United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Director
Bureau of Consumer Protection

Cleveland-Marshall College of Law
Cybersecurity and Privacy Protection Conference

Keynote Remarks of Samuel Levine
Director, Bureau of Consumer Protection, Federal Trade Commission

May 19, 2022

I want to thank Brian Ray for that introduction and for inviting me to speak today. I really regret that I'm not able to join you in person, but I'm delighted to be here virtually to discuss the Federal Trade Commission's privacy and data security program and priorities. Before I begin, I want to note that my comments today are my own and do not necessarily reflect the position of the Federal Trade Commission or any individual Commissioner.[1]

I'm joining you today 21 years after former FTC Chairman Tim Muris chose a privacy conference in Cleveland as the place to announce his new privacy agenda – one calling for a significant expansion of the Commission's role in protecting consumer privacy.[2] For some historical context, that announcement came less than a month after the 9/11 terrorist attacks on the United States.

That time was relatively early in the development of the online marketplace and the overall digitization of our daily lives. Indeed, the world has changed dramatically since 2001. That year, Jeff Bezos was an online book seller without a single space flight under his belt, and Mark Zuckerberg was in high school. Google had been incorporated for a short time and had only recently begun selling advertisements associated with search keywords. And Netflix was a business that rented DVDs by mail and competed with Blockbuster Video.

Today, we live in a world in which vast numbers of products and services are connected and able to collect enormous amounts of personal data about every conceivable aspect of our lives. From turning on our internet-connected coffee makers when we wake up, to unlocking our phones through facial scans, to using navigation apps to get to work, to uploading our workouts

---

[1] I wish to thank Jim Trilling and Peder Magee for their substantial assistance in preparing these remarks. In addition, I am grateful to Aaron Alva, Stephanie Nguyen, Rashida Richardson, Olivier Sylvain, and Monica Vaca for their comments and suggestions.

[2] *See* Timothy J. Muris, former FTC Chairman, *Protecting Consumers' Privacy: 2002 and Beyond* (Oct. 4, 2001), https://www.ftc.gov/news-events/news/speeches/protecting-consumers-privacy-2002-beyond.

to fitness platforms, to monitoring the status of our online grocery orders, to walking past connected cameras, each of us is creating long and detailed data trails that businesses are collecting, using, and sharing in ways that far exceed what most of us likely expect or comprehend.

These technologies and the business models that employ them to constantly commodify and monetize our personal information have created a "surveillance economy," a concept that retired Harvard Business School Professor Shoshana Zuboff helped popularize in her 2019 book, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.[3] This sprawling, "always-on" surveillance has crept into every aspect of our lives with implications and consequences that few, if any, fully anticipated in 2001.[4] These problems continue to vex us today.

In the two decades since Chairman Muris delivered his remarks, the FTC has made privacy and data security a major priority. The Commission has built an impressive track record by aggressively using our existing law enforcement tools – Section 5 of the FTC Act, the Children's Online Privacy Protection Act ("COPPA"), the Gramm-Leach-Bliley ("GLB") Act, the Do Not Call Registry, just to name a few – to protect consumers' privacy. But the scope of today's surveillance economy calls into question whether existing tools and approaches are sufficient. In particular, I think it is fair to ask whether notice and choice can adequately protect consumer privacy in the face of all-encompassing surveillance. And a key question I want to address today is whether notice imposes too much of a burden on consumers, and whether choice is too often illusory.

In talking about privacy in 2022, we need to expand our perspective. Privacy means more than "I have nothing to hide." Rather, it is crucial we recognize that the surveillance economy imposes very real costs on individuals – including consumers, workers, and young people – as well as on our society in general, including around our critical infrastructure, our political and religious liberties, and our social cohesion.

Surveillance is also posing threats to competition in our economy. Experience has shown that a surveillance-based economy can entrench the dominance of firms with the greatest access to, and control over, personal information and the ability to attract and monetize consumer attention. These firms can leverage their power to position themselves as gatekeepers that smaller competitors must rely on to reach consumers.

*

To drill down a little deeper, I want to explain what I mean by "surveillance." I'm referring to the pervasive and comprehensive tracking of consumers' movements and behaviors

[3] *See also, e.g.*, Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133 (2017).

