

**PREPARED TESTIMONY AND STATEMENT FOR THE  
RECORD  
OF**

**DR. SARAH MYERS WEST  
MANAGING DIRECTOR, AI NOW INSTITUTE**

**on behalf of herself and Amba Kak, Executive Director, AI Now Institute**

**“THE NEW INVISIBLE HAND? THE IMPACT OF ALGORITHMS ON COMPETITION  
AND CONSUMER RIGHTS.”**

**BEFORE THE**

**U.S. SENATE COMMITTEE ON THE JUDICIARY  
SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS**

Chair Klobuchar, Ranking Member Lee, and esteemed Members of the Committee, thank you for inviting me to testify on this important set of issues. My name is Sarah Myers West, and I am the managing director of the AI Now Institute, a leading policy research institute founded in 2016 to study artificial intelligence technologies. I hold doctoral and master’s degrees from the Annenberg School at the University of Southern California, where I studied the economics of the tech industry. I recently served as a Senior Advisor on Artificial Intelligence at the Federal Trade Commission, where my role was to provide technological expertise in support of the agency’s enforcement work. I worked across competition and consumer protection enforcement matters addressing the role of algorithmic systems in mediating vast swaths of the economy, an experience that underscored for me the importance of the issues we will be discussing today.

As someone who brings over 15 years of experience examining these issues, I deeply appreciate this Subcommittee’s ongoing attention to the role of algorithmic systems in shaping the economy at large, often in ways that harm consumers and workers while benefiting centralized actors.

In this testimony, I highlight three core areas of concern that I urge this Committee to consider as urgent priorities for intervention:

1. Concentration among the firms producing and deploying AI and algorithmic systems risks creating single points of failure through which flaws introduced in one system could have ripple effects throughout the economy.

2. Algorithmic systems distort the market by enabling companies with preferential access to data to charge higher prices.
3. There is a risk that these systems enable groups and individuals to be excluded from access to the market, including on the basis of membership in protected classes, thus scaling patterns of inequality.

I also offer three broad paths forward in terms of how we can start to address these harms proactively:

1. We need to use existing enforcement mechanisms to ensure strong oversight of this sector by robustly resourcing the agencies with existing authority. We already have a range of enforcement mechanisms that can be applied to anticompetitive and harmful uses of AI and algorithmic systems.
2. Second, we need specific bright line rules to curb AI use where it has demonstrated harms to consumers and competition. The passage of a federal data privacy law, including a strong data minimization mandate, should be an urgent priority given that it serves as a potent antidote to a range of algorithmically enabled harms, including harms to competition.
3. Lastly, we need legislation to tackle the market structure and gatekeeper power of dominant digital platforms, which hold an unprecedented amount of economic and political power.

As this hearing underscores, algorithmic systems have a profound impact on the economy at large in ways that are harming consumers, workers, and small businesses. In their most basic sense, algorithms, in the context of computation, are simply instructions that systems follow. They can be as simple as a decision tree, or as vast and complex as a transformer model, which is a type of deep learning architecture undergirding recent developments in artificial intelligence. Frequently, they apply statistical techniques to large swaths of data, often to arrive at a particular decision or recommendation: for example, tailoring the price of a given item based on processing personal data about a potential buyer, and setting the price to the maximum the system predicts that buyer will be willing to pay.

While many of the underlying techniques have existed for decades, such systems are supercharged by the surveillance business model promulgated by the tech industry: this incentivized the instrumentation of technologies that collect detailed and often intimate information about us as we move about our lives. These data traces can then be collected by firms either directly or purchased by others through third parties, creating information and power asymmetries that have profound societal effects that I've described as *data capitalism*.<sup>1</sup> Firms

---

<sup>1</sup> West, Sarah Myers. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business and Society*, 58(1). <https://journals.sagepub.com/doi/10.1177/0007650317718185>

use the data they are able to obtain through surveillance and other means to set prices based on their algorithmic prediction of what an individual is likely to pay. This fundamentally advantages firms with greater access to data, and disadvantages individuals wishing to purchase goods. This behavior is variously classed as algorithmic or personalized pricing, and includes *dynamic pricing*, or the use of algorithms to make frequent changes to the prices of goods, as well as *personalized pricing*, or the use of privileged information to set prices, enabling firms to extract the maximum amount of money from consumers possible based on information targeted to them.<sup>2</sup>

