CAP

Center for American Progress
1333 H Street NW, Suite 100E
Washington, DC 20005

202.682.1611

americanprogress.org

November 21, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Request for Comments pursuant to Commercial Surveillance ANPR, R111004

Dear Chair Khan,

The Center for American Progress applauds the decision of the Federal Trade Commission ("FTC") to fulfill its mission of protecting consumers and competition by scrutinizing commercial surveillance and data security practices.

For the average American, these practices are ubiquitous, unavoidable, and unwanted. For many companies, the use of deceptive and harmful practices by some creates a race to the bottom on privacy and data protection for entire industries. On both fronts, intervening to protect consumers and competition is highly consistent with the core mission and authority of the Commission.

We appreciate the invitation to comment on this project and respectfully offer several ideas for your consideration.

Sincerely,

Adam Conner
Vice President of Technology Policy

Marc Jarsulic
Senior Fellow and Chief Economist

Executive Summary

The Center for American Progress (CAP) applauds the Federal Trade Commission (FTC) for its advanced notice of proposed rulemaking (ANPR) for public comments regarding "Trade Regulation Rule on Commercial Surveillance and Data Security."[1] Rulemaking from the Commission is desperately needed to address the pernicious and pervasive harms created by the collection and monetization of consumer data and lax data security practices.

This step is long overdue. As online services have proliferated, so too have the attendant harms generated by the unregulated commercial data economy. The Commission is nearing the limits of what it can accomplish using its existing tools. It is well within its mission to formulate rules that address unfair and deceptive practices to mitigate their harms to consumers and competition.

In the foundational report from the Center for American Progress "How To Regulate Tech: A Technology Policy Framework for Online Services," [2] CAP argued that multiple approaches are required in order to address the challenges created by online services. CAP called for new rulemaking from the Commission and other entities to establish clear prohibitions on harmful practices. The report highlighted the importance of ex ante enforcement as a tool for addressing harms alongside ex post enforcement such as antitrust action.

The following comment draws upon the authors' past work to answer key questions posed by the ANPR. Its conclusions are summarized below and elaborated on in the text that follows.

> **Question 1**: To the question of what practices are used to surveil consumers, CAP offers a research-based explanation of common surveillance technologies, including those used in ad targeting, creation of social graphs, third-party cookies, Federated Learning of Cohorts, and software development kits ("SDKs").
>
> **Question 4**: To the question of how commercial surveillance harms consumers, CAP outlines literature illustrating the economic, privacy, and consumer protection issues arising from commercial surveillance practices and related services. This synthesis notes that these harms to consumers are difficult for them to avoid, even with substantial work and expertise, and fall asymmetrically on low-income communities and communities of color.
>
> **Question 5:** To the question of harms that consumers may not easily discern or identify, CAP highlights polling and other measures which show that, while consumers are generally concerned about corporate surveillance of their activities, they have little detailed knowledge or understanding about those practices or their potential impacts on the services and information they receive.
>
> **Questions 11 and 17:** To Question 11 on commercial incentives and business models that lead to lax data security measures or harmful commercial surveillance practices, CAP outlines common tech industry algorithmic strategies to increase user engagement. Simultaneously, this response draws connections to Question 17 on "techniques that manipulate consumers into prolonging online activity (e.g., video autoplay, infinite or endless scroll, quantified public popularity)." Question 17 has a specific focus on

children and teenagers, and CAP's response focuses on the algorithmic techniques which impact all users, including children and teenagers.

Question 12: To the question of which "commercial surveillance practices are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them," CAP encourages the Commission to develop rules that clearly prohibit certain harmful practices in commercial surveillance and data security, especially those practices which present an inherent risk to civil rights.

Question 30: To the question of whether the Commission should commence a Section 18 rulemaking on commercial surveillance and data security, CAP makes an argument in the affirmative. Amidst a lack of regulation, the market for more data has created a race-to-the-bottom on commercial surveillance. Thoughtful regulatory interventions are an appropriate tool to fix this market failure, and it is well within the Commission's power to do so. There is no reason to believe that continued reliance on self-regulation will produce anything but the status quo: predatory, deceptive practices as the industry standard.

Question 31: To the question of whether the Commission should commence a Section 18 rulemaking exclusively on data security, CAP provides a set of questions about process and scope to help inform the Commission's decision. It notes that the scope of entities that would be affected by a data security rulemaking are likely to be far wider (potentially all entities that store data) than those entities who utilize commercial surveillance data collection, monetization, and movement.

Question 65: To the question of the prevalence of algorithmic discrimination based on protected categories such as race, sex, and age, CAP discusses the broad civil rights harms stemming from the rise of online services and their impacts on low-income communities and communities of color.

Question 86: To the question of opacity in different forms of commercial surveillance practices, including technical or legal mechanisms companies use to shield them from public scrutiny, CAP highlights the impact of the loss of third-party analytics firms. Previously, such firms sought to provide insight into online activity, especially on large digital gatekeeper platforms. Their closure or acquisition by digital gatekeepers who wish to foreclose access to the limited information they provided contributes to the excessive opacity with which digital gatekeepers shield even basic operations and widespread practices.

Response to Questions

The Commission has offered questions on a wide range of areas involving commercial surveillance and data security. In keeping with the Commission's guidance, CAP will direct its responses to a handful of questions on which it has the most expertise.

Question 1

On Question #1 regarding what practices companies use to surveil consumers, CAP encloses the following section from CAP Senior Fellow and Chief Economist Marc Jarsulic's recent article "Addressing the Competitive Harms of Opaque Online Surveillance and Recommendation Algorithms" in *The Antitrust Bulletin*:[3]

> "Online ad sales depend on the ability of [Facebook and Alphabet] to individually target ads and messaging to huge numbers of people. In the case of Facebook, the ads are targeted to Facebook users and are delivered on Facebook's platforms. Alphabet sells ads that are targeted to users on Google, YouTube and other apps. Targeting is possible because both businesses have detailed information about individual users, and the ability to analyze that information to suit the needs of the platform and online advertisers.
>
> The information about individual platform users is derived from elaborate and effective systems of online surveillance. Facebook has unrestricted access to an astounding variety of user data. The site can monitor what users watch and read in the Facebook Newsfeed and how long they spend doing so, what users tag with Facebook "likes", along with their communications with others using the Facebook app. Facebook also can follow users as they engage with apps such as Instagram, What'sApp, and Messenger, which are now part of the Facebook platform. The site constructs a social graph for each user, which shows with whom and with what the user has connected. Because Facebook has a graph for each user, it can see both direct and indirect interconnections between individuals, activities, and websites across the Facebook platform and beyond. While a Facebook application called Graph Search has allowed users to search for certain public information, most interconnections are not observable to an individual user.[4]
>
> Alphabet likewise has a highly effective surveillance system in place. It records the search histories of individuals on Google, the viewing histories of users on YouTube, and gathers purchasing history, location, and other information from apps like Google Maps and GMail. The Android operating system used on smartphones also provides information about the physical location, movements, and activities of users.[5]
>
> These platforms also follow individuals when they use other websites.[6] Companies track users by installing small data files called "cookies" in user browsers. Third-party websites who want to host advertisements collaborate with firms like Facebook and Alphabet by installing discrete computer code called "pixels" or other tracking software on their websites. These "third-party" pixels then signal Facebook or Alphabet whenever the individual visits one of the cooperating websites.[7] Given the central importance of these two platforms in delivering ads, publisher websites have very strong incentives to collaborate with them in placing tracking code on browsers. Moreover, the platforms can offer website operators some of the data collected about users visiting their sites.
>
> The use of third-party cookies has come under pressure from EU regulations, and some browsers now block them by default. Alphabet has announced that they will be blocked by the Chrome browser by 2022. This may act to Alphabet's advantage, since it still will be able to gather information about users of its widely used platforms and apps.[8] It is nonetheless possible that Chrome users will be tracked in other ways. In a recent experiment Alphabet

placed special-purpose software in a set of Chrome browsers. The software records browser use in the past week, uses this history to assign the browser to a cohort of users with similar browsing histories, and then assigns the members of that cohort a Federated Learning of Cohorts (FLoC) identifier. This identifier is displayed to advertisers and websites, who can then determine common characteristics of the cohort using machine learning.

The experiment with FLoC, which were executed without notice or consent of affected Chrome users, has been paused because the FLoC identifier assigned by Chrome can aid internet trackers who engage in so-called "browser fingerprinting", a technique which allows tracking sites to uniquely identify a browser and the device on which it is operating.[9]

Both platforms also can track individuals on the web when they are using cell phones or other mobile devices, whether they are using browsers or not. Mobile app developers who want third-party ads or other integrations place so-called software development kits (SDK's), provided by Facebook, Alphabet and other firms, in their apps. The SDK's have access to data gathered by the app, including location or camera access granted to the app. The Android system associates a unique "ad ID" with each device, which is available to all app developers.[10] The amount of data obtained by app trackers can be surprisingly large. One reporter found thousands of trackers reporting data from his iPhone in a single week.[11]

The data gathered by platform surveillance is correlated with information from data brokers, such as credit scores, purchase history, voting history, recent life events such as weddings and house moves, along with demographics such as job type, income, net worth, marital status, and location, to provide very detailed information about the activities, connections, and preferences of individual website users. Facebook correlates platform and broker data to create profiles of users that advertisers use to target individuals on the Facebook platform. [12] Facebook also generates "LookaLike Audiences", which machine learning techniques identify as having characteristics similar to an already existing set of target individuals.[13]

Although we do not know if either Facebook or Alphabet have done so, it is possible using machine learning to accurately profile an individual based on information gathered from her social network. According to an author of a recent study, the implication is that "at least in theory, a company, government, or other actor can accurately profile a person -- think political party, favorite products, religious commitments -- from their friends, even if they've never been on social media or delete their account." [14]

In short, both Facebook and Alphabet gather remarkable amounts of data about individual users of their consumer-facing platforms -- from their activity on the platforms and elsewhere on the internet. These data can be combined with other information from data brokers. The profiling which this enables is the basis for the sale of targeted online messaging."

Question 4

To **Question #4** on harms to consumers, CAP encloses the following section from its 2021 report, "How To Regulate Tech: A Technology Policy Framework for Online Services,"[15] discussing the holistic economic harms (including price and quality), privacy harms, and consumer protection harms (including fraud and manipulation) arising from commercial surveillance practices and related services:

> "The growth of the internet has produced significant social, cultural, and economic benefits for the United States. Providers of online services have helped shepherd the internet from its infancy into a more accessible digital layer that interweaves with most Americans' lives on a daily basis. With the exponential growth of online services and their attendant benefits, however, a number of harms have also emerged, enacted or enabled by online services providers. While many Americans have grown up accepting these harms as a cost of engaging online, the harms generated by online services are not inevitable. Current problems are not necessary evils for the sake of digital innovation, and improved regulation has a dual role to play in promoting beneficial development and curbing predatory practices.
>
> In order to support a vibrant, dynamic internet that serves the public interest, it is necessary to understand not just the benefits but also the harms from online services and the risks they pose to economic, social, and democratic health. These harms are salient and widespread, even where services are offered at low or no monetary cost to users—for example, free email or social networking platforms, which are subsidized by intensive data collection, online tracking, and targeted advertising. These harms tend to be disproportionately borne by marginalized groups—including people of color, low-wage workers, and women—whereas technology's benefits asymmetrically accrue to more privileged groups.[16] In aggregate, these issues amount to troubling threats to commerce, civil rights, and democratic function. To make these issues more legible to traditional regulatory approaches, they are grouped below into four overlapping and deeply interconnected areas: economic harms, privacy harms, consumer protection harms, and civil rights harms.
>
> **Economic harms**
> The proliferation of the internet and digital communication technologies have produced new and complex online businesses. The largest of these businesses have developed communication and information services that have become essential to billions of consumers and are protected from new competitors by powerful barriers to entry. As noted above, these barriers exist because of inherent features of digital markets such as network effects, economies of scope and scale, data advantages, first-mover advantages, and other economic forces.[17] They have been preserved, reinforced, and compounded over time by strategic acquisitions and successful efforts by firms to foreclose nascent competitors and discourage competitive threats,[18] resulting in traditional problems arising from a lack of competition—higher prices, lower quality, and less innovation. In markets dominated by an incumbent digital gatekeeper, the threat of the dominant firm copying or killing any new innovations results in decreased investment, deterrence of entry, and decreased innovation in the digital platform industry.[19] Big tech mergers likewise have adverse competitive effects on growing markets,[20] and incumbent firms may acquire younger firms explicitly to curb innovation that threatens their position.[21] More than 80 percent of Americans believe acquisitions from large online platforms are likely unfair and undermine competition.[22] But with few alternatives, high switching costs—for

example, the difficulty or inability to move personal data when shifting to a new service—and extremely powerful network effects mean that American consumers have a limited ability to "vote with their clicks." Even with great effort, it is difficult to avoid using major firms; journalist Kashmir Hill described her experiment living without any services from five nearly inescapable technology companies as "hell."[23] This lack of choice further removes incentives for dominant players to innovate to improve services.

