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.

erially 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., *t 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*

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 P

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 len

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 unlawful72.024 7r07y12 792 reW* nBT/TT1 12 Tf309.05nO00444 6044A>9 44 (ti)02au.FdrFult0