Through this constellation of practices, firms positioned at key chokepoints in the consumer economy are best positioned to leverage information asymmetries in a manner that is harmful both to competition and to consumers. This creates extended potential for collusion in markets where this otherwise would not be possible:<sup>3</sup> while this is most notable when we see systems go awry by producing spirals that lead to skyrocketing prices, such as surges in the cost of hand sanitizer during the pandemic, more frequently it takes shape in more invisible ways that are harder to identify from the outside.<sup>4</sup>

The harms associated with algorithmic pricing go beyond collusive behavior: algorithmic pricing can result in higher prices even in the absence of collusion,<sup>5</sup> and can be used to manipulate consumer behavior.<sup>6</sup> This urgently necessitates policy intervention that breaks down silos between competition enforcement, consumer protection law and data minimization, among others, and most important, attends to the tremendous concentration of power that is the hallmark of the tech industry.

It's particularly critical that we not discuss these technologies in the abstract, but attend to how they're actually being used. Often that's automating austerity, increasing corporate control, or supercharging a firm's ability to drive up prices to the maximum someone is willing to pay. This has profound effects for the public, when algorithms shape the public's access to resources, the cost and availability of credit and housing, or whether they are paid a fair wage at the end of a

---

<sup>2</sup> Personalised Pricing in the Digital Era - Note by the United States. (2018). OECD.

[https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/personalized\\_pricing\\_note\\_by\\_the\\_united\\_states.pdf](https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/personalized_pricing_note_by_the_united_states.pdf).

<sup>3</sup> Competition and Markets Authority. (2018). Pricing Algorithms.

[https://assets.publishing.service.gov.uk/media/5bbb2384ed915d238f9cc2e7/Algorithms\\_econ\\_report.pdf](https://assets.publishing.service.gov.uk/media/5bbb2384ed915d238f9cc2e7/Algorithms_econ_report.pdf)

<sup>4</sup> Soper, Spencer and Porter Jr., Gerald. (2020, Mar. 5) That \$400 Bottle of Hand Sanitizer Is Very Hard to Police. *Bloomberg*, <https://www.bloomberg.com/news/articles/2020-03-05/that-400-bottle-of-hand-sanitizer-is-very-hard-to-police>

<sup>5</sup> MacKay, Alexander and Weinstein, Samuel. (2022). Dynamic Pricing Algorithms, Consumer Harm and Regulatory Response. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3979147](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3979147)

<sup>6</sup> Mathur, Arunesh; Acar, Gunes; Friedman, Michael J.; Lucherini, Elena; Mayer, Jonathan; Chetty, Marshini; Narayanan, Arvind (November 2019). "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites". *Proceedings of the ACM on Human-Computer Interaction*. **3** (CSCW): 81:1–81:32. <https://dl.acm.org/doi/10.1145/3359183>

day's work. For example, in healthcare, we've seen numerous examples where insurers employ 'cost' as a proxy variable to decide whether or not to approve patients' access to certain resources. Research has demonstrated that when instrumented in practice, this can lead to the denial of critical care to particular groups.<sup>7</sup> Similar effects can be seen in 'digital redlining' that results in exclusion from key markets in housing and finance, among others.<sup>8</sup>

Algorithmic systems are optimized for incentives we already understand, and sometimes these incentives may violate existing law - so we shouldn't fall for an algorithmic mirage. These systems are tools that serve whatever interests the firm developing them is designing for, and are not at all neutral. That doesn't mean enforcement will be easy: there is a profound mismatch between the impact on people's wallets, opportunities, and life chances on the one hand, and the opacity and obscurity of the systems used to perpetuate this impact, on the other.<sup>9</sup> By denying the public information about how algorithmic systems affect their lives, each of us lacks the information we would need to ask others what we are seeing, to understand whether the decisions are accurate, to seek remedy or push back.

We have granted a staggering amount of power to the scant few firms with the data and computational infrastructure required to develop and deploy algorithmic systems, and given up consumer sovereignty in the process. This is why effective regulatory intervention that foregrounds bright line measures is particularly needed for this sector, otherwise enforcers and the public will constantly be playing catch-up.

