard. Here are just a few things WSJ reporter Tom Gara found out about himself.

2,702 Contacts

Google knows the people that Tom emails the most. At the top is a friend in Egypt.

134,966 Emails

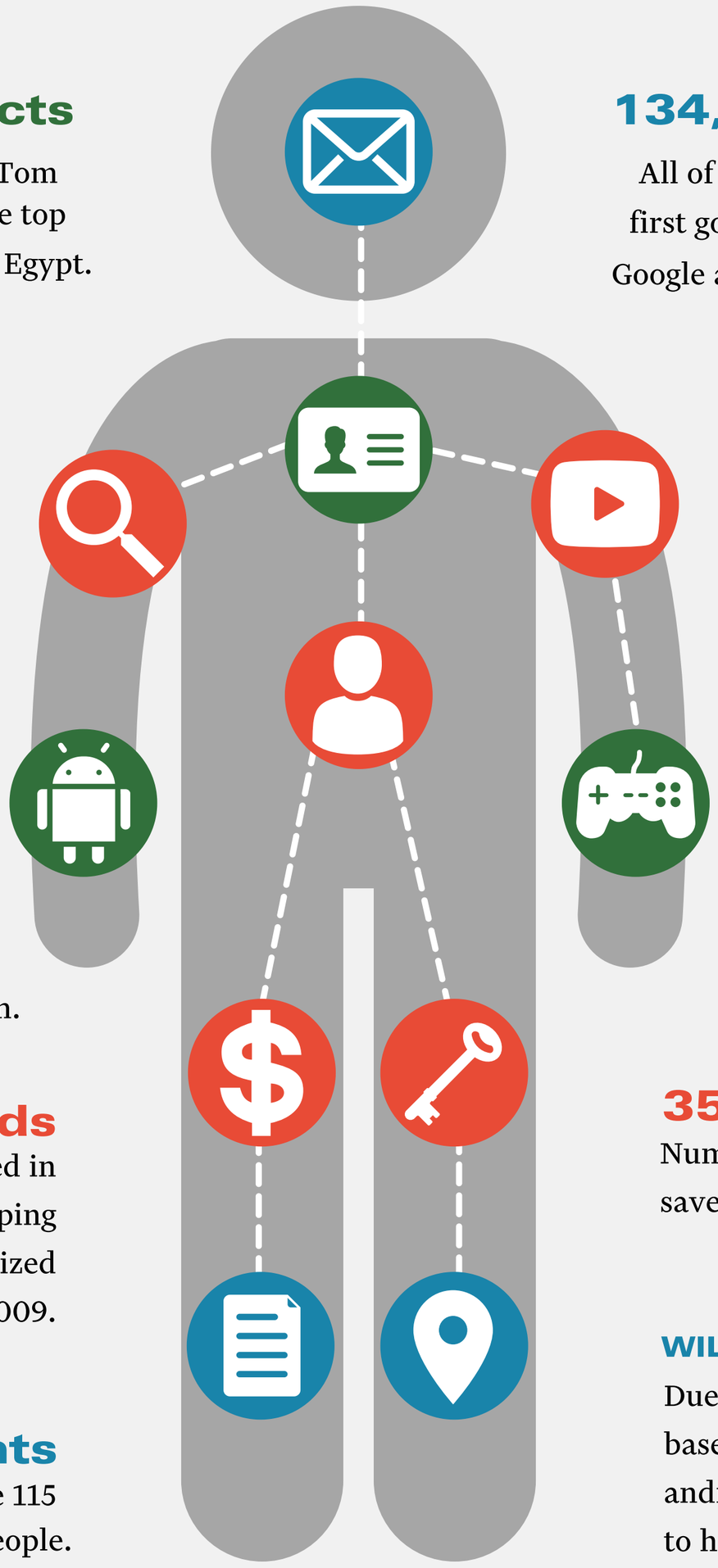
All of Tom's emails since he first got a Gmail account in 2004. Google also stores his 6,147 chats.