Centralization of research and development (R&D) resources at dominant firms may additionally result in selective or reduced innovation. A lack of external competition, for instance, discourages innovation,[24] and internal research that threatens dominant business lines is often avoided, hidden, or systematically challenged.[25] There may be significant opportunity costs to having only a few big U.S. technology companies driving the direction of technological progress for the economy more broadly, especially given the competitive incentives for dominant firms.[26] Experts have also raised concerns about the national security risks of relying on only a handful of dominant global technology companies that may not prioritize U.S. national security interests and do not have sufficient competitive incentives to ensure continued innovation, performance, and efficiency.[27] There is nothing wrong with firms pursuing innovations entirely compatible with their business models. But when such R&D capacity is concentrated among only a few major technology firms with similar incentives and limited demographic diversity, there is cause for concern about whether these innovations will benefit low-wage workers, address climate change, and benefit the public interest, or whether they will continue to concentrate America's R&D efforts around issues such as selling online advertising.[28]

A lack of competition also produces pricing harms, even when the direct consumer price is zero or the upfront consumer price is competitive. Indeed, a multisided platform—for example, a website that brings together consumers, business users, and advertisers and provides a platform for sales and interaction—may charge fees to business users that are directly passed on to consumers down the line. Consumers who enjoy low prices from digital giants today might also face higher prices in the future: Incumbent firms may use price-cutting strategies or subsidies to kill potential competitors and build or maintain market power, producing lower prices in the near term but ultimately resulting in higher prices and lower quality. Amazon, for example, dropped its diaper prices by more than 30 percent, effectively curbing the growth of online retailer Diapers.com and undercutting the company whenever it dropped prices.[29] Through cross-subsidization with other business lines, Amazon was able to absorb losses on baby products in the short term, "no matter what the cost,"[30] in order to maintain its dominant market position and price-setting ability in the long term, catalyzing the forced sale of the once-burgeoning diaper retailer. In her landmark paper "Amazon's Antitrust Paradox," Lina Khan argued, "The fact that Amazon has been willing to forego profits for growth undercuts a central premise of contemporary predatory pricing doctrine, which assumes that predation is irrational precisely because firms prioritize profits over growth."[31] While many markets experience this kind of short-term corporatism, its effects in digital markets are more harmful. As noted earlier in this report, digital markets are prone to tipping, wherein one firm is likely to "win" and maintain most of the market after gaining an early lead. Firms then leverage existing dominance for further expansion, tipping, and entrenchment in adjacent markets, making the economic consequences of unchecked predatory behavior particularly high.

American small businesses are likewise harmed by a lack of competition among digital platforms. Facing few alternative choices, high switching costs, and little power to change platform conditions, American small businesses face a high degree of platform precarity: increased risk due to heavy reliance on a handful of dominant platform services over which they have little influence or recourse if problems arise, even when platforms are treating them unfairly. Dominant platforms use this knowledge to extract rent in the form of unfavorable pricing, terms, agreements, and more;[32] examples include third-party business users such as restaurants using food delivery apps, third-party retailers creating storefronts on major online retail services, and content creators monetizing their video or audio content. Small and medium-sized businesses are forced to invest significant resources to compete effectively on online platforms, but sudden, unilateral changes in terms,[33] ranking,[34] pricing,[35] design, or a sudden suspension[36] can wipe out the value of a business' investment. Even getting out of these service arrangements can be costly: Cloud services, for example, may make it cheap to transfer data into the service but charge ultra-high rates for egress fees to leave a service.[37] Worse, platforms may exploit data about a business' sales and products to develop copycat products and undercut small businesses,[38] potentially even self-preferencing first-party services through pricing, data, design, ranking, and bundling strategies.[39] Increasingly, dominant platforms' theft of content threatens internet openness and undermines small or growing firms.

American workers are also harmed under the status quo. When dominant firms drive out competitors and achieve market capture, firms become labor monopsonists,[40] meaning that they acquire disproportionate power to set and decrease wages because they face little competition that might otherwise motivate a competitive wage and safe working conditions.[41] Worker abuse is easy to disguise through the ubiquitous use of opaque business software and algorithmic management systems, which may rely on surveillance to monitor and shape worker behavior.[42] While some of these issues can be addressed through updating and robustly enforcing labor laws, the competitive failings of digital markets will continually put downward pressure on wages and working conditions in monopsonized labor markets.

A persistent lack of transparency and data asymmetry exacerbate these problems. While workers or business users may feel that abuse is occurring, it is difficult to investigate problems without greater data access. These issues are of growing importance to Americans, with 81 percent of voters saying they are "concerned about consolidation among Big Tech corporations hurting small businesses and consumers."[43]

Privacy harms

Historically, while businesses such as telephone networks have also been protected by strong network effects and high barriers to entry, online service providers are unique in that many also surveil their consumers—sometimes without consumers' awareness—and use the information they gather to manipulate user behavior to increase usage and revenue. Other companies then buy this information from surveillant firms, develop

predictive statistical models, and sell those models for wider use. The application of these models materially affects peoples' lives in ways that are often hidden from them; the resulting invasions of privacy and invisible impacts on people's health, economic prospects, education, and liberty have produced novel forms of harm to society. Due to the complex and sometimes deliberately obscured workings of online services, it can be difficult or impossible for individuals to understand, address, or even identify the origin of these harms—let alone choose a better option if one is available**.**
Unwanted and invasive data collection, processing, and sale have become standard practice in online services industries, and Americans are overwhelmingly concerned about the data platforms hold.[44] The scope and detail of corporate data collection and consumer surveillance are astounding. For example, Google reportedly has acquired information on 70 percent of all U.S. credit and debit card transactions[45] to combine with its detailed user profiles. An entire industry has grown around creating and selling constant, unwanted records of billions of people's locations at scale in gross detail:[46] One analysis found that location trackers in common, innocuous mobile phone apps were updated more than 14,000 times per day, identifying individuals' location down to within only a few yards.[47] These data are profoundly abused. Companies collect consumer contact information and movements without consent;[48] perpetuate the pretense that consumers give informed consent with the click of "I agree";[49] use deceptive disclosures and settings to trick consumers into allowing data sharing with third parties;[50] track consumers' location within a few feet inside their homes;[51] track consumers' location even after tracking is turned off;[52] develop new products using consumers' personal emails, photographs, and conversations;[53] track people's ovulation data without consent;[54] and then too frequently fail to secure the massive troves of intimate and valuable data they acquire. It is not just dominant firms engaging in this behavior: In some cases, small businesses and third-party data buyers are the worst abusers of consumer privacy.[55]

Indeed, privacy harms are acute in combination with competitive harms. Experts have shown that firms that achieve market dominance and successfully suppress competitive threats are able to lower privacy protections in order to pursue and extract greater data gains from consumers.[56] Consumers, without a reasonable choice of substitutes, are forced to put up with suboptimal privacy protections and even privacy invasions. Within digital markets, experts including Howard Shelanski have argued that "one measure of a platform's market power is the extent to which it can engage in [data usage that consumers dislike] without some benefit to consumers that offsets their reduced privacy and still retain users."[57] As illustrated by Dina Srinivasan, Facebook's pivot away from privacy protection toward privacy exploitation upon achieving monopoly status is emblematic of this power, with consumer data extraction constituting a part of the firm's "monopoly rent."[58]

The collective costs of individual privacy incursions, of which consumers are often unaware, are staggering. These costs are not just economic—although billions of dollars have been lost through corporate negligence to protect these data, especially sensitive information concerning individuals' credit, finances, and identity[59]—but also democratic, social, and humanitarian. Troublingly, Americans have changed their social and political behavior because they know they are being watched by corporations and law enforcement.[60] Ambient surveillance has chilling effects on expression, civil liberties, and freedom of movement, particularly for Black and Hispanic communities that are persistently oversurveilled and overpoliced.[61] Americans' personal interactions, behavior, and political activity have become commodities to be tracked without consent, bought, and sold. As companies reach beyond merely advertising to manipulating people's behavior,[62] the societal costs and implications are profound.

Consumer protection harms

Consumer protection issues in online services include but extend beyond traditional privacy concerns:[63] Issues with fraud, scams, manipulation, discrimination, and systemic failures in content promotion and moderation have leveled devastating individual and collective harms.

A scale-at-any-cost growth mindset,[64] overly broad interpretations of intermediary liability laws that cover the sale of physical goods,[65] and other factors have disincentivized the development of more reasonable responsibility for consumer protection. For years, lawmakers have asked e-commerce sites to stop selling unsafe, banned, fraudulent, or knock-off products and asked other websites to stop advertising them.[66] A lack of quality control makes it easy to place false listings or reviews online to scam consumers, scam businesses, damage competitors, harass victims, and divert traffic from legitimate small businesses.[67] Negligent safety standards on large platforms have enabled bad actors to commit elaborate frauds, ranging from digital advertising schemes that scam advertisers to fake accommodations listings that defraud would-be guests to marketplaces that fail to protect users from scammers at scale.[68] In some cases, the gap between self-defined platform terms and actual enforcement across these issues is apparent.[69]

Due in part to the shift to online services during the pandemic, people are facing growing threats from long-standing consumer protection and cybersecurity issues. Losses to identify fraud, for example, topped $56 billion in 2020.[70] These costs are disproportionately felt: One analysis found that "Black people, Indigenous people, and People of Color (BIPOC) are more likely to have their identities stolen than White people (21 percent compared to 15 percent), and BIPOC people are the least likely to avoid any financial impact due to cybercrime (47 percent compared to 59 percent of all respondents)."[71]

Beyond sensitive financial and identity issues, the unprecedented amount of detailed behavioral data held by online services firms also poses unique consumer protection challenges. Platforms are able to exploit behavioral shortcomings and biases among consumers in real time to a greater degree than previously feasible.[72] They may intentionally complicate the process of changing privacy settings, opting out of data collection, deleting accounts, canceling services, and more.[73] These designs may hide or misrepresent costs,[74] fee structures,[75] and data collection.[76] In a digital environment, firms are able to more fully manipulate the buyer experience, making consumer manipulation of heightened concern.[77] Some firms employ deceptive behavioral design, sometimes called "dark patterns," which have been found to successfully manipulate

> consumers into giving up time, money, or information.[78] The ability to use detailed data and pricing systems has given rise to new forms of dynamic pricing, which too often replicate long-standing biases against historically marginalized communities.[79] Nearly three-quarters of Americans think this type of personal data-driven dynamic pricing is a "major or moderate problem."[80]
>
> Online services have also given abusers and harassers more ways to locate and target victims while regularly failing to provide people with sufficient tools for preventing, curbing, or avoiding those attacks.[81] A recent poll found, "Of the types of harms people experience online, Americans most frequently cite being called offensive names (44 percent). More than 1 in 3 (35 percent) say someone has tried to purposefully embarrass them online, 18 percent have been physically threatened, and 15 percent have been sexually harassed."[82] Numerous online service companies have failed to take adequate steps to prevent these harms from occurring.[83] Over the past two years, the number of teenagers who reported encountering racist or homophobic material online almost doubled.[84] Marginalized communities—especially transgender people, immigrants, people of faith, people of color, and women of color—are disproportionately harmed through negligent or actively harmful platform business models around content and bear the brunt of their collective costs.[85]
>
> [. . .]
>
> This survey of harms is necessarily incomplete. While a full examination of online harms is beyond the scope of this report, the limited information available also speaks to the profound asymmetry and lack of transparency in the online services space. This information asymmetry—the stark lack of data accessible to government and the public compared with the mountains of data held by digital platforms—is a persistent issue across different areas of harm. Indeed, harms described below may only be the tip of the iceberg. Researchers are starved for data on online harms and competition, and many of these issues have only come to light through formal government inquiries, whistleblowing, or intrepid investigative journalism.[86]"

Question 5

On Question 5 regarding harms that consumers may not easily discern or identify, CAP encloses the following section from Marc Jarsulic's recent article "Addressing the Competitive Harms of Opaque Online Surveillance and Recommendation Algorithms" in *The Antitrust Bulletin*:[87]

> "While surveillance has negative effects on user privacy, and algorithms have had powerful effects on user attitudes and behavior, platform users have limited knowledge about how these practices operate or their impacts. As survey evidence about online privacy shows, users are uncomfortable about the way the online platforms may be gathering and using data about them, but know little about how surveillance operates. Understanding the operation and effects of recommendation algorithms requires an additional level of technical sophistication.

