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

Office of the Chair

Statement of Chair Lina M. Khan
Regarding the Report to Congress on
Privacy and Security
Commission File No. P065401

October 1, 2021

Policing data privacy and security is now a mainstay of the FTC's work. While the Commission has long served as the country's de facto enforcer in this domain, growing digitization across the economy has rendered this work even more critical. Security vulnerabilities today can have sweeping effects, disrupting fuel supply for an entire fraction of the country and halting meat process operations nationwide.[1] Privacy breaches can be similarly consequential, with violations exposing millions of children in the course of doing their homework or resulting in the commercialization of sensitive health data.[2] Meanwhile, greater adoption of workplace surveillance technologies and facial recognition tools is expanding data collection in newly invasive and potentially discriminatory ways.[3] All too aware of these risks, a significant majority of Americans today feel that they have scant control over the data collected on them and believe the risks of data collection by commercial entities outweigh the benefits.[4]

Given the high stakes, ensuring that we pursue this work with a commitment to maximizing efficacy and learning from new evidence is paramount. In our report to Congress, the FTC detailed its work to protect Americans' privacy and data security, identifying areas in need of greater resources and areas for improving our effectiveness. As my predecessors and fellow Commissioners alike have long noted, a substantial increase in resources would help bring the

---

[1] *See, e.g.*, Collin Eaton & Amrith Ramkumar, *Colonial Pipeline Shutdown*, WALL ST. J. (May 13, 2021), https://www.wsj.com/articles/colonial-pipeline-cyberattack-hack-11620668583; *see also* 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?sref=fmFtnZNQ.

[2] Zack Whittaker, *Animal Jam was hacked, and data stolen; here's what parents need to know*, TECHCRUNCH (Nov. 16, 2020), https://techcrunch.com/2020/11/16/animal-jam-data-breach/; *see also* Kat Jercich, *Healthcare data breaches on the rise*, HEALTHCARE IT NEWS (Aug. 5, 2021), https://www.healthcareitnews.com/news/healthcare-data-breaches-rise.

[3] 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; Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-castsdoubt-their-expanding-use.

[4] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. 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/ (noting that 81% of Americans believe that they "have very little/no control over the data companies collect" and that "the potential risks of companies collecting data about them outweigh the benefits").

FTC more in line with similar agencies internationally and enable us to recruit additional talent.[5] Even absent these increases, however, we must update our approach to keep pace with new learning and technological shifts.

One area for improvement that our report highlights is cross-disciplinary work, which includes understanding "the overlap between data privacy and competition."[6] This statement reflects the growing recognition that persistent commercial data collection implicates competition as well as privacy. In particular, concentrated control over data has enabled dominant firms to capture markets and erect entry barriers, while commercial surveillance has allowed firms to identify and thwart emerging competitive threats.[7] Monopoly power, in turn, can enable firms to degrade privacy without ramifications—as the Commission itself recently alleged in court.[8] Given that the competitive significance of data has been under-appreciated by enforcers across the board, breaking down siloes to better grasp these interconnections is key to ensuring rigorous analysis and effective enforcement.[9]

Of course, recognizing that privacy and competition are interconnected is not the same as claiming that competition and privacy always align.[10] Indeed, recent events are surfacing the ways in which the pretext of privacy may be weaponized to undermine competition on the merits, and scholars have long recognized that unfettered competition can fuel a race-to-the-bottom.[11] But it

---

[5] *See, e.g.*, Written Testimony of Hon. Maureen Ohlhausen, Former Acting-Chair, Federal Trade Commission, Co-Chair, 21st Century Privacy Coalition, Hearing on Examining Legislative Proposals to Protect Consumer Data Privacy Before the Sen. Comm. on Commerce, Sci., and Trans., at 7 (Dec. 4, 2019), https://www.commerce.senate.gov/services/files/30994150-8879-48B7-9BC0-625D8C81A7F2; Transcript, Oversight of the Federal Trade Commission: Hearing Before the Sen. Comm. on Commerce, Sci., and Trans., Subcomm. on Consumer Protection, Product Safety, Insurance, and Data Security, at 25:58 (Nov. 27, 2018), https://www.c-span.org/video/?455021-1/federal-trade-commission-oversight (Commissioner Rohit Chopra noting "In my past agency experience, I've seen how going up against a company with legions of lawyers and lobbyists and PR professionals can be daunting for an agency with finite resources, but Congress can't expect any agency, including the FTC, to meet its mission unless it is unambiguous to the market that we have the resources and the resolve to go to court no matter how big or connected a company may be."); *id*. at 51:52 (Chairman Simons noting that in order to increase litigation, the agency would need more resources); Kate Kaye, *'Don't lie': FTC Commissioner Rebecca Slaughter on why today's data privacy approaches don't work (Audio Q&A)*, DIGIDAY (July 7, 2021), https://digiday.com/media/dont-lie-a-qa-with-ftc-commissioner-rebecca-slaughter-on-why-todays-data-privacy-approaches-dont-work/.

[6] FED. TRADE COMM'N, REPORT ON PRIVACY AND SECURITY TO THE SENATE AND HOUSE COMMITTEES ON APPROPRIATIONS PURSUANT TO THE JOINT EXPLANATORY STATEMENT ACCOMPANYING THE CONSOLIDATED APPROPRIATIONS ACT, 2021 P.L. 116-260, at 7 (2021).