64,019 Searches

Google thinks Tom performs most of his searches around 8 a.m. ET. but this is probably skewed by years spent outside the U.S.

9,220 Videos

Tom has watched, listed in chronological order, including a series viewed in June about canoes.



3 Androids

Google knows all of Tom's synched Android phones, including the old Nexus phone that he gave to his Mom.

117 Apps

that Tom has downloaded from Google's store.

3 Credit Cards

(two expired) saved in Google Wallet, plus two shipping addresses and 13 itemized purchases since June 2009.

35 Passwords

Number of website passwords saved in Google's Chrome browser.

855 Documents

that Tom has created, plus the 115 he has opened that belong to other people.

WILLUNGA, SOUTH AUSTRALIA

Due to an unknown glitch, Google bases Tom's location from one of his old android phones, which he gave to his mother in Australia.

Sources: Alberto Cervantes, Tom Gara, and The Wall Street Journal.

Thirdly, many people don't realize the risks associated with having their data circulating around the internet. Every day, personal data is stolen from legitimate, trusted businesses and used to defraud Americans. Cybercrime is more profitable than the global illegal drug trade, totaling an estimated $1.5 trillion in revenue annually.

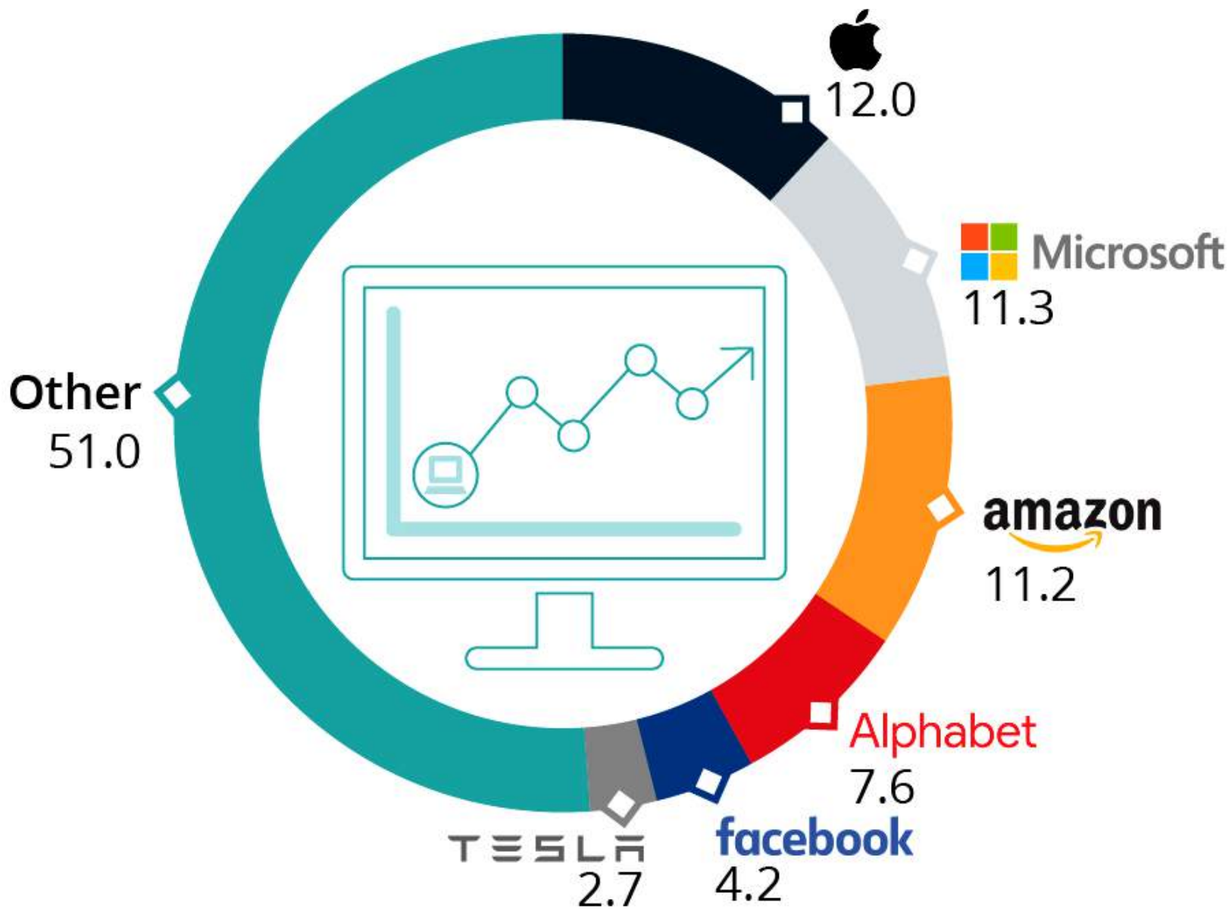
Even the most advanced companies have cybersecurity vulnerabilities: Facebook stored hundreds of millions of passwords in plain text files in 2019—a realization that forced Facebook's engineers to reassess the company's entire security infrastructure. In 2019, there were over 1,500 data breaches in the United States alone. Most hackers are looking to sell that personal data on the black market for buyers to commit various forms of fraud, which can be done very cheaply. Personal data is so readily available that buying someone's Social Security Number on the dark web only costs $1 on average.