> These information asymmetries between platforms and users have important competitive effects. They divert users from competing platforms that do not engage in these business practices, and inhibit entry and the innovation it would stimulate, thereby helping sustain the monopoly power of dominant incumbents.
>
> [. . .]
>
> Internet users generally recognize that they can be subject to online surveillance and violations of the privacy, but a majority know little beyond that. In a 2019 Pew Research Center survey, over 72 percent of adults said that all or almost all of what they do online or using cellphones is tracked by technology firms, advertisers, and other companies. But 59 percent of those surveyed said they had little or no understanding of what companies do with the data collected.
>
> This lack of understanding is confirmed by survey data on Facebook users. Another 2019 Pew survey showed that 74 percent of Facebook users did not know that Facebook categorized their interests on a "Your ad preferences page", although they are able to view it.[88] But even if they looked, the information revealed by this page only indicates that Facebook is in the business of analyzing user behavior. It does not indicate the existence or scale of off-platform surveillance, the use of data from data-brokers, or the machine learning processes used to target users for business and political messaging. Moreover, even sophisticated Facebook users find it almost impossible to determine the extent to which Facebook has tracked their off-Facebook activity and gathered data about them. The platform's recently introduced "Off-Facebook Activity" tool apparently does little to help.[89]
>
> Because recommendation algorithms are inherently complex and operate in the background, as discussed above, their effects are difficult to discern. However, recent actions by Facebook suggest a belief that wider understanding of algorithm design could threaten platform use. While Facebook's own experiments have shown that the Newsfeed recommendation algorithm can have powerful effects on the attitudes and actions of platform users, information about its day-to-day operation and impact is not accurately described to users. When Facebook publicly described changes to the Newsfeed algorithm in 2018, they were characterized as shifting the focus from media consumption to interaction with friends and family. However, recently disclosed internal documents show that "[t]he goal of the algorithm change was to reverse the decline in comments, and other forms of engagement, and to encourage more original posting. It would reward posts that garnered more comments and emotion emojis, which were viewed as more meaningful than likes…"[90]

Questions 11 and 17

Questions 11 and 17 pertain to "commercial incentives and business models that lead to lax data security measures or harmful commercial surveillance practices" and "techniques that manipulate consumers into prolonging online activity (e.g.,video autoplay, infinite or endless scroll, quantified public popularity)." While Question 17 is focused specifically on children and teenagers, the information submitted below refers to the impact of those techniques on all users, which includes but is not specific to children and teenagers. CAP encloses the following section from Marc Jarsulic's recent article "Addressing the Competitive Harms of Opaque Online Surveillance and Recommendation Algorithms" in *The Antitrust Bulletin*:[91]

> "From the point of view of the platforms, success is not measured by number of users alone. Time spent on the platform is crucial, because use increases an individual's potential exposure to advertising and other paid messaging. Increased use also provides more detailed information about the user – who she is, what she likes, with whom connected, what she does when she is using the site, even where the cursor is moved when viewing something. Therefore, Facebook and YouTube have adopted sophisticated strategies to increase engagement by people who use their services.
>
> When someone views a video on YouTube, they are presented with a list of recommended videos to watch next. For most users, YouTube will automatically select and "auto-play" one of these recommended videos by default at the conclusion of a video. Those recommendations are generated by an algorithm which has been described, in general terms, by Alphabet data scientists. Given a user search, the algorithm first identifies a few hundred candidate videos from the billions on the YouTube platform. Next, the algorithm generates a ranked list of videos to be recommended. If the request is by a user that YouTube can identify, then it generates a "recommended-for-you" list, which incorporates past user behavior on YouTube along with demographic and other information. The extent and source of these additional data are not revealed, but Alphabet has access to a huge amount of data on individuals, described above. Other requests provide recommendations that are not individualized.
>
> YouTube says that the watch-next ranking is based on the likelihood of achieving multiple objectives, which are described as viewer engagement (clicks and watch time) and satisfaction (likes, dismissals). While the likelihoods of achieving these objectives are generated by machine learning models of user behavior on YouTube, the weights given to objectives like watch time are "manually tuned". That is, the rankings are determined by the self-interest of YouTube, which means watch time and the associated revenue are central to the ranking.[92]
>
> Although the YouTube algorithm and the data on which it is based are proprietary, there is evidence that the emphasis on watch time can influence user behavior on the site and elsewhere. Theoretical work by Google DeepMind data scientists has shown that "feedback loops in recommendation systems can give rise to 'echo chambers' and 'filter bubbles' which can narrow a user's content exposure and ultimately shift their world view." [93] Empirical research confirms that the algorithm has created this kind of attitude-reinforcing feedback. For example, a study of recommendations on YouTube informational channels showed a large increase in the relative frequency of conspiracy video recommendations at the end of 2018, peaking at nearly 10 percent. Moreover, there was clear positive correlation between the conspiracy likelihood of the source video and the conspiracy likelihood of the recommended video. Both relative frequency and correlations declined after YouTube intervened beginning in January 2019. [94]

While there is continuing debate about the scope and importance of these effects, the algorithm does appear to produce them.

Facebook likewise uses a recommendation algorithm to determine what users see on the site in their “Newsfeed”, which it describes as a “constantly updating list of stories in the middle of your home page. Newsfeed includes status updates, photos, videos, links, app activity and likes from people, Pages and groups that you follow on Facebook.” [95] The ranking of items in the Newsfeed is designed to encourage engagement and use.

One way to stimulate engagement, as Facebook CEO Mark Zuckerberg has acknowledged, is to include extreme content.[96] There is evidence that the algorithm does just that. According to internal Facebook documents obtained by the Wall Street Journal, adjustments to the weights in the Facebook algorithm in 2018, intended to increase user engagement, had the effect of rewarding outrage and lies. Fixes were proposed by Facebook engineers, but they were not implemented because they would reduce user engagement. [97] A recent academic study likewise has shown that increased referrals to news sites on Newsfeed make the dominant news sources of a user more extreme.[98]

According to other internal Facebook documents, and Congressional testimony by a former Facebook employee, the platform is also cavalier about the effect of Instagram, one of its apps, on teenage girls.[99] Evidence that the use of this app can affect mental health was apparently ignored in favor of user engagement. The role of Facebook recommendation algorithms in promoting Instagram use is unclear, but similar recommendation systems power Instagram’s Explore page.

Facebook has been aware that Newsfeed can have measurable effects on user attitudes for some time. In an experiment to test whether posts with emotional content are more engaging than those without, posts with positive emotional content were reduced in some users’ Newsfeeds. As a result, these users changed their posting behavior, producing fewer positive posts and more negative posts. The Facebook data scientists concluded this was evidence of “massive-scale emotional contagion”.[100]

Although the results of this study were published in the Proceedings of the National Academy of Sciences, the journal editor-in-chief subsequently published an “editorial expression of concern” because Facebook’s data collection “…may have involved practices that were not fully consistent with the principles of obtaining informed consent and allowing participants to opt out.”[101] In the paper itself the authors noted that the research was “…consistent with Facebook’s Data Use Policy, to which all users agree prior to creating an account on Facebook, constituting informed consent for this research”.[102]

Another Facebook experiment demonstrated that the Newsfeed can change political behavior. On the day of the 2010 Congressional elections Facebook conducted a randomized control trial of political mobilization messages, involving 61 million voters. One group of voters was shown a “social message” encouraging voting and featuring pictures of friends who clicked an “I voted” button. A second group received information

> about voting, but no social content, and a control group received no message. The social message group were more likely to vote than the informational, and even more likely to vote than the control group, with the differences being statistically significant.[103] The messaging is estimated to have increased the number of voters in the 2010 election by 340,000. In the recent Presidential election state vote totals smaller than this had decisive effects on the outcome.
>
> In summary, both YouTube and Facebook deploy sophisticated proprietary algorithms that increase user engagement and watch-time. These algorithms significantly affect what users read or view, and can measurably influence their attitudes, emotions, and behavior."

Question 12

Question 12 asks, in part, "Which commercial surveillance practices, if any, are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them?"

CAP encourages the development of clear rules that entirely prohibit or otherwise clearly limit certain harmful practices in commercial surveillance and data security. While Question 95 acknowledges the importance of being attentive to potential obsolescence, there is now a vast body of work that demonstrates that certain data surveillance and lax security practices are clearly harmful and should be prohibited.

Previously, CAP proposed anchoring any new ex ante rulemaking powers for online services with a series of key unlawful prohibitions: anti-competitive practices; violations of civil rights; insecure and data-extractive practices; and unfair, deceptive, or abusive acts or practices for consumer and business users.[104] The Commission should consider specifically enumerating and banning practices related to commercial surveillance and data security within these categories, especially for practices which pose inherent but unavoidable risks to civil rights.

Question 30

Question 30 asks if the Commission should pursue a Section 18 rulemaking on commercial surveillance and data security. CAP strongly believes that the Commission should do so. As CAP argued previously, fully maximizing the existing authorities of the Commission is an essential component of establishing consumer protections for online services:[105]

> "Existing laws, authorities, and agencies can address a subset of interlocking online services harms outlined above [Excerpt included above in this document as well]. In particular, the Center for American Progress strongly supports more aggressive antitrust action, more robust competition policies, increased privacy and civil rights capacity at the FTC, and strong federal privacy legislation or rules."

Continuing, CAP argued in favor of using ex ante regulation to address harms from online services, such as the Commission's proposed Section 18 rulemaking:[106]

> "Such proactive rule-making powers—sometimes called "ex ante" regulation—are distinct from reactive or "ex post" approaches, which are litigated after harms have occurred. Proactive rule-making could identify and prohibit harmful measures prior to significant harm or as harms are occurring."
>
> […]
>
> "Historically, after-the-fact litigation has been too slow-moving to alone address online services harms. As Americans increasingly grapple with these harms and threats to the public interest, an ad hoc approach to online services is increasingly insufficient. To anticipate technology's evolution and balance difficult trade-offs, regulators should have proactive rule-making abilities to curb problems before or as they occur. New statutory prohibitions of problematic online services practices are likewise required to set clear rules of the road, especially for stable, long-standing online services markets. In combination, a hybrid regulatory approach backed by substantial resources and oversight powers is needed to tackle the range of public interest issues raised by online services."

These sentiments echoed those of FTC Commissioner Rebecca Slaughter, who noted in her testimony before Congress in March 2021: "Effective enforcement is a complement, not an alternative, to thoughtful regulation. That is especially true for regulatory models that cannot be effectuated by ex post enforcement actions, even those with the broadest deterrent effect."[107]

While CAP believes a broader framework for ex ante rules to regulate online services is needed, a Section 18 rulemaking on commercial surveillance and data security fills a critical gap in addressing the harms from online services in this area. As noted by the Commission in the ANPR, the Commission is reaching the limits of what case-by-case enforcement and existing authorities allow. While these case-by-case decisions have created what GW Professor Daniel Solove has called "the new common law of privacy"[108] they have never been formalized or clarified more broadly. Additionally, while the Commission has made use of its existing tools, their limited resources and a pattern of industry ignoring consent decrees has led to repeated violations in this space from companies like Meta/Facebook. As former FTC Commissioner Rohit Chopra noted in 2019, "FTC orders are not suggestions."[109] The formalization of some of these rules into formal federal regulations will add additional deterrence and enforcement teeth to companies that may be otherwise willing to press the boundaries and pay a fine later.

Many commentators have noted the extra steps that the Commission must undertake to complete a Section 18 rulemaking as compared to a rulemaking under the Administrative Procedures Act. Given the scope and breadth of this topic, as outlined in the numerous questions in the ANPR, the additional process and extended ability for stakeholders to weigh in multiple times means that, if completed, a Section 18 rulemaking on Commercial Surveillance and Data Security will be the product of extensive public input and oversight. Such robust public input will provide an appropriate foundation for clear rules, prohibitions, and limitations on harmful practices going forward.

Question 31

For Question 31, asking if the Commission should undertake a Section 18 rulemaking on data security, CAP offers the following questions on categorization and process.

In considering which entities are engaged in the practices discussed in the ANPR, it's useful to group the areas of inquiry into three distinct foci: 1) commercial surveillance data collection and use, 2) commercial surveillance monetization and movement, and 3) data security practices. While commercial surveillance data collection and use and commercial surveillance monetization and movement are closely related to each other and have a narrower scope of participants and entities, data security practices are a much broader category that could potentially encompass nearly all businesses and even non-business entities that store data.

As the ANPR states, "the term "data security" in this ANPR refers to breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices."[110] By necessity, this rulemaking may have to cover all data stored by affected entities, not just data gathered by various commercial surveillance techniques. As such, the scope of stakeholders affected by a rule on data security would be huge, potentially as large as all entities that store data on consumers. Any proposed rules will have to grapple with this broad swath of entities and their varying abilities to carry-out data security rules, which may require distinct compliance regimes from more general commercial surveillance compliance.

Any proposed rules around data security would also require significant consultation with other U.S. government entities with major equities in cybersecurity, including the Cybersecurity and Infrastructure Agency (CISA) which is part of the Department of Homeland Security, the Department of Defense, the Securities and Exchange Commission, the newly created Office of the National Cyber Director, and others. Agencies that can speak to the global impacts of such a rule on multilateral cybersecurity discussions may also need to be consulted. Overall, as recent attempts to create rules around cyber reporting by CISA[111] and the SEC[112] have shown, data security rulemaking is a complicated endeavor with multiple stakeholders and competing interests.

