UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

Remarks of Chair Lina M. Khan[1]
As Prepared for Delivery
IAPP Global Privacy Summit 2022
Washington, D.C.

April 11, 2022

Thanks so much to Trevor Hughes and the IAPP members for the invitation to speak today. It's a tremendous honor to be with you all.

It's a striking moment to be discussing the state of data privacy and security today, with the landscape having shifted so significantly even over the last few years. The pandemic hastened the digitization of our economy and society, further embedding digital technologies deeper into our lives, with schools, workplaces, and all manner of life switching over to virtual formats effectively overnight. We also saw that this digital transition was not experienced equally by all Americans, since many still lack access to reliable internet and affordable personal technologies.[2] The experience of the last couple of years has both illustrated the tremendous benefits of these tools as well as the challenges and risks posed by this growing dependence.

We've seen how security vulnerabilities can have sweeping effects, disrupting fuel supply for an entire segment of the country and halting meat processing operations nationwide.[3] We've also seen how privacy breaches can be materially consequential, with violations exposing millions of children during the course of doing their schoolwork, or resulting in the purchase and sale of individuals' sensitive health data.[4] Meanwhile, greater adoption of workplace surveillance technologies and facial recognition tools is expanding data collection in newly invasive and potentially discriminatory ways.[5]

---

[1] The views expressed in these remarks are my own and do not necessarily represent the views of the Federal Trade Commission or any other Commissioner.

[2] Nicholas W. Allard, *Digital Divide: Myth, Reality, Responsibility*, 24 HASTINGS COMM. & ENT. L.J. 449 (2002); Douglas C. Schmidt, *Google Data Collection* (2018), https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf (finding that Android phones, which tend to be more inexpensive, collect more data about its users).

[3] *See, e.g.*, Collin Eaton & Amrith Ramkumar, *Colonial Pipeline Shutdown: Is There a Gas Shortage and When Will the Pipeline Be Fixed?*, WALL ST. J. (May 13, 2021), https://www.wsj.com/articles/colonial-pipeline-cyberattack-hack-11620668583; Fabiana Batista et al., *All of JBS's U.S. Beef Plants Were Forced Shut by Cyberattack*, BLOOMBERG (May 31, 2021), https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs.

[4] *See, e.g.*, Joe Hoem, *Computer Hackers Attack Fairfax County School System*, WASH. POST (Sept. 11, 2020), https://www.washingtonpost.com/local/education/computer-hackers-attack-fairfax-county-school-system/2020/09/11/5a944d32-f474-11ea-999c-67ff7bf6a9d2_story.html; Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, U.S. Dep't of Health and Hum. Services Off. of Civ. Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Apr. 11, 2022).

[5] Kathryn Zickuhr, *Workplace 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; Aaron Rieke & Miranda Bogen, Upturn, *Help Wanted: An Examination of Hiring*

Americans are aware of the stakes and the potential hazards. One survey showed that close to two-thirds of Americans believe that it is no longer possible to go through daily life without companies collecting data about them, while over 80% feel that they have meager control over the data collected on them and believe that the risks of data collection by commercial entities outweigh the benefits.[6]

Against this backdrop, the Federal Trade Commission is charged with ensuring that our legal tools and our approach to law enforcement keep pace with market developments and business practices. With its longstanding expertise in how companies collect and deploy Americans' data—along with its unique combination of enforcement, policy, and research tools—the FTC is especially well suited to the task.

In my remarks today, I will offer a few observations about the new political economy of how Americans' data is tracked, gathered, and used; identify a few ways that the Federal Trade Commission is refining its approach in light of these new market realities; and share some broader questions that I believe these realities raise for the current frameworks we use for policing the use and abuse of individuals' data.

*

Concerns about Americans' privacy has long preceded the digital age. Louis Brandeis and Samuel Warren in 1890 famously sought to "define anew the exact nature and extent of" privacy protections guaranteed by law in the face of "recent inventions and business methods."[7] At bottom, they explained, the law protects people from the unwanted, prying eyes of private actors, almost in the same way that it protects against physical injury.