But there are effective steps that we could take, and these should follow from a clear understanding of the problems at hand. To return to the points I started with:

**First, concentration among the firms producing and deploying algorithmic systems is working to create single points of failure that could have ripple effects throughout the economy.**<sup>10</sup> Overreliance on the same algorithmic model, or on the same data, presents imminent risks to financial stability, and could very literally trigger a financial crisis. And these risks aren't simply posed to financial markets. Anywhere these systems are deployed, from housing, to credit, to payments, to transportation, and well beyond, flaws, vulnerabilities, or malicious

---

<sup>7</sup> Obermeyer, Ziad, Powers, Brian, Vogeli, Christine and Mullainathan, Sendhil. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464): 447-453. <https://www.science.org/doi/10.1126/science.aax2342>.

<sup>8</sup> Gillard, Christopher. (2019, Nov. 21). Prepared testimony and statement for the record of Christopher Gilliard PhD, Hearing on Banking on your Data the Role of Big Data in Your Financial Services, Before the House Financial Services Committee Task Force on Financial Technology. <https://www.congress.gov/116/meeting/house/110251/witnesses/HHRG-116-BA00-Wstate-GillardC-20191121.pdf>

<sup>9</sup> Pasquale, Frank. (2016). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

<sup>10</sup> Palma, Stefania and Jenkins, Patrick. (2023, Oct. 16). Gary Gensler urges regulators to tame AI risks to financial stability. *Financial Times*. <https://www.ft.com/content/8227636f-e819-443a-aeba-c8237f0ec1ac>

configurations lurk as significant threats. The more broadly a single system is used across such domains, the greater the consequences.

Put simply, such systems are not infallible: to the contrary, where investigative journalists, security researchers, and enforcers have looked under the hood they often find that the underlying data on which these systems are trained is often flawed, leading to widespread errors in decision making.<sup>11</sup> Think about the frustration of experiencing an insurance claims denial because the evaluator on the other side was in a rush, or hadn't had their coffee yet that morning. We can think of algorithmic systems as taking each of those individual decisions and replicating them at massive scale, often with little to no scrutiny before they are commercially deployed.

**Second, algorithmic systems enable companies that gain preferential access to data to charge higher prices, leveraging network effects to undermine competition and exploit consumers.**<sup>12</sup> For example, car insurance firm Allstate used what it described as a 'price adjustment algorithm', to make determinations about changes to customer policies. To the public, they claimed that they were doing this to improve customer retention. Whether this was actually the intent, we do not know. What we do know is that in practice the algorithm was employed to identify which customers the system predicted were 'willing to pay', using the data Allstate collected from its customers to squeeze more money out of them through rate hikes of up to 20 percent, while instituting rate increases of only five percent from others.<sup>13</sup> This should perhaps not surprise us. The insurance industry, like most other market actors, is incentivized to increase revenue and profits. And an algorithm that does this, even at the expense of the rest of us, is perversely fulfilling these incentives.

In another example, reporters at the *Wall Street Journal* found that Staples was adjusting prices for consumers if Staples knew a competitor store was in the same zip code, increasing the cost if there were no alternatives close by. While this practice was applied across many regions, its effect could produce higher prices for customers in rural areas not because of distance or inventory, but simply because Staples leveraged its information to extract more money from

---

<sup>11</sup> For instructive examples, see: Charette, Robert N. (2018, Jan. 24). Michigan's MiDAS Unemployment System: Algorithm Alchemy Created Lead, Not Gold. *IEEE Spectrum*. <https://spectrum.ieee.org/michigans-midas-unemployment-system-algorithm-alchemy-that-created-lead-not-gold>; Burgess, Matt, Schot, Evaline, and Gabriel Geiger. (2023, Mar. 6). This Algorithm Could Ruin Your Life. *WIRED*. <https://www.wired.com/story/welfare-algorithms-discrimination/>.