Ultimately, it may make sense to limit the scope of a data security rulemaking to a smaller subset of entities than the commercial surveillance rulemaking. Alternatively, the Commission may wish to pursue two separate rulemakings. In either case, CAP urges the Commission to pursue a data security rulemaking strategy that does not slow or otherwise complicate its critical work pursuing a commercial surveillance rulemaking.

Question 65

Question 65 asks about the prevalence of algorithmic discrimination based on protected categories such as race, sex, and age. It inquires whether such discrimination is more pronounced in some sectors than others. CAP encloses the following section from its 2021 report, "How To Regulate Tech: A Technology Policy Framework for Online Services," discussing the broad civil rights harms stemming from the rise of online services and the commercial surveillance economy:[113]

> **"Civil rights harms**

Online services regularly introduce risks to Americans' civil rights and liberties.[114] Use of digital technologies—including software, algorithmic decision-making systems, digital advertising tools, surveillance tools, wearable technology, biometric technology, and more—have introduced new vectors to continue the deeply rooted historical exploitation of and discrimination against protected classes. Because privacy rights are also civil rights, these harms are inextricably linked to the privacy harms described above, wherein mined data feed into algorithms that are used to profile individuals, make decisions, target ads and content, and ultimately lead to discrimination.[115]

Leading scholars and advocates have exposed the numerous risks that automated decision-making systems—encompassing everything from static algorithms to machine learning to AI programs—pose to civil and human rights.[116] These systems can produce deeply inequitable outcomes, including and beyond issues of algorithmic bias.[117] Discrimination can occur at any point in the development process or produce, obfuscate, and launder discriminatory use. Already, they have resulted in a slew of civil rights violations that materially affect Americans' liberty, opportunity, and prospects. Algorithmic decision-making systems have produced and reproduced discrimination in recruiting,[118] employment,[119] finance,[120] credit,[121] housing,[122] K-12 and higher education,[123] policing,[124] probation,[125] and health care,[126] as well as the promotion of services through digital advertising[127] and beyond.[128] Algorithmic racism in particular extends the project of white supremacy in pernicious ways:[129] With a glut of consumer data and the veneer of technical objectivity, online services companies have myriad ways to discriminate among consumers and obfuscate that discrimination.[130] For instance, digital advertisers can use proxy metrics to enable discrimination in advertising without technically using protected classes,[131] although Facebook has been sued for allowing discrimination based on protected classes explicitly.[132] Insurance, credit, and financial companies can bake historical data, which reflect long-standing inequities and biases, into decision-making algorithms that enable them to reproduce systemic racism and other biases while using a seemingly "objective" algorithm that processes applications in an identical manner—churning out preferential products and opportunities for white, wealthy people as they have for decades.[133]

Technology-enabled discrimination is especially dangerous because the application of these tools can be hidden and nonconsensual, limited forms of redress exist, and technical processes are often wrongly assumed to be objective, thereby receiving inappropriate deference or insufficient scrutiny. New AI and algorithmic hiring tools, for example, have been hailed for their "efficiencies," yet are found to compound existing issues in disability-based discrimination, despite long-standing Americans with Disabilities Act protections.[134] A range of algorithmic and platform design choices can likewise enable discrimination.[135]

Facial recognition and other biometric surveillance technologies erode civil liberties, particularly for communities of color.[136] The biases in these technologies[137] and their use by law enforcement[138] have led to traumatic violations of civil liberties, including a number of recent wrongful arrests of innocent Americans who were misidentified by faulty facial recognition software.[139] But more broadly, their increasing use in public spaces and employment as tools to continue the overpolicing and oversurveillance of people of color threatens civil liberties, chills political speech, and inhibits freedom of movement and assembly.

Content moderation challenges and negligence also introduce asymmetric risks to protected classes. Platforms' failures to prevent the exploitation of social networking for purposes of harassment, discrimination, hate speech, voter suppression, and racialized disinformation have made long-standing problems newly urgent. Further, major platforms have been found to increase radicalization and participation in extremist groups.[140] At the individual level, these problems have subjected people to harm and serious duress[141] and enabled the deprivation of rights, including the right to vote.[142] Civil rights experts have drawn parallels between the discriminatory nature of these business decisions and platform designs and the public accommodation laws that protect against discriminatory practices in brick-and-mortar businesses, highlighting the need to update and reinforce current digital protections.[143]

Collectively, the sheer quantity and amplification of such civil rights-suppressing content introduces barriers to and discourages full participation in public life and cultural discourse by already excluded groups. The prevalence of false information and propaganda on social media in particular can grossly warp public discourse and societal understanding of public events. Misinformation has been used to maintain and advance racist, sexist, transphobic, and other prejudices, while "astroturfing" strategies—wherein coordinated networks of accounts, including "fake" accounts not representing "real" people, artificially inflate the popularity and visibility of certain posts—are used to misrepresent the prevalence of these attitudes. For example, despite the majority of Americans supporting Black Lives Matter, 70 percent of Facebook posts from users discussing the topic in June 2020 were critical of the movement.[144]

Beyond posing risks to specific enumerated rights and liberties for protected classes, online services have reified, maintained, and extended racism, sexism, and other social prejudices generally in the United States, through both their technology development and business model negligence. For example, Dr. Safiya Noble's pioneering work illustrated that, for years, searching "black girls" on Google returned pornographic search results and ads, whereas searches for "white girls" did not.[145] Similarly, searches of Black-identifying names disproportionately returned ads mentioning "arrests" compared with searches of white-identifying names.[146] Numerous other instances of search engine and predictive text results enhancing and extending social discrimination abound,[147] and similar problems exist in voice technologies, facial recognition, and other biometric and visual processing techniques."[148]

Question 86

Question 86 asks about the mechanisms for opacity in commercial surveillance, including technological or legal mechanisms companies rely on to shield their commercial surveillance practices from public scrutiny. While there are numerous examples of opacity in the commercial surveillance and data security markets, the following response focuses on opacity into the activity of digital gatekeepers. A major contributor to this continued opacity is the active opposition to or acquisition of third-party analytics firms or tools that seek to shed light on digital gatekeeper products. Here, CAP uses the purchase of the analytics tool Crowdtangle by Meta/Facebook as an example, drawing from its April 2021 comment submission to the DOJ/FTC RFI for Merger Guidelines.[149] It focused on the competitive impact of the loss of third party analytics firms or tools, but nonetheless provides a clear example of how opacity is maintained on large digital gatekeeper platforms:

> "As described above, many gatekeepers operate their digital properties like a one-way mirror—collecting for themselves detailed private data on the interactions amongst consumer users, business users, rivals, and more. Because of this opaqueness, entire industries have been created in response to the demand for business tools that provide insight, analytics, and monitoring of performance or activities on digital platforms. Such tools are used by their customers to better understand and adjust their participation on the platform, perhaps allowing for greater differentiation or competition. Such services operate in a difficult market position. They require either cooperation from platforms of focus or creative techniques that gather on-platform information in unauthorized (if not actively opposed) methods.[150] Some of these data collection strategies are now being examined by the courts.[151] Amidst these odds, numerous products have withered or shut down. The remainder of the industry focuses on social media content tracking, advertising analytics, and more. For the purposes of this section, these will be referred to as "third-party analytics firms."
>
> When third party analytics firms are acquired by the very platforms to which they seek to provide insight, the already limited visibility into digital platforms is significantly harmed or reduced. Acquisition removes a key independent source of information, which customers, regulators, researchers, and the public may rely on to understand activity and competition in major digital spaces. Therefore, mergers or acquisitions of tools that provide independent analysis or tracking of digital markets by their firms of focus harm competition and should be presumed to be anticompetitive.
>
> The acquisition of a third-party analytics firm called CrowdTangle is illustrative of this risk. CrowdTangle was purchased by Facebook in 2016. CrowdTangle allowed companies to gather insights across multiple social media platforms including Facebook, Twitter, Instagram, and Vine.[152] Facebook adapted CrowdTangle into a tool that allowed for monitoring, searching, and analyzing content primarily on Facebook and Instagram (though it also added Reddit later). It was made available for free to certain Facebook partners, media organizations, non-profits, and others. It was used by academics[153] and activists[154] to help support their work identifying disinformation and other harmful content on the Facebook platform. As it is a product owned by Facebook, it had better access than any other third-party analytics or monitoring tool.
>
> In 2020, *New York Times* reporter Kevin Roose began to use CrowdTangle to identify the top ten posts containing URLs from Pages on Facebook.[155] A Facebook Page is distinct from a Facebook Profile in that it is optimized for broadcast communication to large audiences on the platform. Pages facilitate one-way connections and are primarily used by celebrities, athletes, businesses, and politicians. Roose began by pulling this information manually from CrowdTangle, assembling the lists, and posting them to

Twitter. He eventually automated this process, publishing daily to a dedicated Twitter account: Facebook's Top 10.[156]

At the time, the nature of the top trending posts on Facebook garnered significant public attention, especially when those lists were dominated by political commentators. Use of CrowdTangle by Roose, journalists, academics, and researchers provided important public interest insights—which sometimes appeared to contradict what Facebook was telling the public.[157] Facebook seemed uncomfortable with the transparency and the results. Even the limited data transparency about Facebook that CrowdTangle enabled was regularly creating negative narratives for its parent company.[158]

Facebook began to argue in public that while the CrowdTangle data was technically accurate, as it was pulling from Facebook's own data as a Facebook product, it was misleading. They argued that CrowdTangle tools only measured engagement on public posts[159] (a user interacting with the content on Facebook in the form of commenting, liking, or sharing) and that the actual internal Facebook metrics showed a very different picture of the most popular content on the site. For a period of time, to rebut the picture painted by Roose's publication of the CrowdTangle data, Facebook attempted to release its own list of top performing content on the site, culled from its internal data.[160] The *New York Times* later reported that even with data broader than engagement, political commentators still dominated the most viewed content.[161]

In 2021, Facebook dissolved the CrowdTangle team. The founder and head of CrowdTangle left the company[162] and CrowdTangle announced it would pause new sign-ups for the service in 2022.[163] If CrowdTangle is shut down by Facebook, there are few, if any, tools with visibility into the site with access to officially sanctioned Facebook data. In August 2021, Facebook announced the creation of a widely viewed content report,[164] a quarterly report that aimed to provide data on the most widely viewed content on the platform in the last quarter. In March 2022, Facebook released its Q4 2021 Widely Viewed Content Report.[165] The most widely viewed page for Q4 2021 was unnamed with the notation "This Page was removed by Facebook for violating Community Standards" and no additional information or insight provided for the 121 million content views it got in that time period.[166] Reporters have suggested that the page might have been a junk page but there is no official confirmation or elucidation.[167]

Due to their stringent data restrictions, there are few tools available to examine or understand digital platforms. Acquisitions of independent third-party analytics firms by their gatekeeper platforms of focus should be disfavored due to their immense potential to shut down some of the only available, semi-transparent tools. In a highly asymmetrical information environment, the preservation of non-sensitive insights and data access may help to promote competition and advance understanding of key public interest issues. The absence of such services due to platform acquisition and degradation almost certainly harms them."

Conclusion

CAP strongly supports the Commission beginning a Section 18 rulemaking to address harms from commercial surveillance and data security. The need for ex ante regulation on these issues is a critical first step in addressing the harms from online services. It will be important for the Commission to focus on prohibiting practices that have been shown to be most harmful while allowing for flexibility in scope and innovation. On data security in particular, CAP urges the Commission to consider the differences in stakeholders and scope relative to entities impacted by rules on commercial surveillance alone. Though a significant undertaking, a Section 18 rulemaking is a long overdue and essential step to making the nation safer and more competitive. CAP applauds the Commission for its effort.

[1] U.S. Federal Trade Commission, "Trade Regulation Rule on Commercial Surveillance and Data Security," *Federal Register* 87 (161) (2022): 51273–51299, available at https://www.regulations.gov/document/FTC-2022-0053-0001.

[2] Erin Simpson and Adam Conner, "How To Regulate Tech: A Technology Policy Framework for Online Services" (Washington: Center for American Progress, 2021), available at https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/.

[3] Marc Jarsulic, "Addressing the Competitive Harms of Opaque Online Surveillance," *The Antitrust Bulletin* 67 (1) (2022): 1-13, available at https://journals.sagepub.com/doi/abs/10.1177/0003603X211066983.

[4] Catherine Shu, "Changes to Facebook Graph Search leaves online investigators in the lurch", Techcrunch, June 11, 2019, available at https://techcrunch.com/2019/06/10/changes-to-facebook-graph-search-leaves-online-investigators-in-a-lurch/.

[5] Dale Smith, "Google collects a frightening amount of data about you. You can find and delete it now", CNET, June 28, 2020, available at https://www.cnet.com/tech/services-and-software/google-collects-a-frightening-amount-of-data-about-you-you-can-find-and-delete-it-now/.

[6] Bennett Cyphers and Gennie Gebhart, "Behind the One-Way Mirror: A Deep Dive into the Technology of Corporate Surveillance" (San Francisco: Electronic Frontier Foundation, 2019) available at https://www.eff.org/wp/behind-the-one-way-mirror.