Data collection has become so widespread that people cannot meaningfully opt out of this collection. One in nine users consent to data collection without being fully aware of what they're sharing—the details of which are buried in Byzantine terms-of-service agreements. The average American would need to set aside almost 250 hours to read all the digital contracts they accept—several times longer than it takes the average person to read the complete works of William Shakespeare.

WHAT CONSTITUTES A MODERN MONOPOLY?

In 2020, the five largest American technology companies—Microsoft, Apple, Amazon, Google, and Facebook—held a combined valuation of over $5 trillion (which is more than 40% of the value of the Nasdaq 100). However, under U.S. law, a company is not necessarily a monopoly simply because it is dominant in its market.

Several U.S. Supreme Court decisions have determined that size only becomes a matter of antitrust if the company has achieved its size through exclusionary or predatory conduct to harm competitors. According to the framework established by the D.C. Circuit Court, to successfully bring an antitrust case, the FTC and Department of Justice would need to demonstrate that a company has perpetrated "anticompetitive behavior" that has harmed both the competitive process and consumers—for example, by restricting market access by mandating exclusive distribution agreements.



Right Image: CNBC.

THE CASE OF GOOGLE: A STRANGLEHOLD ON DIGITAL ADVERTISING

Just two companies, Google and Facebook, collected 63% of all U.S. digital advertising dollars in 2017. Google's parent company Alphabet made $162 billion in ad revenue in 2019. For comparison, this makes Google's annual ad revenue higher than two-thirds of all countries' gross domestic product (GDP).

To understand the extent to which Google dominates online advertising, one must understand how "ad exchanges" work. Approximately 86% of digital advertising space in the U.S. is bought and sold on electronic trading venues (so-called "ad exchanges.")

Prices for ad space are determined through real-time bidding, similar to the structure of electronically traded financial markets. Google's parent company Alphabet simultaneously dominates the sell-side platforms that publishers use and the buy-side platforms used by advertisers. This is the digital equivalent of the New York Stock Exchange owning and operating Goldman Sachs—with no laws governing potential conflicts of interest.

As best explained in a Keach Hagey and Vivien Ngo visual article for The Wall Street Journal:

"When a reader visits the website of a large online publisher, the publisher uses an ad server to put ad space up for sale and determine which ad to show the reader.

Ad space is put up for sale through exchanges, marketplaces where transactions happen in real-time between buyers (advertisers) and sellers (publishers)...