<sup>12</sup> Mackay, Alexander and Weinstein, Samuel. (2021, Dec. 15). Dynamic Pricing Algorithms, Consumer Harm, and Regulatory Response. 100 Wash. U. L. Rev. 111. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3979147](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3979147)

<sup>13</sup> Varner, Maddy and Sankin, Aaron. (2020, Feb. 25). Suckers List: How Allstate's Secret Auto Insurance Algorithm Squeezes Big Spenders. *The Markup*. <https://themarkup.org/allstates-algorithm/2020/02/25/car-insurance-suckers-list>.

people they assumed would be unwilling to experience the inconvenience of finding an alternate store.<sup>14</sup>

Companies are harmed by this behavior too: firms can leverage unique access to data and network effects to exclude others from competing with them. For example, rental companies like RealPage that own properties across multiple real estate markets can leverage information across these holdings to tailor price recommendations in ways smaller companies cannot.<sup>15</sup> RealPage also has cross-ownership of additional holdings that may provide rich troves of data, such as its tenant screening software offering.<sup>16</sup> Similarly, many large tech firms have both vertically integrated holdings as well as ownership or stakes in companies in particular sectors, and are incentivized to leverage these information asymmetries to get ahead of their competitors. For example, after acquiring the VPN app Onavo, Facebook used data from Onavo users to monitor competitors. The company then used this data to inform its attempt to acquire Snap and its successful acquisition of WhatsApp.<sup>17</sup> Such practices are particularly concerning where firms have access to data in markets that are particularly sensitive, such as healthcare and finance.

And we need to mention workers and work. In the workplace, we have already seen multiple troubling examples in which, algorithmic techniques have been used to drive wages down. Dr. Veena Dubal, a Professor of Law at UC Irvine, has studied and written about the use of algorithmic models to determine the wages of rideshare drivers. Her work revealed this model as reliant on algorithmic wage discrimination, that may violate competition laws.<sup>18</sup> For example, rideshare drivers have reported observing that bonuses that are key to making their base salary may be rendered harder to reach the closer they are to attaining them.<sup>19</sup> This is far from a fair day's pay for a good day's work. And here we begin to see the dual bind that so many of us are faced with—personalized pricing and algorithmic price discrimination on one end, that extracts as much money as possible from us as we engage in purchases necessary for survival. And on the other end, wage discrimination and algorithmic wage arbitrage, that reduces our pay in unfair

---

<sup>14</sup> Valentino-DeVries, Jennifer, Singer-Vine, Jeremy and Soltani, Ashkan. (2012, Dec. 24). Websites Vary Prices, Deals Based on Users' Information. *The Wall Street Journal*. <https://www.wsj.com/articles/SB10001424127887323777204578189391813881534>

<sup>15</sup> Vogell, Heather, Coryne, Haru, and Little, Ryan. (2022, Oct. 15). Rent Going Up? One Company's Algorithm Could Be Why. *ProPublica*. <https://www.propublica.org/article/yieldstar-rent-increase-realpage-rent>

<sup>16</sup> Kirchner, Lauren and Goldstein, Matthew. (2020, May 28). Access Denied: Faulty Automated Background Checks Freeze Out Renters. *The Markup*. <https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renters>.

<sup>17</sup> Bell, Karissa. (2018, Dec. 5) 'Highly confidential' documents reveal Facebook used VPN app to track competitors. *Mashable*. <https://mashable.com/article/facebook-used-onavo-vpn-data-to-watch-snapchat-and-whatsapp>

<sup>18</sup> Dubal, Veena. (2023). On Algorithmic Wage Discrimination. *Columbia Law Review* 123(7). <https://columbialawreview.org/content/on-algorithmic-wage-discrimination/>

<sup>19</sup> Qadri, Rida and Mateescu, Alexandra. (2021, Jun. 20). Uber and Lyft: woo drivers with stable pay, not short-term honeypots. *The Guardian*. <https://www.theguardian.com/commentisfree/2021/jun/20/gig-economy-companies-uber-lyft-drivers-pandemic>.

and often incontestable ways. In both cases, everyday people lose, and large, data-rich firms that benefit from obscure infrastructures and vast information asymmetries benefit.