[7] Ibid, pp. 15.

[8] Sara Morrison and Rani Molla, "Google Chrome's cookie ban is good news for Google — and maybe your privacy", Vox Recode (January 16, 2020), available at https://www.vox.com/recode/2020/1/16/21065641/google-chrome-cookie-ban-advertisers.

[9] Electronic Frontier Foundation, "Am I FLoCed?," available at https://amifloced.org (last accessed September 2021); Zak Doffman, "Why You Should Delete Google Chrome After New Tracking Admission," Forbes, August 28, 2021, available at https://www.forbes.com/sites/zakdoffman/2021/08/28/stop-using-google-chrome-on-windows-10-android-and-apple-iphones-ipads-and-macs/?sh=4066abbf4a97.

[10] Cyphers and Gebhart, "Behind the One-Way Mirror", *supra*, 17.

[11] Geoffrey A. Fowler, "It's the middle of the night. Do you know who your iPhone is talking to?", The Washington Post, May 28, 2019, available at https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/.

[12] Wolfi Christl, “Corporate Surveillance in Everyday Life”, (Vienna, Austria: Cracked Labs, 2017), available at https://crackedlabs.org/en/corporate-surveillance; Laura Hautala, “Shadow profiles: Facebook has information you didn't hand over,” CNET, April 11, 2018, available at https://www.cnet.com/tech/services-and-software/shadow-profiles-facebook-has-information-you-didnt-hand-over/.

[13] Facebook (Meta), “About lookalike audiences”, available at https://www.facebook.com/business/help/164749007013531?id=401668390442328; see also Larry Kim, “5 Ridiculously Powerful Facebook Ad Targeting Strategies”, Wordstream, (last accessed July 2, 2020), available at https://www.wordstream.com/blog/ws/2015/01/28/facebook-ad-targeting.

[14] University of Vermont, “On Facebook and Twitter your privacy is at risk -- even if you don't have an account, study finds,” Science Daily, January 21, 2019, available at https://www.sciencedaily.com/releases/2019/01/190121115354.htm, summarizing results from James P. Bagrow, Xipei Liu, Lewis Mitchell, “Information flow reveals prediction limits in online social activity,” 3 *Nature Human Behaviour*, 122 (2019).

[15] Simpson and Conner, "How to Regulate Tech: A Technology Policy Framework for Online Services."

[16] See the disparate impacts in sources throughout the harms section of this report, particularly throughout the subsection titled “Civil rights harms.” See additionally U.S. Senate Select Committee on Intelligence, “On Russian Active Measures, Campaigns and Interference in the 2016 U.S Election, Volume 2: Russia’s Use of Social Media With Additional Views” (Washington: 2021), available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf; Vera Bergengruen, “Ya Basta. A New Coalition Calls on Facebook to Tackle the Spanish Misinformation Crisis,” Time, March 16, 2021, available at https://time.com/5947262/spanish-disinformation-facebook/; Federal Trade Commission, “Consumer Sentinel Network Data Book 2020,” available at https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic (last accessed October 2021); Federal Trade Commission, “Combating Fraud in African American and Latino Communities: The FTC’s Comprehensive Strategic Plan” (Washington: 2016), available at https://www.ftc.gov/system/files/documents/reports/combating-fraud-african-american-latino-communities-ftcs-comprehensive-strategic-plan-federal-trade/160615fraudreport.pdf; Anti-Defamation League Center for Technology and Society, “Online Hate and Harassment: The American Experience 2021” (New York: March 2021), available at https://www.adl.org/online-hate-2021; Emily A. Vogels, “The State of Online Harassment,” Pew Research Center, January 13, 2021, available at https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/; Galen Sherwin and Esha Bhandari, “Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform,” American Civil Liberties Union, March 19, 2019, available at https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping; Jinyan Zang, “Solving the problem of racially discriminatory advertising on Facebook” (Washington: Brookings Institution, 2021), available at https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/; Malwarebytes, “Demographics of Cybercrime Report” (Santa Clara, CA: 2021), available at https://www.malwarebytes.com/resources/2021-demographics-of-cybercrime-report/index.html; Ridhi Shetty, “Faster is Not Always Better – Disability Discrimination in Algorithm-driven Hiring Tools” (Washington: Center for Democracy and Technology, 2020), available at https://cdt.org/insights/faster-is-not-always-better-disability-discrimination-in-algorithm-driven-hiring-tools/.

[17] Committee for the Study of Digital Platforms, “Market Structure and Antitrust Subcommittee Report,” (Chicago: Chicago Booth Stigler Center, 2019), available at https://www.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure-report.pdf.

[18] U.S. House Committee On The Judiciary, “Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations - Subcommittee on Antitrust Commercial and Administrative Law of the Committee on the Judiciary,” (Washington: U.S. Congress, 2020), available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519 ; Stigler

Committee on Digital Platforms, “Final Report” (Chicago: Chicago Booth Stigler Center, 2019), available at https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf ; *Federal Trade Commission v. Facebook, Inc.*, U.S. District Court for the District of Columbia, No. 1:20-cv-03590-JEB (December 9, 2020), available at https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacted_complaint.pdf; Marc Jarsulic, “Using Antitrust Law To Address the Market Power of Platform Monopolies”(Washington: Center for American Progress, 2020), available at https://www.americanprogress.org/article/using-antitrust-law-address-market-power-platform-monopolies/ ; Marc Jarsulic and others, “Reviving Antitrust,” (Washington: Center for American Progress, 2016), available at https://www.americanprogress.org/article/using-antitrust-law-address-market-power-platform-monopolies/ ; Lina M. Khan, “Amazon’s Antitrust Paradox,” The Yale Law Journal 126 (3) (2017): 564 – 907, available at https://www.yalelawjournal.org/note/amazons-antitrust-paradox

[19] Sai Krishna Kamepalli, Raghuram G. Rajan, and Luigi Zingales, “Kill Zone” (Chicago: University of Chicago Becker Friedman Institute for Economics, 2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3555915; Elizabeth Dwoskin, “Facebook’s Willingness to Copy Rivals’ Apps Seen as Hurting Innovation,” The Washington Post, August 10, 2017, available at https://www.washingtonpost.com/business/economy/facebooks-willingness-to-copy-rivals-apps-seen-as-hurting-innovation/2017/08/10/ea7188ea-7df6-11e7-a669-b400c5c7e1cc_story.html.

[20] Massimo Motta and Martin Peitz, “Big tech mergers,” *Information Economics and Policy* (54) (2021): 100868, available at https://www.sciencedirect.com/science/article/abs/pii/S0167624520300111.

[21] Colleen Cunningham, Florian Ederer, and Song Ma, “Killer Acquisitions,” *Journal of Political Economy* 129 (3) (2021): 649–702, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3241707; The Economist, “American Tech Giants Are Making Life Tough for Startups,” June 2, 2018, available at https://www.economist.com/business/2018/06/02/american-tech-giants-are-making-life-tough-for-startups; *Federal Trade Commission v. Facebook, Inc.*, U.S. District Court for the District of Columbia, No. 1:20-cv-03590-JEB (December 9, 2020), available at https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacted_complaint.pdf.

[22] Consumer Reports, “Platform Perceptions: Consumer Attitudes on Competition and Fairness in Online Platforms” (Yonkers, NY: 2020), available at https://digital-lab.consumerreports.org/wp-content/uploads/2020/09/FINAL-CR-survey-report.platform-perceptions-consumer-attitudes-.september-2020.pdf.

[23] Kashmir Hill, “I Cut the ‘Big Five’ Tech Giants From My Life. It Was Hell,” Gizmodo, February 7, 2019, available at https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

[24] Tim Wu, “Taking Innovation Seriously: Antitrust Enforcement if Innovation Mattered Most,” Antitrust Law Journal 78 (2012): 313, available at https://scholarship.law.columbia.edu/faculty_scholarship/1767/.

[25] Karen Hao, “We read the paper that forced Timnit Gebru out of Google. Here’s what it says.”, *MIT Technology Review*, December 4, 2020, available at https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/; Daron Acemoglu, “Opinion: Breaking up Google and the rest of big tech wouldn’t be enough to fix our innovation problems,” MarketWatch, November 4, 2020, available at https://www.marketwatch.com/story/breaking-up-google-and-the-rest-of-big-tech-wouldnt-be-enough-to-fix-our-innovation-problems-11604515300?mod=home-page.

[26] Acemoglu, “Breaking up Google and the rest of big tech wouldn’t be enough to fix our innovation problems.”

[27] Ganesh Sitaraman, “The National Security Case for Breaking Up Big Tech” (New York: Knight First Amendment Institute at Columbia University, 2020), available at https://knightcolumbia.org/content/the-national-security-case-for-breaking-up-big-tech.

[28] Ashlee Vance, “This Tech Bubble Is Different,” Bloomberg Businessweek, April 14, 2011, available at https://www.bloomberg.com/news/articles/2011-04-14/this-tech-bubble-is-different?sref=qy93ZUWO

[29] Will Oremus, “The Time Jeff Bezos Went Thermonuclear on Diapers.Com,” Slate, October 10, 2013, available at https://slate.com/technology/2013/10/amazon-book-how-jeff-bezos-went-thermonuclear-on-diapers-com.html.

[30] Nadler and others, “Investigation of Competition in Digital Markets”; U.S. House Committee on the Judiciary, “Investigation of Competition in Digital Markets” at “AMAZON-HJC-00151722.”

[31] Khan, “Amazon’s Antitrust Paradox.”

[32] Lina Khan, “The Separation of Platforms and Commerce,” *Columbia Law Review* 119 (2019): 973 – 1093, available at https://awards.concurrences.com/IMG/pdf/1._the_separation_of_platforms_and_commerce.pdf?55712/971e09a98ec2b57acf922b6d70b5033dd5a43e836894d39153d3080c3704ba1b. See Part I, A: “Separate from policies that explicitly or implicitly require merchants and vendors to buy additional Amazon services, sellers worry about subtler forms of discrimination. There are numerous means by which Amazon can disfavor any particular merchant: It can suspend or shut down accounts overnight, withhold merchant funds, change page displays, and throttle or block favorable reviews.” See also Leah Nylen and Cristiano Lima, “Big Tech’s 'bully' tactics stifle competition, smaller rivals tell Congress,” Politico, January 17, 2020, available at https://www.politico.com/news/2020/01/17/big-tech-competition-investigation-100701; Emily Stewart, “How big business exploits small business,” Vox, June 30, 2021, available at https://www.vox.com/the-goods/22550608/how-big-business-exploits-small-business; Josh Dzieza, “Prime and Punishment: Dirty Dealing in the $175 Billion Amazon Marketplace,” The Verge, December 19, 2018, available at https://www.theverge.com/2018/12/19/18140799/amazon-marketplace-scams-seller-court-appeal-reinstatement; Stacy Mitchell, “Amazon Doesn’t Just Want to Dominate the Market—It Wants to Become the Market,” The Nation, February 15, 2018, available at https://www.thenation.com/article/amazon-doesnt-just-want-to-dominate-the-market-it-wants-to-become-the-market/.

[33] Karen Weise, “Prime Power: How Amazon Squeezes the Businesses Behind Its Store,” The New York Times, December 19, 2019, available at https://www.nytimes.com/2019/12/19/technology/amazon-sellers.html; Jason Del Rey, “An Amazon revolt could be brewing as the tech giant exerts more control over brands,” Vox, November 29, 2018, available at https://www.vox.com/2018/11/29/18023132/amazon-brand-policy-changes-marketplace-control-one-vendor.

[34] Tripp Mickle, “Apple Dominates App Store Search Results, Thwarting Competitors,” The Wall Street Journal, July 23, 2019, available at https://www.wsj.com/articles/apple-dominates-app-store-search-results-thwarting-competitors-11563897221.

[35] Spencer Soper, “Amazon Is Accused of Forcing Up Prices in Antitrust Complaint,” Bloomberg, November 8, 2019, available at https://www.bloomberg.com/news/articles/2019-11-08/amazon-merchant-lays-out-antitrust-case-in-letter-to-congress.

[36] Kurt Wagner, “Facebook’s Small Advertisers Say They’re Hurt by AI Lockouts,” Bloomberg, December 31, 2021, available at https://www.bloomberg.com/news/articles/2020-12-21/facebook-s-small-advertisers-say-they-re-hurt-by-ai-lockouts.

[37] Matthew Prince and Nitin Rao, “AWS’s Egregious Egress,” The Cloudflare Blog, July 23, 2021, available at https://blog.cloudflare.com/aws-egregious-egress/; Nadler and others “Investigation of Competition in Digital Markets.”