[4] Interestingly, Professor Zuboff cites 2001, also the year of Chairman Muris's speech, as the year surveillance capitalism started. *See* John Laidler, *High tech is watching you*, THE HARVARD GAZETTE (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/.

across virtually every aspect of our daily lives. This surveillance results in the collection and aggregation of sensitive and other personal data from disparate sources and contexts to create detailed consumer profiles that commercial entities monetize and use to make inferences and determinations about consumers, frequently without our knowledge or permission and, far too often, resulting in disparate impacts on racial minority groups or other protected classes.

Companies today collect information about all aspects of our lives. This includes, for example, information about our location and movements, our health data, the searches we conduct, the things we purchase and which sellers we purchase them from, the content we consume, who is in our social network, and more. On its own, the collection of some of this information may arguably be innocuous, but when this information is stored, aggregated, and used in ways and in contexts that most of us could never have imagined, it can lead to serious harms.

The harms stemming from surveillance are myriad, but I think of them as falling into four categories: manipulation, discrimination, exploitation, and the chilling of participation. I will discuss each in turn.

First, mass collection of data can fuel consumer manipulation and fraud. Honest marketers as well as bad actors can weaponize data to predict which types of techniques are likely to be most effective against an individual consumer. This can result in individual consumers being presented with the particular form of "dark pattern" that is most likely to manipulate or even deceive them into unintended actions they do not realize or anticipate, such as allowing more data collection or signing up for a subscription.

Mass data collection can also result in individual consumers being targeted for particular scams based on inferences about them. For example, a United States Senate report pointed to data brokers selling data sets that can be used to target consumers based on their categorization into groups such as "Rural and Barely Making It" or "Ethnic Second-City Strugglers."[5] As one illustration of how this targeting might play out, a list brokerage firm recently pleaded guilty to knowingly providing lists of potential victims to fraudulent mass-mailing schemes that tricked older adults and other consumers into paying fees for bogus cash prizes and "psychic" services.[6] In short, our surveillance economy is making it easier for unscrupulous firms to prey on consumers.

---

[5] *See* Justin Sherman, *Data Brokers Are a Threat to Democracy*, WIRED (Apr. 13, 2021), https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/, citing U.S. Senate Comm. on Commerce, Science, and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (Dec. 18, 2013), *https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a*.

[6] *See* Press Release, U.S. Dep't of Justice, *List Brokerage Firm Pleads Guilty to Facilitating Elder Fraud Schemes* (Sept. 28, 2020), https://www.justice.gov/opa/pr/list-brokerage-firm-pleads-guilty-facilitating-elder-fraud-schemes. *See also, e.g.*, Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y. TIMES (May 20, 2007), https://www.nytimes.com/2007/05/20/business/20tele.html (noting that a large data broker sold lists of names and personal information of older American consumers to known scam artists who contacted and tricked the consumers into revealing their banking information; lists called "Suffering Seniors" and "Oldies but Goodies" contained 4.7 million people with cancer or Alzheimer's disease, and 500,000 gamblers over 55 years old, respectively).

A second category of harm is discrimination, and in particular, the use of data to shape what information we see, what opportunities we are presented with, and the outcomes we experience. Companies use our data to make inferences about us and to serve us ads or other content based on those inferences. This pervasive practice, which some have called "boxing," limits consumers' exposure to other views and information, including content as well as offers for products and services.[7] And there is no avoiding this type of harm – often consumers have no idea this is happening, and no idea what information they may be missing out on. In the commercial context, this can mean that certain services are simply not offered to certain groups. And in the political context, it is easy to see how this practice can fuel polarization.[8]

Another key concern around discrimination is the use of automated decision-making systems that rely upon personal information to differentiate consumers. For example, these systems may base distinctions on protected characteristics such as race or age. There have been reports of automated systems replicating existing biases and leading to discriminatory outcomes that harm historically undeserved groups.[9] Reproducing and reinforcing discrimination in the digital world is a trend that should concern us all, and it's a direct outgrowth of our surveillance economy.

A third category of harm is exploitation, especially against young people, workers, and our society at large.