Similarly, lawmakers in 1970 passed the Fair Credit Reporting Act, the first federal law to govern how private businesses could use Americans' personal information. The law prescribed the types of information that credit reporting agencies could use and guaranteed a person's right to see what was in their file, a recognition of the unique harms that can result when firms have unchecked power to create dossiers on people that can be used to grant or deny them opportunities.

Though these basic principles governing what types of personal information businesses can and cannot collect and use extend back decades, the context in which we must now apply them today looks dramatically different.

Algorithms, Equity, and Bias (Dec. 10, 2018), https://www.upturn.org/work/help-wanted/; NAT'L INST. OF STANDARDS AND TECH., TOWARDS A STANDARD FOR IDENTIFYING AND MANAGING BIAS IN ARTIFICIAL INTELLIGENCE (2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

[6] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CENTER (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/. *See also* Chris Teale, *Nothing Concerns the Public More About the Metaverse Than the Misuse of Their Personal Data*, MORNING CONSULT (Apr. 11, 2022), https://morningconsult.com/2022/04/11/metaverse-public-concerns-survey ("According to the survey, 55% of adults said they have major concerns about how their personal data could be tracked and misused in the metaverse.").

[7] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Digital technologies have enabled firms to collect data on individuals at a hyper-granular level, tracking not just what a person purchased, for example, but also their keystroke usage, how long their mouse hovered on any particular item, and the full set of items they viewed but did not buy. As people rely on digital tools to carry out a greater portion of daily tasks, the scope of information collected also becomes increasingly vast, ranging from one's precise location and full web browsing history to one's health records and complete network of family and friends. The availability of powerful cloud storage services and automated decision-making systems, meanwhile, have allowed companies to combine this data across domains and retain and analyze it in aggregated form at an unprecedented scale—yielding stunningly detailed and comprehensive user profiles that can be used to target individuals with striking precision.

Some firms—like weather forecasting or mapping apps, for example—may primarily use this personal data to customize service for individual users. Others can also market or sell this data to third-party brokers and other businesses in ancillary or secondary markets that most users may not even know exist. Indeed, the general lack of legal limits on what types of information can be monetized has yielded a booming economy built around the buying and selling of this data. This has let firms provide services for zero dollars while monetizing personal information, a business model that seems to incentivize endless tracking and vacuuming up of users' data. Indeed, the value that data brokers, advertisers, and others extract from this data has led firms to create an elaborate web of tools to surveil users across apps, websites, and devices. As one scholar has noted, today's digital economy "represents probably the most highly surveilled environment in the history of humanity."[8]

While these data practices can enable forms of personalization that could in some instances benefit users, they can also enable business practices that harm Americans in a host of ways.[9] For example, firms can target scams and deceptive ads to consumers who are most susceptible to being lured by them. They can direct ads in key sectors like health, credit, housing, and the workplace based on consumers' race, gender, or age, engaging in unlawful discrimination.[10] Collecting and sharing data on people's physical movements, phone use, and online activities, meanwhile, can put people in serious danger, allowing stalkers to track them in real time.[11] And failing to keep sensitive personal information secure can also expose users to hackers, identity thieves, and cyber threats.

---

[8] NEIL RICHARDS, WHY PRIVACY MATTERS 84 (2021). *See also* OSCAR GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (2021).

[9] Latanya Sweeney, *Discrimination in Online Ad Delivery* (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240; Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U.L. REV. 53 (2017). *See generally* JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH (2013).

[10] See Julia Angwin & Terry Paris, Jr., *Facebook Lets Advertisers Exclude Users by Race*, PROPUBLICA (Oct. 28, 2016), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race; Tamara K. Nopper, *Digital Character in "The Scored Society": FICO, Social Networks, and Competing Measurements of Creditworthiness*, in CAPTIVATING TECHNOLOGY (Ruha Benjamin ed., 2019); Ho-Chun Herbert Chang et al., *Targeted Ads and/as Racial Discrimination: Exploring Trends in New York City Ads for College Scholarships* (Sept. 30, 2021), https://arxiv.org/abs/2109.15294.