[38] European Commission, “Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon,” Press release, July 17, 2019, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291; Dana Mattioli, “How Amazon Wins: By Steamrolling Rivals and Partners,” The Wall Street Journal, December 22, 2020, available at https://www.wsj.com/articles/amazon-competition-shopify-wayfair-allbirds-antitrust-11608235127; Jack Nicas and Daisuke Wakabayashi, “Sonos, Squeezed by the Tech Giants, Sues Google,” The New York Times, January 7, 2020, available at https://www.nytimes.com/2020/01/07/technology/sonos-sues-google.html; Aditya Kalra and Steve Stecklow, “Amazon copied products and rigged search results to promote its own brands, documents show,” Reuters, October 13, 2021, available at https://www.reuters.com/investigates/special-report/amazon-india-rigging/.

[39] European Commission, "Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon," Press release, July 17, 2019, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291; Dana Mattioli, "How Amazon Wins: By Steamrolling Rivals and Partners," The Wall Street Journal, December 22, 2020, available at https://www.wsj.com/articles/amazon-competition-shopify-wayfair-allbirds-antitrust-11608235127; Jack Nicas and Daisuke Wakabayashi, "Sonos, Squeezed by the Tech Giants, Sues Google," The New York Times, January 7, 2020, available at https://www.nytimes.com/2020/01/07/technology/sonos-sues-google.html; Kalra and Stecklow, "Amazon copied products and rigged search results to promote its own brands, documents show"; Frédéric Lambert and others, "Letter to Commissioner Margrethe Vestager: Google's ongoing abuse of market power is harming consumers and digital companies all over Europe. Comparison shopping services call for vigorous actions against Google's non-compliance with the European Commission's decision in the *Google Search (Shopping)* case," November 28, 2019, available at https://www.hausfeld.com/uploads/documents/final_version_joint_letter_of_css_to_ms_vestager_on_google_shopping-non-compliance_26.11.2019.pdf; Adrianne Jeffries and Leon Yin, "Google's Top Search Result? Surprise! It's Google," The Markup, July 28, 2020, available at https://themarkup.org/google-the-giant/2020/07/28/google-search-results-prioritize-google-products-over-competitors; Mickle, "Apple Dominates App Store Search Results, Thwarting Competitors"; Adrianne Jeffries and Leon Yin, "Amazon Puts Its Own 'Brands' First Above Better-Rated Products," The Markup, October 14, 2021, available at https://themarkup.org/amazons-advantage/2021/10/14/amazon-puts-its-own-brands-first-above-better-rated-products.

[40] José Azar, Ioana Marinescu, and Marshall I. Steinbaum, "Labor Market Concentration" (Cambridge, MA: National Bureau of Economic Research, 2019), available at https://www.nber.org/papers/w24147.

[41] Council of Economic Advisers, "Labor Market Monopsony: Trends, Consequences, and Policy Responses" (Washington: White House, 2016), available at https://obamawhitehouse.archives.gov/sites/default/files/page/files/20161025_monopsony_labor_mrkt_cea.pdf.

[42] Spencer Soper, "Fired by Bot at Amazon: 'It's You Against the Machine,'" Bloomberg, June 28, 2021, available at https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out; Alexandra Mateescu and Aiha Nguyen, "Explainer: Algorithmic Management In The Workplace," Data and Society, Feburary 6, 2019, available at https://datasociety.net/library/explainer-algorithmic-management-in-the-workplace/ ; Sam Adler-Bell and Michelle Miller, "The Datafication of Employment: How Surveillance and Capitalism Are Shaping Workers' Futures without Their Knowledge" (New York: The Century Foundation, 2018), available at https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/?session=1.

[43] American Family Voices, "New Poll Shows Bipartisan Majority Of Americans Want Congress To Rein In Big Tech," Press release, October 13, 2020, available at https://www.prnewswire.com/news-releases/new-poll-shows-bipartisan-majority-of-americans-want-congress-to-rein-in-big-tech-301151327.html.

[44] Consumer Reports, "Platform Perceptions: Consumer Attitudes On Competition and Fairness in Online Platforms."

[45] Mark Bergen and Jennifer Surane, "Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales," Bloomberg, August 30, 2018, available at https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales.

[46] Justin Brookman, "Understanding the Scope of Data Collection by Major Technology Platforms" (Yonkers, NY: Consumer Reports, 2020), available at https://digital-lab-wp.consumerreports.org/wp-content/uploads/2020/05/Understanding-the-scope-of-data-collection-by-major-platforms_2020_FINAL.pdf.

[47] Jennifer Valentino-DeVries and others, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," The New York Times, December 10, 2018, available at https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[48] Daniel Shane, "Facebook collected 1.5 million users' email contacts without their knowledge," CNN Business, April 18, 2019, available at https://www.cnn.com/2019/04/18/business/facebook-email-contacts/index.html; Ryan Nakashima, "Google tracks your movements, like it or not," Associated Press, April 20, 2018, available at https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb.

[49] Anne Brunon-Ernst, "The Fallacy of Informed Consent: Linguistic Markers of Assent and Contractual Design in Some E-User Agreements," *Alicante Journal of English Studies* 28 (2015): 37–58, available at https://doi.org/10.14198/raei.2015.28.03; Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* 4 (3) (2008): 543–568, available at https://kb.osu.edu/handle/1811/72839.

[50] Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," Press release, July 24, 2019, available at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[51] Nick Statt, "Google will fix Chromecast and Google Home bug that reveals a user's location," The Verge, June 18, 2018, available at https://www.theverge.com/2018/6/18/17475766/google-home-chromecast-bug-user-location-reveal.

[52] Nakashima, "Google tracks your movements, like it or not."

[53] Douglas MacMillan, "Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail," The Wall Street Journal, July 2, 2018, available at https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442; James Vincent, "Google wants you to help train its AI by labeling images in Google Photos," The Verge, November 11, 2020, available at https://www.theverge.com/2020/11/11/21559930/google-train-ai-photos-image-labelling-app-android-update; James Vincent, "Yep, human workers are listening to recordings from Google Assistant, too," The Verge, July 11, 2019, available at https://www.theverge.com/2019/7/11/20690020/google-assistant-home-human-contractors-listening-recordings-vrt-nws.

[54] Associated Press, "Facebook reportedly received users' sensitive health data from apps: 'It's incredibly dishonest,'" CBS News, February 22, 2019, available at https://www.cbsnews.com/news/facebook-reportedly-received-sensitive-health-data-from-apps-without-consent/.

[55] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," The New York Times, January 18, 2020, available at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Valentino-DeVries and others, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret."

[56] Howard A. Shelanski, "Information, Innovation, and Competition Policy for the Internet," *University of Pennsylvania Law Review* 161 (2013): 1663–1705, available at https://scholarship.law.upenn.edu/penn_law_review/vol161/iss6/6/.

[57] Ibid.

[58] Dina Srinivasan, "The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*,"* *Berkeley Business Law Journal* 16 (1) (2019): 39, available at https://lawcat.berkeley.edu/record/1128876?ln=en.

[59] Javelin, "Total Identity Fraud Losses Soar to $56 Billion in 2020," Press release, March 23, 2021, available at https://apnews.com/article/science-business-technology-pandemics-public-health-69347fdac36544cb923022dd3df8d19d; Chris Krebs, "Survey: Americans Spent $1.4B on Credit Freeze Fees in Wake of Equifax Breach," Krebs on Security, March 22, 2018, available at https://krebsonsecurity.com/2018/03/survey-americans-spent-1-4b-on-credit-freeze-fees-in-wake-of-equifax-breach/; Megan Leonhardt, "Consumers lost $56 billion to identity fraud last year—here's what to look out for," CNBC, March 23, 2021, available at https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html.

[60] Jonathon W. Penney, “Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study,” *Internet Policy Review* 6 (2) (2017), available at https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case; Jonathon W. Penney, “Whose Speech Is Chilled by Surveillance?”, Slate, July 7, 2017, available at https://slate.com/technology/2017/07/women-young-people-experience-the-chilling-effects-of-surveillance-at-higher-rates.html; Alison Snyder, “How surveillance changes behavior,” Axios, September 7, 2019, available at https://www.axios.com/surveillance-changes-behavior-36cc1c06-bd2b-4994-8d30-c1b7c274b961.html.

[61] Georgetown Law Center on Privacy and Technology, “The Color of Surveillance: Government Monitoring of American Immigrants,” June 22, 2017, available at https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2017/; Our Data Bodies, “Data Justice and Human Rights,” available at https://www.odbproject.org/ (last accessed August 2021); Tawana Petty, “Defending Black Lives Means Banning Facial Recognition,” Wired, July 10, 2020, available at https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/; Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, “The Perpetual Line-Up: Unregulated Face Recognition in America” (Washington: Georgetown University Law School Center on Privacy and Technology, 2016), available at https://www.perpetuallineup.org/; Alvaro M. Bedoya, “Privacy as Civil Right,” *New Mexico Law Review* 50 (3) (2020): 301–319, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3599201.

[62] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019)

[63] Charlotte Slaiman, “Data Protection is About Power, Not Just Privacy,” Public Knowledge, March 3, 2020, available at https://publicknowledge.org/data-protection-is-about-power-not-just-privacy/

[64] Hannah Kuchler, “How Facebook grew too big to handle: The tech giant’s ‘growth team’ brought it over a billion users – but did it also sow the seeds for current troubles?”, Financial Times, March 28, 2019, available at https://www.ft.com/content/be723754-501c-11e9-9c76-bf4a0ce37d49.

[65] Colin Lecher, “How Amazon escapes liability for the riskiest products on its site: Who’s at fault when something you buy on Amazon goes bad?”, The Verge, January 28, 2020, available at https://www.theverge.com/2020/1/28/21080720/amazon-product-liability-lawsuits-marketplace-damage-third-party.

[66] Annie Gilbertson and Jon Keegan, “Amazon’s Enforcement Failures Leave Open a Back Door to Banned Goods—Some Sold and Shipped by Amazon Itself,” The Markup, June 18, 2020, available at https://themarkup.org/banned-bounty/2020/06/18/amazons-enforcement-failures-leave-open-a-back-door; Alexandra Berzon, Shane Shifflett, and Justin Scheck, “Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products,” *The Wall Street Journal*, August 23, 2019, available at https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990; Alexandra Berzon, Justin Scheck, and Shane Shifflett, “Senators Want Answers About Listings for Unsafe Merchandise on Amazon.Com,” The Wall Street Journal, August 29, 2019, available at https://www.wsj.com/articles/democratic-senators-want-answers-about-listings-for-unsafe-merchandise-on-amazon-com-11567101615.

[67] Jon Keegan, “Is This Amazon Review Bullshit?”, The Markup, July 21, 2020, available at https://themarkup.org/ask-the-markup/2020/07/21/how-to-spot-fake-amazon-product-reviews; Rob Copeland and Katherine Bindley, “Millions of Business Listings on Google Maps Are Fake—and Google Profits,” The Wall Street Journal, June 20, 2019, available at https://www.wsj.com/articles/google-maps-littered-with-fake-business-listings-harming-consumers-and-competitors-11561042283; Nicole Nguyen, “Fake Reviews and Inflated Ratings Are Still a Problem for Amazon,” The Wall Street Journal, June 13, 2021, available at https://www.wsj.com/articles/fake-reviews-and-inflated-ratings-are-still-a-problem-for-amazon-11623587313; Craig Silverman, “These Hugely Popular Android Apps Have Been Committing Ad Fraud Behind Users’ Backs,” Buzzfeed News, November 26, 2018, available at https://www.buzzfeednews.com/article/craigsilverman/android-apps-cheetah-mobile-kika-kochava-ad-fraud ; Greg Bensinger, “Google and Amazon List Gun Accessories for Sale, in Apparent Violation of

Their Own Policies," The Washington Post, August 6, 2019, available at https://www.washingtonpost.com/technology/2019/08/06/google-amazon-prohibit-firearm-parts-listings-its-easy-find-them-anyway/.

[68] Craig Silverman, A.C. Thompson, and Peter Elkind, "Facebook Grew Marketplace to 1 Billion Users. Now Scammers Are Using It to Target People Around the World," ProPublica, September 22, 2021, available at https://www.propublica.org/article/facebook-grew-marketplace-to-1-billion-users-now-scammers-are-using-it-to-target-people-around-the-world; Anna Merlan, "Here Are the Most Common Airbnb Scams Worldwide," Vice, January 31, 2020, available at https://www.vice.com/en/article/epgvm7/airbnb-scam-how-to-tell; Allie Conti, "I Accidentally Uncovered a Nationwide Scam Run by Fake Hosts on Airbnb," Vice, October 31, 2019, available at https://www.vice.com/en/article/43k7z3/nationwide-fake-host-scam-on-airbnb; Silverman, "These Hugely Popular Android Apps Have Been Committing Ad Fraud Behind Users' Backs."

[69] Berzon, Shifflett, and Scheck, "Amazon Has Ceded Control of Its Site."

[70] Javelin, "Total Identity Fraud Losses Soar to $56 Billion in 2020."

[71] Malwarebytes, "Demographics of Cybercrime Report."

[72] Committee on Digital Platforms, "Market Structure and Antitrust Subcommittee Report."