Let's start by discussing the exploitation of young people. Children and teens are least able to recognize potential harms of online activity and the digital world, including the repercussions of sharing their information.[10] And firms that rely on surveillance-based business models have a financial incentive to keep young people engaged, which can lead to addiction and other serious harms. While COPPA cuts off its protections at age 13, we know that the harms of digital surveillance are affecting teens, too.

Digital surveillance is also becoming increasingly common in the workplace, a trend that threatens to undermine workers' dignity and allow firms to exploit the power imbalance between employees and employers. Imagine being required, as a condition of employment, to submit to having your physical movements or biometric data tracked throughout your workday. How many seconds has your keyboard been idle? What tone of voice did you use when speaking on the phone? How many times did you use the restroom? In some cases, there may be legitimate safety concerns that lead to monitoring workers; however, as some have observed, justifications such as improved efficiency and productivity are vague and may frequently be misguided. This can be especially true when surveillance is coupled with automated management technologies that

---

[7] *See* Privacy & Info. Sec. Law Blog, Hunton Andrews Kurth, *Boxing and Concepts of Harm: Are Consumers Suffering a TKO on Content?* (Oct. 5, 2009).

[8] *See, e.g.*, Transcript, FTC Hearing, *The FTC's Approach to Consumer Privacy* (Apr. 9, 2019), at 211-12 (remarks of Laura Moy), https://www.ftc.gov/news-events/events/2019/04/ftc-hearing-12-ftcs-approach-consumer-privacy.

[9] *See*, *e.g.*, Ziad Obermeyer, et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, SCIENCE Vol. 366 at 447-453 (Oct. 24, 2019). *See generally* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*,104 CAL. L. REV. 671 (2016).

[10] *See*, *e.g.*, Transcript, FTC Workshop, *The Future of the COPPA Rule* (Oct. 7, 2019), at 12 (remarks of Dr. Jenny Radesky), https://www.ftc.gov/news-events/events/2019/10/future-coppa-rule-ftc-workshop.

evaluate worker performance. And, as the costs of these technologies continue to fall, we can expect that workplace surveillance will likely intensify.[11]

Finally, the surveillance economy provides an opportunity for bad actors to exploit security vulnerabilities. The accumulation and maintenance of massive stores of consumer data creates an inviting target to cyber threat actors – including both private entities seeking to monetize stolen data, as well as hostile state actors seeking to undermine a rival. Too often companies fail to implement even rudimentary security measures, thereby putting consumers at risk of financial loss, identity theft, blackmail, and reputational and other harms. Further, lack of reasonable data security jeopardizes our critical infrastructure and national security as we have recently seen with attackers disrupting access to U.S. fuel and food supplies.[12]

The final category of harm is difficult to define, but easy to understand. We are seeing how surveillance threatens to chill our ability as individuals to seek needed healthcare, participate in the political process, or exercise our religious freedom. Consider the impact that mass collection of geolocation data is already having.

This data can reveal incredibly sensitive information, such as when and where we seek medical care. There are recent media reports of data brokers selling location information revealing that consumers had visited abortion clinics.[13] And it is not difficult to imagine that fear of similar surveillance could discourage an individual from seeking needed treatment for addiction or a mental disorder. This type of surveillance can also chill participation in civil and political discourse or religious practice.[14] For example, some have raised concerns that location data collected through Muslim prayer apps may be sold to data brokers that in turn pass it on to other entities, and it is easy to see how this type of practice could have a chilling effect on our religious freedom.[15] In short, surveillance is a direct threat to our liberty and autonomy.

*

The harms I just described should, by now, feel familiar. And equally familiar is the traditional approach to combating these harms – giving consumers notice of what information is being collected, and giving them a choice whether to consent. Indeed, a key focus of former Chairman Muris's remarks two decades ago was making sure that websites posted privacy

---

[11] *See* Kathryn Zickuhr, *Worker surveillance is becoming the new normal for U.S. Workers*, WASH. CTR. FOR EQ. GROWTH (Aug. 18, 2021), https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/.

[12] *See* Arielle Waldman, *FBI: Ransomware hit 659 critical infrastructure entities in 2021*, TECHTARGET (Mar. 24, 2022), https://www.techtarget.com/searchsecurity/news/252515076/FBI-Ransomware-hit-649-critical-infrastructure-entities-in-2021.