Advertisers use sophisticated buying tools to bid for ad space in the exchange... The exchange runs an auction, and the highest bidder gets to place its ad in front of the user."

1. Ad server. Google's DoubleClick for Publishers is the most popular ad-serving tool.

2. Ad exchanges. Google owns the largest ad exchange through its subsidiary Double Click.

3. Buying tools. Google's DV360 is a popular buying tool.

Some antitrust advocates, including members of the House Antitrust Subcommittee, have argued that Google was able to throttle competition by controlling these ad markets. For example, before 2016, Google allowed rival ad exchanges to sell advertising on YouTube, the second largest social media platform in America. However, five years ago, Google changed its policy to only allow Youtube ads to be bought through Google's products. This pushes advertisers to do more of their spending through Google.

Simultaneously, these practices may be affecting the price of online advertisements. As described by Dina Srinivasan for the Stanford Technology Law Review:

> "Competition authorities, publishers, and advertisers also look quizzically at Google's dominance because ad trading costs remain suspiciously high. In theory, electronic trading should push transaction costs (and dealers' spreads) down. However, in advertising, transparency is a challenge. Some authorities estimate that middlemen take 30 to 50% of every trade. When a local car dealership uses Google's buy-side to purchase ad space from Google's exchange, Google does not tell that advertiser what the ad space ultimately cleared for or how much Google keeps as its share. Google also does not disclose to the publisher on the other end of this trade how much the advertiser paid to purchase the publishers' inventory."

In other markets where participants display these same behaviors, federal agencies have stepped in to investigate. In the digital financial market in 2009, the broker-dealer Barclays started "preferentially routing its clients' stock orders into Barclays' 'dark pool'—a trading venue where parties can trade with each other anonymously," according to Srinivasan. Over the next four years, Barclays's specialized trading venue became one of the top two in the U.S. by funneling customers into higher-risk trading categories without their knowledge. The Securities and Exchange Commission, an independent U.S. agency created to protect investors, issued a $70 million fine in 2016 for this behavior, arguing that it misled consumers and created a conflict of interest between the dark pool platform and the brokers making money off customers' riskier investments.

MISINFORMATION

In an effort to keep users on their platforms and sell more advertising, social media companies' algorithms show users information and news that they most often interact with. But several studies have shown that people are most likely to interact with Facebook posts that promote fear, anger, and tribalism—and social media algorithms have often prioritized this kind of content as it keeps users on the platform a little longer.

A 2016 PNAS study found that Facebook users tend to interact with news sources that reinforce their own political ideology, potentially creating echo chambers online. And according to Elon University Professor Janna Anderson and Pew Research Center Internet Director Lee Rainie, "this makes many vulnerable to accepting and acting on misinformation."

Additionally, the growth of misinformation in America mostly emanates from active disinformation campaigns by bad actors and foreign governments looking to take advantage of division in America. In fact, a 2018 Knight Foundation study found that just ten predominantly fake news and conspiracy outlets were responsible for 65% of tweets linking to such stories. Despite this, Congress has struggled to craft modern regulation for these modern problems. For example, Section 230 of the Communications Decency Act was created in 1996 to provide a liability shield for internet platforms, meaning that social media companies are not responsible for illegal content or misinformation posted by their users. But the internet has evolved in ways policymakers never could have imagined in 1996. When Section 230 was passed, Facebook founder Mark Zuckerberg was in middle school coding computer games for his friends, and it hasn't been updated since.

CENSORSHIP

People increasingly don't understand what kind of content is permissible online. About three in four Americans feel it is very likely or somewhat likely that social media sites "intentionally censor political viewpoints that they find objectionable," according to a 2020 Pew Research Poll. Perhaps unsurprisingly, many of these concerns about tech companies are adding to their increasingly negative public perception.