[73] Forbrukerrådet, "New analysis shows how Facebook and Google push users into sharing personal data," Press release, June 27, 2018, available at https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/; Forbrukerrådet, "You Can Log Out, But You Can Never Leave: How Amazon Manipulates Consumers to Keep Them Subscribed to Amazon Prime," January 14, 2021, available at https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf; Aja Romano, "How Facebook made it impossible to delete Facebook," Vox, March 22, 2018, available at https://www.vox.com/culture/2018/3/22/17146776/delete-facebook-how-to-quit-difficult.

[74] Dark Patterns, "Hidden Costs," available at https://www.darkpatterns.org/types-of-dark-pattern/hidden-costs (last accessed September 2021).

[75] Consumer Reports, "Collecting #Receipts: Food Delivery Apps & Fee Transparency" (Yonkers, NY: 2020), available at https://digital-lab.consumerreports.org/wp-content/uploads/2021/02/Food-delivery_-Report.pdf.

[76] John Brownlee, "After Lawsuit Settlement, LinkedIn's Dishonest Design Is Now A $13 Million Problem," Fast Company, October 5, 2015, available at https://www.fastcompany.com/3051906/after-lawsuit-settlement-linkedins-dishonest-design-is-now-a-13-million-problem.

[77] Ryan Calo, "Digital Market Manipulation," *The George Washington Law Review* 82 (2013): 995–1051, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703#.

[78] Alfred Ng and Sam Morris, "Dark Patterns that Mislead Consumers Are All Over the Internet," The Markup, June 3, 2021, available at https://themarkup.org/2021/06/03/dark-patterns-that-mislead-consumers-are-all-over-the-internet; Yoree Koh and Jessica Kuronen, "How Tech Giants Get You to Click This (and Not That)," The Wall Street Journal, May 31, 2019, available at https://www.wsj.com/articles/how-tech-giants-get-you-to-click-this-and-not-that-11559315900; Jamie Luguri and Lior Jacob Strahilevitz, "Shining a Light on Dark Patterns," *Journal of Legal Analysis* 13 (1) (2021): 43–109, available at https://academic.oup.com/jla/article/13/1/43/6180579; Lauren E. Willis, "Deception by Design" (Los Angeles: Loyola Law School, 2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694575#.

[79] Alex P. Miller and Kartik Hosanagar, "How Targeted Ads and Dynamic Pricing Can Perpetuate Bias," *Harvard Business Review*, November 8, 2019, available at https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias; Giuseppe Dari-Mattiacci and Francesco Parisi, "The Cost of Delegated Control: Vicarious Liability, Secondary Liability and Mandatory Insurance," *International Review of Law and Economics* 23 (4) (2003), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=343120.

[80] Consumer Reports, "Platform Perceptions."

[81] Akshay Bhargava, "Stalkerware: The Growing Hidden-Software Crisis," Forbes, August 28, 2020, available at https://www.forbes.com/sites/forbestechcouncil/2020/08/28/stalkerware-the-growing-hidden-software-crisis/; Molly

Dragiewicz and others, "Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms," *Feminist Media Studies* 18 (4) (2018): 609–625, available at https://www.tandfonline.com/doi/full/10.1080/14680777.2018.1447341; Rebecca Lewis, Alice E. Marwick, and William Clyde Partin, "'We Dissect Stupidity and Respond to It': Response Videos and Networked Harassment on YouTube," *American Behavioral Scientist* 65 (5) (2021): 735–756, available at https://journals.sagepub.com/doi/10.1177/0002764221989781; Michael Salter, "From Geek Masculinity to Gamergate: The Technological Rationality of Online Abuse," *Crime Media Culture* 14 (2017), available at https://journals.sagepub.com/doi/10.1177/1741659017690893; Tyler Kingkade and Davey Alba, "A Man Sent 1,000 Men Expecting Sex And Drugs To His Ex-Boyfriend Using Grindr, A Lawsuit Says," BuzzFeed News, January 10, 2019, available at https://www.buzzfeednews.com/article/tylerkingkade/grindr-herrick-lawsuit-230-online-stalking.

[82] Knight Foundation and Gallup, "Free Expression, Harmful Speech, and Censorship in a Digital World" (Miami: Knight Foundation, 2020), available at https://knightfoundation.org/reports/the-future-of-tech-policy-american-views/.

[83] Ryan Mac and Tariq Panja, "How Facebook Failed to Stem Racist Abuse of England's Soccer Players," The New York Times, August 11, 2021, available at https://www.nytimes.com/2021/08/11/technology/facebook-soccer-racism.html.

[84] Victoria Rideout and others, "Coping with COVID-19: How Young People Use Digital Media to Manage Their Mental Health" (San Francisco: Common Sense, Hope Lab, and California Health Care Foundation, 2021), available at https://www.commonsensemedia.org/sites/default/files/uploads/research/2021-coping-with-covid19-full-report.pdf.

[85] U.S. Senate Select Committee on Intelligence, "On Russian Active Measures, Campaigns and Interference in the 2016 U.S Election, Volume 2"; Bergengruen, "Ya Basta."; Anti-Defamation League Center for Technology and Society, "Online Hate and Harassment"; Vogels, "The State of Online Harassment"; Shelly Banjo and Bloomberg, "TikTok apologizes after being accused of censoring black users," Fortune, July 1, 2020, available at https://fortune.com/2020/06/01/tiktok-apologizes-after-being-accused-of-censoring-black-users/.

[86] A recent letter to the FTC regarding the need to protect civil rights and privacy in online commerce—authored by numerous national advocacy groups, including the Center for American Progress—drew significantly from research and analysis in this section. See Ian Weiner, "Federal Trade Commission Must Protect Civil Rights, Privacy in Online Commerce," Lawyers' Committee for Civil Rights Under Law, Press release, August 4, 2021, available at https://www.lawyerscommittee.org/federal-trade-commission-must-protect-civil-rights-privacy-in-online-commerce/

[87] Marc Jarsulic, "Addressing the Competitive Harms of Opaque Online Surveillance."

[88] Paul Hitlin and Lee Raine, "Facebook Algorithms and Personal Data" (Washington: Pew Research Center, 2019), available at https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/01/PI_2019.01.16_Facebook-algorithms_FINAL2.pdf.

[89]Natasha Lomas, "Facebook's latest 'transparency tool doesn't offer much-so we went digging," Techcrunch, February 25, 2020, available at https://techcrunch.com/2020/02/25/facebooks-latest-transparency-tool-doesnt-offer-much-so-we-went-digging/.

[90] Keach Hagey and Jeff Horowitz, "Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead", Wall Street Journal, September 15, 2021, available at https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215?st=1l56qnz84yjtmiz&reflink=desktopwebshare_permalink

[91] Marc Jarsulic, "Addressing the Competitive Harms of Opaque Online Surveillance."

[92] Paul Covington, Jay Adams, and Emre Sargin, "Deep Neural Networks for YouTube Recommendations," *RecSys '16: Proceedings of the 10th ACM Conference on Recommender Systems* (2016): 191-198, available at https://dl.acm.org/doi/10.1145/2959100.2959190; Zhe Zhao and others, "Recommending What Video to Watch Next: A Multitask Ranking System," *Proceedings of the 13th ACM Conference on Recommender Systems* (2019): 43 – 51, available at https://dl.acm.org/doi/10.1145/3298689.3346997.

[93]DeepMind, @DeepMind, March 1, 2019, 11:06 a.m. ET, Twitter, available at https://twitter.com/DeepMind/status/1101514121563041792; R. Jiang and others, "Degenerate Feedback Loops in Recommender Systems", (Ithaca, NY: arXiv, 2019) available at https://arxiv.org/pdf/1902.10730.pdf.

[94] Marc Faddoul, Guilliame Chaslot, and Hany Farid, "A Longitudinal Analysis of YouTube's Promotion of Conspiracy Videos," (Ithaca, NY: arXiv, 2020), available at https://arxiv.org/abs/2003.03318?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+arxiv%252FQSXk+%2528ExcitingAds%2521+cs+updates+on+arXiv.org%2529.

[95] Facebook, "How News Feed Works," September 29, 2021, available at https://www.facebook.com/help/1155510281178725

[96] Mark Zuckerberg, "A Blueprint for Content Governance and Enforcement", Facebook (Meta), 2018, available at https://m.facebook.com/nt/screen/?params=%7B%22note_id%22%3A751449002072082%7D&path=%2Fnotes%2Fnote%2F&refsrc=deprecated&_rdr.

[97] Hagey and Horowitz, "Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead."

[98] Brent Kitchens and others, "Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption," *MIS Quarterly* 44 (4) (2020): 1619-1650, available at https://www.darden.virginia.edu/sites/default/files/inline-files/05_16371_RA_KitchensJohnsonGray%20Final_0.pdf.

[99] Georgia Wells, Jeff Howitz, and Deepa Seetharaman, "Facebook Knows Instagram is Toxic for Teen Girls, Company Documents Show", Wall Street Journal, September 14, 2021, available at https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=series_facebookfiles; Cecilia Kang, "Facebook Whistle-Blower Urges Lawmakers to Regulate the Company", The New York Times, October 5, 2021, available at https://www.nytimes.com/2021/10/05/technology/facebook-whistle-blower-hearing.html?name=styln-facebook&region=TOP_BANNER&block=storyline_menu_recirc&action=click&pgtype=Article&variant=show&is_new=false.

[100] Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, "Experimental evidence of massive-scale emotional contagion through social networks," *Proceedings of the National Academy of Sciences* 111 (24) (2014): 8788-8790, available at https://www.pnas.org/content/111/24/8788.

[101] Inder M. Verma, "Editorial Expression of Concern: Experimental evidence of massive scale emotional contagion through social networks," *Proceedings of the National Academy of Sciences* 111 (29) (2014): 10779, available at https://www.pnas.org/content/111/29/10779.1.

[102] Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, "Experimental evidence of massive-scale emotional contagion through social networks," *supra*, at 8789.

[103] Robert M. Bond and others, "A 61-million-person experiment in social influence and political mobilization," *Nature* 489 (2012): 295-298, available at https://doi.org/10.1038/nature11421.

[104] Simpson and Conner, "How to Regulate Tech: A Technology Policy Framework for Online Services."

[105] Ibid.

[106] Ibid.

[107] Ibid.

[108] Daniel J. Solove and Woodrow Hartzog, "The FTC and The New Common Law of Privacy," *Columbia Law Review* 114 (583) (2014): 583 - 676 available at https://columbialawreview.org/wp-content/uploads/2016/04/Solove-Hartzog.pdf

[109] Office of Commissioner Rohit Chopra, "Dissenting Statement of Commissioner Rohit Chopra *In re Facebook, Inc. Commission File No. 1823109*," U.S. Federal Trade Commission, July 24, 2019, available at https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

[110] U.S. Federal Trade Commission, "Trade Regulation Rule on Commercial Surveillance and Data Security."

[111] U.S. Cybersecurity & Infrastructure Security Agency, "CISA Welcomes Input On New Cyber Incident Reporting Requirements," Press release, September 09, 2022, available at https://www.cisa.gov/news/2022/09/09/cisa-welcomes-input-new-cyber-incident-reporting-requirements

[112] U.S. Securities and Exchange Commission, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” *Federal Register* 87 (56) (2022): 16590 – 16624, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf

[113] Simpson and Conner, "How to Regulate Tech: A Technology Policy Framework for Online Services."

[114] Dominique Harrison, “Civil Rights Violations in the Face of Technological Change” (Washington: Aspen Institute, 2020), available at https://www.aspeninstitute.org/blog-posts/civil-rights-violations-in-the-face-of-technological-change/; Leadership Conference on Civil and Human Rights and others, “Civil Rights Principles for the Era of Big Data,” February 27, 2014, available at https://civilrights.org/2014/02/27/civil-rights-principles-era-big-data/#.

[116] Safiya Umoja Noble, *Algorithms of Oppression*, (New York: NYU Press 2018).; Joy Buolamwini and Timnit Gebru, “Gender Shades,” *Proceedings of Machine Learning Research* 81 (2018): 1-15, available at https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf ; Cathy O’Neil, *Weapons of Math Destruction* (New York: Penguin Random House, 2017); Danielle Keats Citron and Frank A. Pasquale, “The Scored Society: Due Process for Automated Predictions,” *Washington Law Review* 89 (2014), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209; Joy Buolamwini, “How I’m fighting bias in algorithms,” TEDxBeaconStreet, March 9, 2017, available at https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms; Mary Madden and others, “Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans,” *Washington University Law Review* 95 (1) (2017): 53–125, available at https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6265&context=law_lawreview; Sarah Myers West, Meredith Whittaker, and Kate Crawford, “Discriminating Systems: Gender, Race and Power in AI” (New York: AI Now Institute, 2019), available at https://ainowinstitute.org/discriminatingsystems.pdf; Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin’s Press, 2018).

[117] Julia Powles, “The Seductive Diversion of ‘Solving’ Bias in Artificial Intelligence,” OneZero, December 7, 2018, available at https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53.