[13] *See* Geoffrey A. Fowler & Tatum Hunter, *Your phone could reveal if you've had an abortion*, WASH. POST (May 4, 2022), https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/.

[14] *See* Zak Doffman, *Black Lives Matter: U.S. Protestors Tracked By Secretive Phone Location Technology*, FORBES (June 26, 2020), https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=762325444a1e.

[15] *See* Joseph Cox, *Leaked Location Data Shows Another Muslim Prayer App Tracking Users*, MOTHERBOARD, TECH BY VICE (Jan. 11, 2021), https://www.vice.com/en/article/xgz4n3/muslim-app-location-data-salaat-first.

policies. But given the pervasive and unavoidable nature of today's surveillance economy, I think we need to ask ourselves whether this traditional notice and choice framework is really capable of meeting this moment.

Let's begin by scrutinizing "notice" more closely. Notice is an important concept – we expect companies to be transparent about how they are collecting consumers' information. But a privacy regime that relies on notice alone places far too much burden on consumers. Consumers lack the time to review lengthy privacy notices of their various devices, applications, or services,[16] each of which has its own specific data practices. These notices are often vague and confusing even for careful readers, and they can be outright impenetrable to the average consumer.[17] To name just one example, it is unreasonable to expect consumers to navigate the intricacies of what data a company's algorithm uses and how that use will affect the consumer today and in the future.

Even in the rare instances when notices are understandable, they might simply inform consumers that the company collects anything and everything it can, and can do with it whatever it wants. These notices can also be subject to repeated change, putting the consumer in the impossible situation of having to constantly monitor their products and services for amended terms and policies.

Another weakness of notice-based regimes is that many of the entities involved in the collection, aggregation, and monetization of personal data are not consumer-facing. Consumers are unaware of, or know little about, the data brokers and third parties who collect and broker consumer data or build consumer profiles based on inferences from this data.[18]

Some of you might have seen the recent episode of *Last Week Tonight with John Oliver*, in which the comedian refers to data brokers as the "middlemen of surveillance capitalism."[19] I think this is an apt characterization, and that it is unreasonable to burden consumers with the Sisyphean task of identifying these middlemen in order to track down and learn about their information practices.

Even if consumers could somehow overcome this obstacle, seldom can they do anything about it. That is because several elements of today's surveillance economy render meaningful

---

[16] *See* Kevin Litman-Navarro, *Opinion: We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html; Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-theprivacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[17] *See* Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[18] *See generally* FTC, *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission* (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[19] *Last Week Tonight with John Oliver* (Apr. 10, 2022).

choice illusory. First, given the digitization of our society, take it or leave it "choice" for many services is really no choice at all. In other words, for most consumers, the "choice" of whether to accept a company's terms of service or forego the service altogether is a false one.

It should be obvious by now that most consumers can't opt out of booking an airline reservation, conducting a job search, or connecting with friends and colleagues on social media. And the pandemic further increased our dependence on online services, ranging from remote learning, to teleworking, signing up for a COVID vaccine, or refilling a prescription online.[20] When we're expecting consumers to have to choose between participating in the digital economy and protecting their privacy, we're not giving them a choice at all – what we're really describing is coercion.

Even when consumers do have a real choice, our surveillance economy has led to companies getting very good at shaping what choices we make. We are increasingly seeing businesses use practices like "dark patterns" to manipulate or trick consumers into "choosing" to allow more data collection and forgoing more privacy-protective settings.[21] This can lead to a vicious cycle, where firms collect more and more data on us, which gives them more and more power to manipulate us further.

And finally, even if consumers did have a real choice to reject a product or service, and even if consumers could overcome the sophisticated dark patterns that are shaping our decisions, we still face the simple reality that in many key digital markets, there just aren't that many players to choose from – we can't vote with our feet.

All in all, I think it's clear that the notice and choice framework that has guided us for decades is no match for the realities of contemporary surveillance. We can no longer persist with the fiction that consumers can read thousands of pages of legalistic privacy notices, especially when businesses may change these notices at will. Nor should we accept the falsehood that consumers have a real choice when it comes to accessing digital tools and services. Simply put, in an economy increasingly fueled by mass commercial surveillance, it is no longer viable to count on consumers alone to protect themselves. That's why it's critical that we – as well as legislators and policymakers across state and federal governments – develop a new approach.