Americans' Views of Technology Companies, by Party Identification

	Positive %	Neutral %	Negative %	Net
2021 Jan 21-Feb 2				
Republican	20	15	65	-45
Independent	33	23	44	-11
Democrat	49	21	30	+19
2019 Aug 1-14				
Republican	43	19	37	+6
Independent	43	23	33	+10
Democrat	49	21	29	+20

Source: Gallup

President Donald Trump and several other GOP leaders have repeatedly accused social media giants of anti-conservative bias. Conversely, Democrats accuse companies of being overly accommodating to conservatives, pointing to the astronomical engagement rates of pro-Trump news outlets on Facebook as evidence against censorship.

So, are social media platforms censoring conservative viewpoints more frequently? It's not exactly clear—and that is a massive problem. Since the buying and selling of data has become more valuable than oil, platform companies like Google and Facebook treat much of their data as proprietary, including information on content moderation. Independent research institutions aren't typically able to analyze companies' practices, so the public must rely on anecdotal instances of content moderation gone awry—like the social media banishment of President Trump.

Big Tech companies increasingly serve as people's news sources and the bedrock of the American economy. And as explained by a report from the University of Chicago's Stigler Center, "Google and Facebook have the power of ExxonMobil, the New York Times, JPMorgan Chase, the NRA, and Boeing combined. Furthermore, all this combined power rests in the hands of just three people. Whether or not you believe censorship is happening, digital platforms are incredibly opaque—this is a problem in itself."

WHAT WE'RE DOING ISN'T WORKING

Despite policymakers and stakeholders increasingly highlighting the problems posed by the growing influence of big tech companies, the government's response has been piecemeal and insufficient.

In the United States, privacy laws protect personal health and financial data, but personal online data is largely unregulated at the federal level. Various state laws attempt to regulate internet privacy, but some tech companies have lobbied to prevent the passage of many of them. Of the laws that have been passed, many are inconsistent with one another.

For example, many states have begun enacting legislation related to online security breaches, but some are preventative while others are reactive. California law mandates notification of a security breach to all affected customers. Other states like Massachusetts require certain preventative measures against security breaches, but their laws do not include provisions addressing what should be done if a breach were to occur.

AN UNDERSTAFFED, OVERWORKED, AND DISEMPOWERED FTC

The Federal Trade Commission casts a wide regulatory net, covering "a variety of antitrust and consumer protection laws affecting virtually every area of commerce." However, despite this agency's purview over many issues relevant to technology companies, it's facing serious procedural and personnel hurdles.

Joseph Simons, the FTC Chairman since 2018, has flagged concerns that the agency only has 40 employees dedicated to monitoring data privacy and security matters—a fraction of the number of privacy- and security-centric employees employed by European governments. Despite their substantially smaller population and fewer large tech companies, the Irish Data Protection Commissioner enlists 110 employees, while the U.K. Information Commissioner's Office has over 500 data employees.

Throughout U.S. history, the government has also devoted substantial resources to industries and technologies with significant power over the broader economy. The Securities and Exchange Commission, which was created to protect investors and the integrity of the banking system following the Great Depression, now employs a staff of over 4,000 to protect markets.

On December 9, 2020, the Federal Trade Commission and 48 state attorneys general filed antitrust lawsuits against Facebook, saying the company used its "dominance and monopoly power to crush smaller rivals and snuff out competition, all at the expense of everyday users." The lawsuits zeroed in on Facebook's acquisitions of Instagram in 2012 for $1 billion and WhatsApp in 2014 for $19 billion, arguing that these purchases broke competition law. However, experts worry that the FTC is facing an uphill battle.

The two primary laws regulating antitrust—the Sherman Act and the Clayton Act—were both passed over a century ago, and even at the time, pro-labor groups lamented these acts were watered down through the heavily lobbied legislative process. Missouri senator James A. Reed stated: "When the Clayton bill was first written...it was a raging lion with a mouth full of teeth. It has degenerated to a tabby cat with soft gums, a plaintive mew, and an anemic appearance."