[118] Miranda Bogen and Aaron Rieke, “Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias” (Washington: Upturn, 2018), available at https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

[119] Alina Köchling and Marius Claus Wehner, “Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development,” *Business Research* 13 (3) (2020): 795–848, available at https://link.springer.com/article/10.1007/s40685-020-00134-w.; Shetty, “Faster is Not Always Better – Disability Discrimination in Algorithm-driven Hiring Tools.”

[120] Robert Bartlett and others, “Consumer-Lending Discrimination in the FinTech Era” (Cambridge, MA: National Bureau of Economic Research, 2019), available at https://doi.org/10.3386/w25943.

[121] Lisa Rice and Deidre Swesnik, “Discriminatory Effects of Credit Scoring on Communities of Color,” *Suffolk University Law Review* 46 (3) (2013), available at https://sites.suffolk.edu/lawreview/2013/12/19/discriminatory-effects-of-credit-scoring/.

[122] Valerie Schneider, “Locked Out by Big Data: How Big Data, Algorithms, and Machine Learning May Undermine Housing Justice,” *Columbia Human Rights Law Review* 52 (1) (2020): 251–305, available at http://hrlr.law.columbia.edu/hrlr/locked-out-by-big-data-how-big-data-algorithms-and-machine-learning-may-undermine-housing-justice/; Emmanuel Martinez and Lauren Kirchner, “The Secret Bias Hidden in Mortgage-Approval Algorithms,” The Markup, August 25, 2021, available at https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

[123] Hannah Quay-de la Vallee and Natasha Duarte, "Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data" (Washington: Center for Democracy and Technology, 2019), available at https://cdt.org/insights/algorithmic-systems-in-education-incorporating-equity-and-fairness-when-using-student-data/; Adam Satariano, "British Grading Debacle Shows Pitfalls of Automating Government," The New York Times, August 20, 2020, available at https://www.nytimes.com/2020/08/20/world/europe/uk-england-grading-algorithm.html.

[124] Julia Angwin and others, "Machine Bias," ProPublica, May 23, 2016, available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?token=HM_vaeiiqqmnZ9h19EC5CdgRYKiACk6M.

[125] Cade Metz and Adam Satariano, "An Algorithm That Grants Freedom, or Takes It Away," The New York Times, February 6, 2020, available at https://www.nytimes.com/2020/02/06/technology/predictive-algorithms-crime.html.

[126] Ziad Obermeyer and others, "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," *Science* 366 (6464) (2019): 447–453, available at https://doi.org/10.1126/science.aax2342; Heidi Ledford, "Millions of Black People Affected by Racial Bias in Health-Care Algorithms," *Nature* 574 (2019): 608-609, available at https://doi.org/10.1038/d41586-019-03228-6

[127] Galen Sherwin and Esha Bhandari, "HUD Is Reviewing Twitter's and Google's Ad Practices as Part of Housing Discrimination Probe," The Washington Post, March 19, 2019, available at https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/.

[128] For a more detailed survey of harms relating to algorithmic racism, see Jane Chung, "Racism In, Racism Out: A Primer on Algorithmic Racism" (Washington: Public Citizen, 2021), available at https://www.citizen.org/article/algorithmic-racism/.

[129] Margaret Hu, "Algorithmic Jim Crow," *Fordham Law Review* 86 (2) (2017): 633–696, available at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=5445&context=flr; Yeshimabeit Milner and Amy Traub, "Data Capitalism and Algorithmic Racism" (New York: Data for Black Lives and Demos, 2021), available at https://www.demos.org/research/data-capitalism-and-algorithmic-racism; Ruha Benjamin, *Race After Technology* (Cambridge, UK: Polity, 2019); Chung, "Racism In, Racism Out."

[130] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30 (1) (2015): 75–89, available at https://journals.sagepub.com/doi/10.1057/jit.2015.5; Tressie McMillan Cottom, "Where Platform Capitalism and Racial Capitalism Meet: The Sociology of Race and Racism in the Digital Society," *Sociology of Race and Ethnicity* 6 (4) (2020): 441–449, available at https://journals.sagepub.com/doi/pdf/10.1177/2332649220949473; Milner and Traub, "Data Capitalism and Algorithmic Racism."

[131] Joseph Blass, "Algorithmic Advertising Discrimination," *Northwestern University Law Review* 114 (2) (2019), available at https://scholarlycommons.law.northwestern.edu/nulr/vol114/iss2/3; Adler-Bell and Miller, "The Datafication of Employment."

[132] Galen Sherwin and Esha Bhandari, "Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform," American Civil Liberties Union, March 19, 2019, available at https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping; Katie Benner, Glenn Thrush and Mike Isaac, "Facebook Engages in Housing Discrimination With Its Ad Practices, U.S. Says," The New York Times, March 28, 2019, available at https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html.

[133] Keats Citron and Pasquale, "The Scored Society"; Solon Barocas and Andrew D. Selbst, "Big Data's Disparte Impact," *California Law Review* 104 (671) (2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899; Milner and Traub, "Data Capitalism and Algorithmic Racism."

[134] Shetty, "Faster is Not Always Better – Disability Discrimination in Algorithm-driven Hiring Tools."

[135] Benjamin Edelman, Michael Luca, and Dan Svirsky, "Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment," *American Economic Journal: Applied Economics* 9 (2) (2017): 1–22, available at https://doi.org/10.1257/app.20160213; Yanbo Ge and others, "Racial and Gender Discrimination in Transportation Network Companies" (Cambridge, MA: National Bureau of Economic Research, 2016), available at https://www.nber.org/papers/w22776; Alex Rosenblat and others, "Discriminating Tastes: Uber's Customer Ratings as Vehicles for Workplace Discrimination," *Policy & Internet* 9 (3) (2017): 256–279, available at https://doi.org/10.1002/poi3.153.

[136] Center for Democracy Technology and others, "Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology," June 3, 2021, available at https://cdt.org/wp-content/uploads/2021/06/2021-06-03-CDT-OTI-Upturn-TLC-FINAL-Civil-Rights-Statement-of-Concerns.pdf.

[137] Buolamwini and Gebru, "Gender Shades."

[138] Garvie, Bedoya, and Frankle, "The Perpetual Line Up."

[139] Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," The New York Times, December 29, 2020, available at https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[140] Rebecca Lewis, "Alternative Influence: Broadcasting the Reactionary Right on YouTube" (New York: Data & Society, 2018), available at https://datasociety.net/library/alternative-influence/; Manoel Horta Ribeiro and others, "Auditing Radicalization Pathways on YouTube" (Barcelona, Spain: 2020), available at https://dl.acm.org/doi/10.1145/3351095.3372879; Jeff Horwitz and Deepa Seetharaman, "Facebook Executives Shut Down Efforts to Make the Site Less Divisive," The Wall Street Journal, May 26, 2020, available at https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

[141] Canadian Centre for Child Protection, "Resources and Research: Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms," available at https://protectchildren.ca/en/resources-research/csam-reporting-platforms/ (last accessed August 2021); J. Nathan Matias and others, "Reporting, Reviewing, and Responding to Harassment on Twitter" (Ithaca, NY: Women, Action, and the Media, 2015), available at https://arxiv.org/abs/1505.03359v1.

[142] Ian Vandewalker, "Digital Disinformation and Vote Suppression" (New York: Brennan Center for Justice, 2020), available at https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression.

[143] Kristen Clarke and David Brody, "It's Time for an Online Civil Rights Act," The Hill, August 3, 2018, available at https://thehill.com/opinion/civil-rights/400310-its-time-for-an-online-civil-rights-act.

[144] Kevin Roose, "Social Media Giants Support Racial Justice. Their Products Undermine It," The New York Times, June 19, 2020, available at https://www.nytimes.com/2020/06/19/technology/facebook-youtube-twitter-black-lives-matter.html.

[145] Noble, "Algorithms of Oppression."

[146] Latanya Sweeney, "Discrimination in Online Ad Delivery" (Cambridge, MA: Social Science Research Network, 2013), available at https://doi.org/10.2139/ssrn.2208240.

[147] Paul Baker and Amanda Potts, "'Why do white people have thin lips?' Google and the perpetuation of stereotypes via auto-complete search forms," *Critical Discourse Studies* 10 (2) (2013): 187–204, available at https://doi.org/10.1080/17405904.2012.744320; Issie Lapowsky, "Google Autocomplete Still Makes Vile Suggestions," Wired, February 12, 2018, available at https://www.wired.com/story/google-autocomplete-vile-suggestions/; Moin Nadeem, Anna Bethke, and Siva Reddy, "StereoSet: Measuring stereotypical bias in pretrained language models" (Ithaca, NY: 2020), available at http://arxiv.org/abs/2004.09456.

[148] Allison Koenecke and others, "Racial Disparities in Automated Speech Recognition," *Proceedings of the National Academy of Sciences* 117 (14) (2020): 7684–7689, available at https://doi.org/10.1073/pnas.1915768117; Tom Simonite, "When It Comes to Gorillas, Google Photos Remains Blind," Wired, January 11, 2018, available at https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/; Buolamwini and Gebru, "Gender Shades."

[149] Marc Jarsulic, Erin Simpson, and Adam Conner, “Strengthening Antitrust Enforcement by Modernizing Merger Guidelines,” Center for American Progress, April 21, 2022, available at https://www.americanprogress.org/article/strengthening-antitrust-enforcement-by-modernizing-merger-guidelines/

[150] The Associated Press,” Facebook Shuts Out NYU Academics’ Research on Political Ads,” NBC News, August 5, 2021, available at https://www.nbcnews.com/tech/tech-news/facebook-shuts-nyu-academics-research-political-ads-rcna1602

[151] Jeffrey D. Neuburger, “Supreme Court Vacates LinkedIn-HiQ Scraping Decision, Remands to Ninth Circuit for Another Look,” *The National Law Review* 11 (167) (2021), available at https://www.natlawreview.com/article/supreme-court-vacates-linkedin-hiq-scraping-decision-remands-to-ninth-circuit

[152] Casey Newton,” Facebook buys CrowdTangle, the tool publishers use to win the internet,” The Verge, November 11, 2016, available at https://www.theverge.com/2016/11/11/13594338/facebook-acquires-crowdtangle

[153] Christina Fan, “CrowdTangle for Academics and Researchers,” CrowdTangle, last accessed March 2022, available at https://help.crowdtangle.com/en/articles/4302208-crowdtangle-for-academics-and-researchers

[154] Chris Miles, “Using CrowdTangle for Elections Coverage,“ CrowdTangle, last accessed March 2022, available at https://help.crowdtangle.com/en/articles/2346958-using-crowdtangle-for-elections-coverage

[155] Will Oremus, “The Battle Over Facebook’s Top 10 List,” OneZero, November 14, 2020, available at https://onezero.medium.com/the-battle-over-facebooks-top-10-list-dc3fca3d799

[156] Kevin Roose and Fabio Giglietto, @FacebooksTop10, Twitter, available at https://twitter.com/FacebooksTop10

[157] Kevin Roose, “Inside Facebook‘s Data Wars,“ The New York Times, July 14, 2021, available at https://www.nytimes.com/2021/07/14/technology/facebook-data.html

[158] The Economist, ”Facebook offers a distorted view of American news,” September 10, 2020, available at https://www.economist.com/graphic-detail/2020/09/10/facebook-offers-a-distorted-view-of-american-news

[159] John Hegeman, @johnwhegeman, July 20, 2020, 7:38 PM ET, Twitter, available at https://twitter.com/johnwhegeman/status/1285358531214888960

[160] Alex Schultz, ”What Do People Actually See on Facebook in the US?”, Facebook (Meta), November 10, 2020, available at https://about.fb.com/news/2020/11/what-do-people-actually-see-on-facebook-in-the-us/

[161] Kevin Roose, “Inside Facebook‘s Data Wars,“ The New York Times, July 14, 2021, available at https://www.nytimes.com/2021/07/14/technology/facebook-data.html

[162] Kevin Roose, “Inside Facebook‘s Data Wars,“ The New York Times, July 14, 2021, available at https://www.nytimes.com/2021/07/14/technology/facebook-data.html

[163] Shivam Patel and Elizabeth Culliford, ”Meta pauses new users form joining analytics tool CrowdTangle,” Reuters, January 28, 2022, available at https://www.reuters.com/technology/meta-pauses-new-users-joining-analytics-tool-crowdtangle-2022-01-29/

[164] Anna Stepanov, ”Introducing the Widely Viewed Content Report,” Facebook (Meta), August 18, 2021, available at https://about.fb.com/news/2021/08/widely-viewed-content-report/

[165] Facebook (Meta), ”Widely Viewed Content Report: What People See on Facebook” (Menlo Park, CA: Meta, 2021), available at https://transparency.fb.com/data/widely-viewed-content-report/

[166] Ibid, available at https://transparency.fb.com/data/widely-viewed-content-report/#widely-viewed-pages

[167] Ryan Broderick, “A Curious Facebook Mystery,” Garbage Day, March 2, 2022, available at https://www.garbageday.email/p/a-curious-facebook-mystery