*

Now that I've painted an alarming picture of our world of ever-on surveillance, I want to turn to what the FTC is doing to establish rules of the road for protecting consumers and their data, to enforce the law against violators, and to study and publish research on opaque practices that are having profound effects on consumers. I'll describe each effort in turn.

---

[20] *See generally, e.g.*, Colleen McClain, et al., *The Internet and the Pandemic*, PEW RES. CTR. (Sept. 1, 2021), https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/.

[21] *See generally* U.K. Competition & Mkts. Auth. Discussion Paper, *Online Choice Architecture: How digital design can harm competition and consumers* (Apr. 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf; Transcript, FTC Workshop, *Bringing Dark Patterns to Light* (Apr. 29, 2021), https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop.

First, the Commission noted last year that it is considering initiating rulemaking to address commercial surveillance and lax data security practices.[22] While we applaud congressional efforts to pass comprehensive privacy legislation, the harms stemming from mass surveillance are becoming too pervasive to ignore, and Chair Khan has made clear that we're prepared to use every tool we have to protect people's privacy.[23]

Second, we are inventorying our existing rules to make sure we're doing everything we can to protect consumers. Over the last few months, under Chair Khan's leadership, the Commission finalized revisions to the GLB Safeguards Rule to provide a clear roadmap for financial institutions around information security, and to ensure that executives are making data protection a top priority.[24] The Commission also recently issued a policy statement affirming that the Health Breach Notification Rule ("HBNR") applies to health apps and connected devices that collect or use consumers' health information. [25] Additionally, we are in the midst of comprehensively reviewing the COPPA Rule. [26] And in an open meeting later today, the Commission plans to vote on a policy statement announcing the agency's prioritization of COPPA enforcement as it applies to education technology.[27]

In addition to taking aggressive action on the policy front, the FTC continues to hold accountable those who engage in unlawful surveillance, and enforcement in this area is a top priority for the agency.

Section 5 of the FTC Act enables us to address a wide range of deceptive or unfair practices that harm consumers. And you can draw out a couple of key principles from our enforcement actions.

First, don't deceive consumers about how their data will be collected, used, or shared. Our surveillance economy can make mass information collection and use feel like an imperative for many businesses, but we will not hesitate to take action against firms that break their promises in pursuit of profits. The Commission's recent case against Flo Health, Inc. is just one

---

[22] *See* Office of Mgmt. and Budget Office of Info. and Regulatory Affairs, RIN 3084-AB69 (Fall 2021), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69.

[23] *See* Lina M. Khan, FTC Chair, *Remarks As Prepared for Delivery*, IAPP Global Privacy Summit 2022 (Apr. 11, 2022), https://www.ftc.gov/news-events/news/speeches/remarks-chair-lina-m-khan-prepared-delivery-iapp-global-privacy-summit-2022.

[24] *See* Press Release, FTC, *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches* (Oct. 27, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data.

[25] *See* Press Release, FTC, *FTC Warns Health Apps and Connected Device Companies to Comply With Health Breach Notification Rule* (Sept. 15, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data.

[26] *See* Press Release, FTC, *FTC Seeks Comments on Children's Online Privacy Protection Act Rule* (July 15, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule.

[27] *See* Press Release, FTC, *FTC Announces Tentative Agenda for May 19 Open Commission Meeting* (May 12, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-announces-tentative-agenda-may-19-open-commission-meeting.

recent example of the Commission taking action to address false privacy promises. In that case, the Commission alleged that that the company pledged to keep private the reproductive health information it collected from consumers, while in reality, the company's app disclosed that information to Facebook, Google, and other third parties.[28]

Second, if your privacy and data security practices can cause harm to consumers, the FTC can take action – regardless of whether these practices are disclosed. The FTC Act defines unfair practices as those that cause or are likely to cause consumers substantial harm that is neither reasonably avoidable nor outweighed by countervailing benefits to consumers or competition.[29] The FTC has used this authority to address harmful practices ranging from unreasonable data security,[30] to the distribution of software that likely caused consumers to inadvertently share their files,[31] to the surreptitious activation of webcams on leased computers placed in consumers' homes,[32] to the selling of Social Security numbers and other sensitive data to known fraudsters.[33]