[11] Press Release, Fed. Trade Comm'n., *FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data* (Sept. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data. *See, e.g.*, Danielle Keats Citron, *Spying Inc.*, 72 WASH. & LEE L. REV. 1243 (2015).

The incentive to maximally collect and retain user information can also concentrate valuable data in ways that create systemic risk, increasing the hazards and costs of hacks and cyberattacks. Some, moreover, have also questioned whether the opacity and complexity of digital ad markets could be enabling widespread fraud and masking a major bubble.[12]

Beyond these specific harms, the data practices of today's surveillance economy can create and exacerbate deep asymmetries of information—exacerbating, in turn, imbalances of power.[13] As numerous scholars have noted, businesses' access to and control over such vast troves of granular data on individuals can give those firms enormous power to predict, influence, and control human behavior.[14] In other words, what's at stake with these business practices is not just one's subjective preference for privacy, but—over the long term—one's freedom, dignity, and equal participation in our economy and society.

*

Our talented FTC teams are focused on adapting the Commission's existing authority to address and rectify unlawful data practices. A few key aspects of this approach are particularly worth noting.

First, we're seeking to harness our scarce resources to maximize impact, particularly by focusing on firms whose business practices cause widespread harm. This means tackling conduct by dominant firms as well as intermediaries that may facilitate unlawful conduct on a massive scale. For example, last year the Commission took action against OpenX, an ad exchange that handles billions of advertising requests involving consumer data and was alleged to have unlawfully collected information from services directed to children.[15] We intend to hold accountable dominant middlemen for consumer harms that they facilitate through unlawful data practices.

Second, we are taking an interdisciplinary approach, assessing data practices through both a consumer protection and competition lens. Given the intersecting ways in which widescale data collection and commercial surveillance practices can facilitate violations of both consumer protection and antitrust laws, we are keen to marshal our expertise in both areas to ensure we are grasping the full implications of particular business conduct and strategies. Also key to our interdisciplinary approach is our growing reliance on technologists alongside the skilled lawyers, economists, and investigators who lead our enforcement work. We have already increased the number of technologists on our staff—drawing from a diverse set of skillsets, including data scientists and engineers, user design experts, and AI researchers—and we plan to continue building up this team.

---

[12] *See, e.g.*, TIM HWANG, SUBPRIME ATTENTION CRISIS: ADVERTISING AND THE TIME BOMB AT THE HEART OF THE INTERNET (2020).
[13] *See, e.g.*, KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017).
[14] *See, e.g.*, RICHARDS, *supra* note 8; JULIE COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); CARISSA VELIZ, PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA (2021).
[15] Press Release, Fed. Trade Comm'n., *Advertising Platform OpenX Will Pay $2 Million for Collecting Personal Information from Children in Violation of Children's Privacy Law* (Dec. 15, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/12/advertising-platform-openx-will-pay-2-million-collecting-personal-information-children-violation.

Third, when we encounter law violations, we focus on designing effective remedies that are directly informed by the business strategies that specific markets favor and reward. This includes pursuing remedies that fully cure the underlying harm and, where necessary, deprive lawbreakers of the fruits of their misconduct. For example, the Commission recently took action against a Weight Watchers subsidiary, Kurbo, alleging that the company illegally harvested children's sensitive personal information, including their names, eating habits, daily activities, weight, birth date, and persistent identifiers. Our settlement required not only that the business pay a penalty for its lawbreaking, but also that it delete its ill-gotten data and destroy any algorithms derived from it.[16]