Since these acts were passed, courts have erred on the side of underenforcement of antitrust and made it increasingly difficult to successfully challenge anticompetitive conduct. According to the Democratic members of House Judiciary Committee in their Investigation of Competition in Digital Markets, “By adopting a narrow construction of ‘consumer welfare’ as the sole goal of the antitrust laws, the Supreme Court has limited the analysis of competitive harm to focus primarily on price and output rather than the competitive process—contravening legislative history and legislative intent.” However, the concept of consumer welfare doesn’t work well for companies that aren’t directly charging customers.

Democratic staffers wrote in their investigation that “the courts have significantly weakened” antitrust laws since their enactment, and contradicted the laws' original intent by focusing on “consumer welfare.” The staff recommended to revert to the initial scope of Congress' antitrust rulings, which were not meant to simply protect consumers, but also “workers, entrepreneurs, independent businesses, open markets, a fair economy and democratic ideals.”

Even if the FTC makes a convincing case against these companies, the agency has struggled to apply substantive penalties in the past. Previous settlements with Google and Facebook in 2019 did little to curb these companies from excessive data collection and re-selling to third parties. The combined financial penalty totaled less than $7 billion.

In its largest fine ever, the FTC required Facebook to pay $5 billion in 2018 for violations of a 2011 agreement that required Facebook to obtain consent from users before it shared their data with third parties. But given the fact that Facebook had almost $56 billion in revenue in 2018 alone, a $5 billion fine for ethically questionable but highly lucrative data sharing arrangements could simply be viewed as the cost of doing business, rather than as an effective deterrent against such activity.

THE DIGITAL COMMERCE AGENCY

It's a familiar pattern throughout U.S. history: a disruptive innovation arises and reshapes how people work and live. But at a certain point, the creators of these innovations accrue enough power and influence that they need to assume greater responsibility for the public interest.

When disruptive innovations arose in the past, federal agencies were formed to tackle the problems that these innovations would inevitably create. To capitalize on the efficiency that freight trains offered during World War I —made even more critical for their role in munitions shipping—the U.S. Railway Administration was created to reconcile the interests of overworked union laborers, bankrupt railway management, and antsy investors.

The Federal Communications Commission was formed in 1934 as an upgraded Federal Radio Commission, the agency charged with regulating radio communication and broadcasting stations. By the 1930s, communications issues had begun to advance past the occasional interference from unlicensed radio transmitters. The U.S. government needed an agency to regulate burgeoning television network monopolies, most notably the National Broadcasting Company and the Columbia Broadcasting System, which dominated network broadcasting and dampened competition from smaller stations.

As 21st-century economic activity evolves, Washington must also evolve to reflect the realities of the digital era. Going into 2021, pre-existing legislation and federal regulatory agencies clearly don't have the capacity to oversee dominant digital platforms. That needs to change, and the new administration and Congress should stand up a new federal Digital Commerce Agency (DCA).

STAFFING UP

An agency that would effectively regulate digital commerce would require specialized technological experience and capabilities, which have been a continued trend when new issues arise in America.

At the dawn of telecommunication, Congress delegated oversight to the Interstate Commerce Commission, the federal agency regulating railways. However, it wasn't long before Congress recognized that the technology required a more focused agency staffed by experts with a specific set of skills, which would become the Federal Communications Commission.

Similar circumstances have given rise to agencies as diverse as the Commodity Futures Trading Commission and the Nuclear Regulatory Commission. The Commodity Futures Trading Commission, created in 1974 to tackle trillion-dollar commodity futures markets, has more than 600 full-time staff members.

At a 2019 Senate Banking Committee hearing, Pinboard founder Maciej Ceglowski likened the challenges presented by personal data to the early days of nuclear regulation:

“I worry that we’re in the same position that the nuclear industry was in the early '50s. We have an amazing new technology with real potential, but we are not being honest about the risks and our incapacity to store a wasteful and harmful byproduct.”

Today, the U.S. Nuclear Regulatory Commission has more than 3,000 employees.