You can expect that the Commission's unfairness authority will be a key tool as we work to curb harmful commercial surveillance practices. For example, some companies have taken the position that they can change their data collection practices at will, even after consumers already rely on the provided product or service. Such conduct underscores how consumer choice can be illusory, and how companies can abuse the power they enjoy over consumers. But firms should think twice before exercising this power. Making retroactive changes to how a business treats data it has already collected can be an unfair practice,[34] and the Commission will be closely monitoring the marketplace for this type of conduct.

---

[28] *See*, *e.g.*, Complaint, *In re Flo Health, Inc.*, FTC File No. 192 3133 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[29] *See* 15 U.S.C. § 45(n).

[30] *See*, *e.g.*, Complaint, *In re InfoTrax Sys., L.C.*, FTC File No. 162 3130 (Dec. 30, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3130-infotrax-systems-lc; Complaint for Permanent Injunction & Other Relief., *FTC v. Equifax, Inc.*, No. 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf; First Amended Complaint for Injunctive and Other Relief, *FTC v. Wyndham Worldwide Corp.*, No. 12-1365 (D. Ariz. Aug. 9, 2012), https://www.ftc.gov/legal-library/browse/cases-proceedings/1023142-x120032-wyndham-worldwide-corporation.

[31] *See*, *e.g.*, Complaint, *FTC v. FrostWire LLC*, No. 1:11-cv-23643 (S.D. Fla. Oct. 7, 2011), https://www.ftc.gov/legal-library/browse/cases-proceedings/112-3041-frostwire-llc-angel-leon.

[32] *See*, *e.g.*, Complaint, *In re DesignerWare, LLC*, F.T.C. File No. 112 3151 (Apr. 11, 2013), https://www.ftc.gov/legal-library/browse/cases-proceedings/112-3151-designerware-llc-matter; Complaint, *In re Aaron's, Inc*., F.T.C. File No. 122 3256 (Mar. 10, 2014), https://www.ftc.gov/legal-library/browse/cases-proceedings/122-3256-aarons-inc-matter.

[33] *See*, *e.g.*, *FTC v. Sequoia One, LLC*, No. 2:15-cv-01512 (D. Nev. Aug. 7, 2015), https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3253-x150055-sequoia-one-llc; Complaint, *FTC v. Sitesearch Corp.*, No. CV-14-02750-PHX-NVW (D. Ariz. Dec. 22, 2014), https://www.ftc.gov/legal-library/browse/cases-proceedings/142-3192-x150060-sitesearch-corporation-doing-business-leaplab.

[34] *See* Complaint, *In re Facebook, Inc.*, FTC File No. 092 3184 (July 27, 2012), https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter; Complaint, *In re Gateway Learning Corp.*, FTC File No. 042 3047 (Sept. 10, 2004), https://www.ftc.gov/legal-library/browse/cases-proceedings/042-3047-gateway-learning-corp-matter.

We are also concerned about companies collecting sensitive personal information that they don't actually need. This is of particular concern when information is being collected from young people. The COPPA Rule explicitly prohibits covered businesses from conditioning a child's participation in an activity on the child disclosing more personal information than is reasonably necessary to participate in the activity. Similarly, under certain circumstances, this practice may also be unfair under Section 5 of the FTC Act.[35]

The FTC will also not hesitate to use its unfairness authority to target online discrimination. For example, the use or sale of algorithms or artificial intelligence systems that rely on surveillance data to inform hiring decisions may lead to discriminatory outcomes based on race or other legally protected status. I would encourage anyone interested in this issue to read the recent statement by Chair Khan and Commissioner Slaughter about the Napleton Automotive Group case, in which they detailed how discrimination can be an unfair practice under the FTC Act.[36]

In addition to the FTC Act, the Commission will continue to enforce the Fair Credit Reporting Act ("FCRA") to help stop unlawful data practices that can impede consumers from obtaining housing, loans, and employment.[37] To support those efforts, the agency recently filed amicus briefs urging two federal circuit courts to overturn flawed lower court decisions that would improperly limit our ability to hold consumer reporting agencies accountable for placing incorrect information on consumers' credit reports[38] and otherwise complying with the FCRA.[39] The FCRA is a decades-old tool, but it remains a critical one for protecting consumers.