Where appropriate, our remedies will also seek to foreground executive accountability through prophylactic limits on executives' conduct. In our action against SpyFone, for example, the FTC banned both the company and its CEO from the surveillance business, resolving allegations that they had been secretly harvesting and selling real-time access to data on a range of sensitive activity. Lastly, we are focused on ensuring that our remedies evolve to reflect the latest best practices in security and privacy. In our recent action against CafePress, for example, our settlement remedied an alleged breach by requiring the use of multi-factor authentication—reflecting the latest thinking in secure credentialing.[17]

*

Even without a federal data privacy or security law, the FTC has for decades served as a de facto enforcer in this domain, using Section 5 of the FTC Act and other statutory authorities to crack down on unlawful practices.[18] No doubt, we will continue using our current enforcement tools to take swift and bold action.

However, the realities of how firms surveil, categorize, and monetize user data in the modern economy invite us to consider how we might need to update our approach further yet.

First, the Commission is considering initiating a rulemaking to address commercial surveillance and lax data security practices.[19] Giving that our economy will only continue to

---

[16] Press Release, Fed. Trade Comm'n., *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. In the Commission's case against Everalbum last year, the Commission obtained orders that forbade the company from profiting from unlawful practices related to its use of automated systems. Decision and Order, In the matter of Everalbum, Inc., Commission File No. 1923172, C-4743 (May 6, 2021).

[17] Press Release, Fed. Trade Comm'n., *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-covert.

[18] For example, the Gramm-Leach-Bliley Act and the Children's Online Privacy Protection Act apply certain limitations on the collection and use of personally identifiable financial information and children's data, respectively, which the FTC enforces. *See also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

[19] OFF. OF INFO. AND REGUL. AFF., OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, RIN No. 3084-AB69, TRADE REGULATION RULE ON COMMERCIAL SURVEILLANCE (Fall 2021), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69.

further digitize, market-wide rules could help provide clear notice and render enforcement more impactful and efficient.

Second, we need to reassess the frameworks we presently use to assess unlawful conduct. Specifically, I am concerned that present market realities may render the "notice and consent" paradigm outdated and insufficient. Many have noted the ways that this framework seems to fall short, given both the overwhelming nature of privacy policies—and the fact that they may very well be beside the point. When faced with technologies that are increasingly critical for navigating modern life, users often lack a real set of alternatives and cannot reasonably forego using these tools.[20]

Going forward, I believe we should approach data privacy and security protections by considering substantive limits rather than just procedural protections, which tend to create process requirements while sidestepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place.[21] The central role that digital tools will only continue to play invites us to consider whether we want to live in a society where firms can condition access to critical technologies and opportunities on users surrendering to commercial surveillance. Privacy legislation from Congress could also help usher in this type of new paradigm.

*

Thank you again for inviting me to speak today. This is an incredibly exciting and momentous time for these issues—with much at stake and a tremendous amount of work to be done, as we chart a path forward that keeps our economies dynamic and our citizens protected.

***

[20] *See* Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, HARV. BUS. REV. (Jan. 30, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data (noting that "even if users wanted to negotiate more data agency, they have little leverage. Normally, in well-functioning markets, customers can choose from a range of competing providers. But this is not the case if the service is a widely used digital platform."); Daniel Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 29 (2021) ("In one survey, 81% of respondents said that they had at least once 'submitted information online when they wished that they did not have to do so.' People often are not afforded much choice or face a choice between two very bad options."); Mary Madden, Opinion, *The Devastating Consequences of Being Poor in the Digital Age*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html.

[21] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1693 (2020) ("[D]ata protection regimes seek to permit more ethical surveillance and data processing at the expense of foundational questions about whether that surveillance and processing should be allowed in the first place."); Solove, *supra* note 20, at 29 ("The fact that people trade their privacy for products or services does not mean that these transactions are desirable in their current form…[T]he mere fact that people make a tradeoff doesn't mean that the tradeoff is fair, legitimate, or justifiable. For example, suppose people could trade away food safety regulation in exchange for cheaper food. There would be a price at which some people would accept greater risks of tainted food. The fact that there is such a price doesn't mean that the law should allow the transaction.").