ADDRESSING THE HARMS OF “FREE” SERVICE

A new Digital Commerce Agency would need to have a nimble regulatory apparatus to keep pace with the rapid rate of technological change while adhering to congressionally mandated principles.

Three principles of regulatory focus have been repeatedly floated by online platform experts from the Congressional Research Office, the Harvard Shorenstein Center and Brookings, and Public Knowledge, as well as foreign governments that have created their own analogues to a Digital Commerce Agency: data protection and privacy, transparent content moderation, and updated antitrust enforcement.

1. Data Protection and Privacy

To promote data protection and privacy, the Digital Commerce Agency could look to the common law principle of “duty of care,” a legal obligation applied in America and across Europe since the early 20th century. It requires companies to anticipate and mitigate the harmful effects of their products and services.

At the advent of the automobile, U.S. courts utilized the principle of "duty of care" on manufacturers for any potentially faulty parts, even if they were produced by a third party. And in 2020, the U.K. government used the principle of “duty of care” to require platform companies to “remove and limit the spread of illegal content,” with fines of up to ten percent of annual global turnover. This “illegal content” is not strictly defined; the measure outlines specific harms that regulators will focus on, such as posts encouraging suicide, child abuse, hate crimes, violence, or terrorism.

This principle is particularly suited to encourage the prudent handling of consumer and commercial data. In a 2019 white paper, the University of Chicago’s Stigler Center suggested that data statutes be based on “the results of well-designed, scientifically rigorous studies that elicit consumer preferences, opt-out costs, and knowledge of the rules and alternatives, as well as ignorance and biases of such rules’ potential costs and benefits.”

2. Transparent Content Moderation

Congress, using enforcement mechanisms within the Digital Commerce Agency, should be charged with updating Section 230 to maintain social media companies' ability to provide content moderation in a way that promotes duty of care, but also adheres to the underlying principles of the First Amendment. Though the First Amendment only restricts the government from limiting free speech, one could argue the reach of tech companies has become so massive, they have in effect become like a public square and that society has an interest in ensuring people are free to speak up in that square.

For effective and transparent content moderation online, it is critical that companies have clear regulatory standards. Congress desperately needs to update Section 230 to address problems in the modern era. A useful starting point for discussion could be the Platform Accountability and Consumer Transparency Act (PACT) Act, proposed by Senators Brian Schatz (D-HI) and John Thune (R-SD), which Thune said would "preserve the benefits of Section 230 – like the internet growth and widespread dissemination of free speech it has enabled – while increasing accountability and consumer transparency."

The Digital Commerce Agency should be able to compel social media companies of a certain size to share data concerning misinformation and content moderation with independent researchers. The Digital Commerce Agency should also be given the authority to evaluate the transparency of companies' terms of service, the efficacy of their appeals processes, and the moderation of political content.

3. Updated Antitrust Enforcement

The "duty to deal" is another common law-derived principle which would prove useful in litigating antitrust for online platforms. This idea is best described by the Shorenstein Center as follows: "When a service is essential or critical owing to its monopoly characteristics, there is a duty to provide non-discriminatory access to that service."

"Duty to deal" was established by United States v. Terminal Railroad Association of St. Louis, which asserted that companies that maintain strategically vital railroads, like one that ran over the Mississippi River, must grant other companies access to their "essential facilities."

Today, experts from Harvard's Shorenstein Center argue that the internet has become an essential service and that data is its critical asset. As a result, internet companies should be subject to duty to deal, including "nondiscriminatory access through interoperable interfaces, free flow of data across services providers, and limits on preferencing dominant platforms over competitors."

Of course, applying any of these principles won't do much without sufficient enforcement mechanisms for a new agency. This means that the new Digital Commerce Agency must be granted the same power of subpoena and civil investigative demands (CIDs) available to the FTC, which the agency considers "critical to the task of investigating potential law violations." These congressionally sanctioned authorities will provide the nascent agency with the teeth to regulate powerful companies.