Now that I've described some of the Commission's authorities, I want to touch on how the FTC is using these tools in our enforcement actions, particularly over the last year under Chair Khan.

When we bring enforcement actions, we are committed to obtaining strong, forward-leaning remedies that not only cure the underlying harm but also reverse structural incentives to maximize information collection and abuses. This starts with the simple principle that companies

---

[35] *See, e.g.*, Complaint, *FTC v. Vizio, Inc.*, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) (alleging that it was an unfair practice for the company to comprehensively collect and share consumers' sensitive television-viewing information contrary to their reasonable expectations and without their consent), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3024-vizio-inc-vizio-inscape-services-llc.

[36] Joint Statement of Chair Lina M. Khan and Commissioner Rebecca Kelly Slaughter, *In re Napleton Auto. Group*, FTC File No. 202 3195 (Mar. 31, 2022), https://www.ftc.gov/news-events/news/speeches/joint-statement-chair-lina-m-khan-commissioner-rebecca-kelly-slaughter-matter-napleton-automotive.

[37] *See, e.g.*, Press Release, FTC, *FTC, DOJ Obtain Ban on Negative Option Marketing and $21 Million for Consumers Deceived by Background Report Provider MyLife* (Dec. 16, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-doj-obtain-ban-negative-option-marketing-21-million-consumers-deceived-background-report.

[38] *See* Press Release, FTC, *FTC Joins Amicus Brief Opposing Liability Shield for Sloppy Credit Reports* (May 6, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-joins-amicus-brief-opposing-liability-shield-sloppy-credit-reports.

[39] *See* Press Release, FTC, *FTC Chair and CFPB Director Issue Joint Statement on Amicus Brief Filed in Henderson v. The Source for Public Data, L.P.* (Oct. 14, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-chair-cfpb-director-issue-joint-statement-amicus-brief-filed-henderson-v-source-public-data-lp.

should not be able to profit from illegal data practices. That's why we are committed to not only requiring the deletion of unlawfully obtained data,[40] but also the deletion of algorithms and other work product derived from the data.[41]

Where appropriate, we will also require businesses to limit their data collection altogether. An example of this approach is in our pending proposed order against the online merchandise platform CafePress. I encourage all of you to review that order carefully, as it includes some novel and important remedies.[42] The proposed order not only requires CafePress to establish a comprehensive security program, but it also places an affirmative requirement on the company to limit the information it collects from consumers. This relief underscores how privacy and security are increasingly interrelated concepts – information that is never collected can't be compromised. And it is a clear signal that the Commission will not limit its tools to consent-based remedies.

Finally, in appropriate cases, we will not hesitate to hold individuals accountable. We have recently held individuals liable for their roles in some of the unlawful activities I have described today.[43] Among other things, doing so helps to deter future unlawful conduct. The revised GLB Safeguards Rule I described earlier similarly fosters accountability by requiring covered financial institutions to designate a single qualified individual to oversee their information security programs and report periodically to the board of directors or a senior officer in charge of information security.[44]

---

[40] *See*, *e.g.*, Press Release, FTC, *FTC Finalizes Order Banning Stalkerware Provider from Spyware Business* (Dec. 21, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-finalizes-order-banning-stalkerware-provider-spyware-business; Press Release, FTC, *FTC Finalizes Settlement with Company that Misled Consumers about how it Accesses and Uses their Email* (Dec. 17, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/12/ftc-finalizes-settlement-company-misled-consumers-about-how-it-accesses-uses-their-email.

[41] *See* Press Release, FTC, *FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data* (Mar. 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive; Press Release, FTC, *California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App* (Jan. 11, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo; Press Release, FTC, *FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield* (Dec. 6, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving-consumers-about-collection-facebook.