[7] *See* MAURICE STUCKE & ALLEN GRUNES, BIG DATA & COMPETITION POLICY (2016).

[8] First Am. Compl. For Injunctive and Other Equitable Relief, *Federal Trade Commission v. Facebook, Inc.*, No. 1:20-cv-03590 (D.C. Cir. Aug. 19, 2021).

[9] Cristina Caffarra et al., *The antitrust orthodoxy is blind to real data harms*, VOXEU (Apr. 22, 2021), https://voxeu.org/content/antitrust-orthodoxy-blind-real-data-harms; Alessandro Acquisti et al., *Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age*, 30 J. CONSUMER PSYCHOL. 736 (2020);

[10] Contrary to Commissioner Phillips' dissent, nowhere does our report assert that competition and privacy are always aligned. Statement of Commissioner Noah Joshua Phillips Regarding the Report to Congress on Privacy and Security, Commission File No. P065401 (Sep. 30, 2021).

[11] *See e.g.,* MAURICE E. STUCKE & ARIEL EZRACHI, COMPETITION OVERDOSE (2020); Neil W. Averitt, *The Meaning of "Unfair Methods of Competition" in Section 5 of the Federal Trade Commission Act*, 21 B.C. L. REV. 227 (1980); Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L. J. FORUM 647 (2021).

is precisely through approaching our competition and data privacy work with these interconnections in mind that the Commission can study these issues.[12]

Moreover, the fact that competition alone is *not* sufficient to safeguard data privacy and security is exactly why the Commission must explore using its rulemaking tools to codify baseline protections. Evidence suggests that the current configuration of commercial data practices do not actually reveal how much users value privacy or security.[13] This is true for a host of reasons, including the fact that users often lack a real set of alternatives and cannot reasonably forego using technologies that are increasingly critical for navigating modern life.[14] The use of dark patterns and other conduct that seeks to manipulate users only underscores the limits of treating present market outcomes as reflecting what users desire or value.[15] A growing recognition that the "notice-and-consent" framework has serious shortcomings further highlights the need for us to consider a new paradigm, which could be implemented through privacy legislation from Congress.[16]

Going forward, I believe the Commission should approach data privacy and security protections by considering substantive limits rather than just procedural protections, which tend to

---

[12] Indeed, the FTC is currently helping spearhead an international project to better understand the intersection of competition, data privacy, and consumer protection—an area that peer agencies around the world similarly recognize as necessary for ensuring the efficacy of our work. *See* Press Release, International Competition Network Addresses Enforcement and Policy Challenges of the Digital Economy at United States-Hosted 19th Annual Conference (Sept. 17, 2020), https://www.ftc.gov/news-events/press-releases/2020/09/international-competition-network-addresses-enforcement-policy ("The ICN Steering Group has begun exploring the issues related to competition enforcement and advocacy pertaining to the intersection between competition, consumer protection, and data privacy law and policy, a project initiated by the FTC.").

[13] See, e.g., Daniel Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 22-32 (2021).

[14] 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."); *see also* Solove, *supra* note 13 at 29 ("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.").

[15] The FTC recently brought a case against Age of Learning, Inc., an educational subscription service that utilized dark patterns to scam millions of dollars from families. *See* Stipulated Order for Permanent Injunction and Monetary Judgement, *Federal Trade Commission v. Age of Learning, Inc.*, No. 2:20-cv-7996 (C.D. Cal Sept. 8, 2020). *See also* Solove, *supra* note 13, at 5 ("Individual risk decisions in particular contexts indicate little about how people value their own privacy."); Zeynep Tufekci, *The Latest Data Privacy Debacle*, N.Y. TIMES, (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html ("Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices.").

[16] *See, e.g.*, Press Release, Senator Markey Introduces Comprehensive Privacy Legislation (Apr. 12, 2019), http://www.markey.senate.gov/news/press-releases/senator-markey-introduces-comprehensive-privacy-legislation ("I have long advocated for privacy protections that include the principles of knowledge, notice and the right to say 'no' to companies that want our information. But it is increasingly clear that a true 21st century comprehensive privacy bill must do more than simply enshrine notice and consent standards."). *See also* 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/ ("Of course, no one is actually going to read all those privacy policies. What that massive number tells us is that the way we deal with privacy is fundamentally broken. The collective weight of the web's data collection practices is so great that no one can maintain a responsible relationship with his or her own data. That's got to change.").

create process requirements while sidestepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place.[17] We also need to be mindful of the ways that behavioral ad-based business models can incentivize constant surveillance, resulting in further mass aggregation of data, potentially heightening the risk of data privacy and security abuses—and further inviting us to consider a market-wide approach. Lastly, we should approach both new policies and legal remedies with an eye to their administrability, given the significant information asymmetries we can face in these contexts.

The digitization further hastened by the pandemic makes this a particularly urgent and opportune time for the Commission to examine how we can best use our tools and update our approach in order to tackle the slew of data privacy and security challenges we presently face. I look forward to working with my colleagues to meet the moment and deliver.

***

[17] 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 13, at 35-36 ("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.").