[42] *See* Press Release, FTC, *FTC Takes Action Against CafePress for Data Breach Cover Up* (Mar. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

[43] *See*, *e.g.*, Press Release, FTC *Finalizes Order Banning Stalkerware Provider from Spyware Business* (Dec. 21, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-finalizes-order-banning-stalkerware-provider-spyware-business; Press Release, FTC, *FTC, DOJ Obtain Ban on Negative Option Marketing and $21 Million for Consumers Deceived by Background Report Provider MyLife* (Dec. 16, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-doj-obtain-ban-negative-option-marketing-21-million-consumers-deceived-background-report; Press Release, FTC, *FTC Finalizes Settlement with Utah Company and its former CEO over Allegations they Failed to Safeguard Consumer Data* (Jan. 6, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/01/ftc-finalizes-settlement-utah-company-its-former-ceo-over-allegations-they-failed-safeguard-consumer.

[44] 16 C.F.R. Part 314.

I've now described our policy and enforcement work in some depth, but I want to touch on two other tools that are sometimes overlooked.

First, the FTC has authority under Section 6(b) of the FTC Act to comprehensively study markets, and we are using this authority to shine a light on opaque data practices. For example, the Commission recently published a major report on the privacy practices of internet service providers,[45] and also issued Section 6(b) orders requiring social media and video streaming services to provide information about their data practices.[46] One of the FTC's earliest achievements – more than a century ago – was issuing a groundbreaking report on the meatpacking industry, a report that led to major reforms.[47] I expect that our ability to inform policy through rigorous study and reporting will only grow in importance.

Second, our mandate at the FTC is not only protecting consumers but also ensuring fair competition. And that makes sense. Our efforts to protect consumers from always-on surveillance can succeed only in a tech marketplace that is vibrant and competitive. That is why we are closely coordinating our consumer protection efforts with the FTC's Bureau of Competition to ensure that we are considering harms to competition in addition to consumer harms.

*

I want to conclude in the same place I began, by reflecting on how the world has changed since Chairman Tim Muris announced his privacy agenda two decades ago.

The data collection and use landscape that Chairman Muris described here in Cleveland in 2001 pales in comparison to the staggeringly expansive surveillance that consumers confront today. And unfortunately, the privacy harms that Chairman Muris cited then – harms like identity theft and the illegal collection of children's personal information – have only grown worse. At the same time, new threats have emerged that can harm individual consumers, as well as our society at large.

Prompting companies to post online privacy policies made sense when most consumers' online activity likely included visits to only a limited number of websites. But today we live in a very different world, one in which consumers' online lives are far more robust and subject to far more invisible data collection and use.

The pervasiveness of contemporary surveillance requires a new paradigm. One that recognizes that our existing tools, in their current form, are insufficient. One that acknowledges

---

[45] *See* Press Release, FTC, *FTC Staff Report Finds Many Internet Service Providers Collect Troves of Personal Data, Users Have Few Options to Restrict Use* (Oct. 21, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-staff-report-finds-many-internet-service-providers-collect-troves-personal-data-users-have-few.

[46] *See* Press Release, FTC, *FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information* (Dec. 14, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services-seeking-data-about-how-they-collect-use.

[47] *See* Report of the Federal Trade Commission on the Meat-Packing Industry (June 30, 1919).

the serious harms being inflicted on our privacy, our communities, and our society by mass commercial surveillance. And one that dispenses with the fiction that consumers can protect themselves by reading notices or opting out of the digital economy.

Fortunately, I work at an agency uniquely positioned to confront these 21st century challenges. As Chair Khan noted yesterday in testimony before Congress, we are a small agency tasked with protecting consumers and competition throughout our economy, and we urgently need more resources to fully deliver on our mission.[48] Nevertheless, with our talented and expert staff, our flexible authority, and our mandate to protect both consumers and competition, the FTC will continue to leverage every tool we have to combat the harms associated with the surveillance economy. We will also look for ways to work with Congress and state legislatures as they consider additional measures to protect consumer privacy and data security, and curb the rising tide of surveillance.

I appreciate the opportunity to share these remarks with you today, and I look forward to hearing your thoughts and answering your questions.

[48] *See* Press Release, FTC, *FTC Chair Lina M. Khan Testifies Before House Appropriations Subcommittee* (May 18, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-chair-lina-m-khan-testifies-house-appropriations-subcommittee.