**Third, because algorithmic systems function by classing people into particular types, they frequently serve to exclude entire groups from access to the market. This means that systems trained on historical data frequently scale longstanding patterns of inequality.<sup>20</sup>**

*Digital redlining* describes the use of algorithmic systems to replicate historical patterns of inequality by training algorithmic decisionmaking technologies on biased data. For example, investigative journalists at the Markup identified distortions in the algorithms used to evaluate mortgage applicants, which led to a systematic increase in denial of access to lending for borrowers of color who were otherwise similarly qualified.<sup>21</sup> In the context of tenant screening, reporters found a widespread use of so-called ‘wildcard searches’, in which criminal background checks were turning up the records of the wrong individual due to small discrepancies in the spelling of a last name - say, Johnsen instead of Johnson. These discrepancies led individuals to be wrongfully denied the rental of apartments, excluding them from housing they were otherwise well-qualified for.<sup>22</sup> These kinds of errors are mundane but profound in their consequences, particularly in markets with limited alternatives - increasingly likely given growing concentration in the tenant screening industry.<sup>23</sup>

**The thread that cuts across all of the examples above is the more fundamental issue raised by granting this level of economic - and political - power to a limited number of firms.** One of the animating principles of our competition laws is that granting too much centralized economic power to too few is harmful to our democracy. High levels of concentration within a tech industry still reliant on consumer surveillance as its fundamental business model renders large tech firms the engine driving the proliferation of these practices, regardless which particular market is under the microscope. This means that policy interventions tackling the concentration of power in the tech industry will have profound effects on the algorithmic harms I’ve just described. This means we need policy interventions that confront, rather than further entrench, this concentration. I have three key recommendations in this vein:

---

<sup>20</sup> Gandy, Oscar. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Oxford: Oxford University Press.

<sup>21</sup> Martinez, Emmanuel and Kirchner, Lauren. (2021, Aug. 25). The Secret Bias Hidden in Mortgage-Approval Algorithms. *The Markup*.

<sup>22</sup> Kirchner, Lauren and Goldstein, Matthew. (2020, May 28). Access Denied: Faulty Automated Background Checks Freeze Out Renters. *The Markup*. <https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renters>. <https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms>.

<sup>23</sup> Consumer Financial Protection Bureau. (2022). Tenant Background Checks Market. [https://files.consumerfinance.gov/f/documents/cfpb\\_tenant-background-checks-market\\_report\\_2022-11.pdf](https://files.consumerfinance.gov/f/documents/cfpb_tenant-background-checks-market_report_2022-11.pdf).

**First and foremost, I'd like to underscore the importance of using existing enforcement mechanisms to ensure strong oversight of this sector, including robustly resourcing the agencies with existing authority.** We already have a range of enforcement mechanisms that can be applied to anticompetitive and harmful uses of AI, including the Sherman and Clayton Acts and the FTC Act. Robust enforcement of consumer protection law can likewise be used to ensure responsibility for the use of these algorithms, including using the Fair Credit Reporting Act, and offering greater legal clarity about what FCRA covers. In fact, agencies like the FTC, CFPB, EEOC etc, with limited resources, have still brought enforcement against some of the worst practices including cracking down on algorithmic wage manipulation,<sup>24</sup> unlawful deceptive secondary use,<sup>25</sup> and algorithmic discrimination.<sup>26</sup> The work of enforcement agencies far predates the current hype around AI, however, this present hype wave does mean there will be more work on their hands, so first and foremost on the list of priorities should be to ensure that these agencies have the resources they need commensurate to the growing scale of the problem.

Second, we need specific bright line rules to curb AI use where it has demonstrated harms to consumers and competition. In this testimony, I highlighted several practices that would benefit from clear and easily administrable restrictions, rather than procedural safeguards or vague standards that are open to creative interpretation and misuse by companies. The Illinois' Biometric Information Privacy Act is instructive as an example of combining a bright line rule that prohibits companies from profiting from the sale of sensitive data with a private right of action. The BIPA has resulted in several successful enforcement actions with market-wide ripple effects, including banning the now notorious company Clearview AI from selling its sensitive database of millions of our faces illegally scraped from the internet for profit. This is closely related to the need for a strong data minimization mandate that puts in place a broader framework of limits on how companies collect, use, and store data. The passage of a federal data privacy law, including a strong data minimization mandate should be an urgent priority given that it serves as a potent antidote to a range of algorithmically enabled harms. As we, Accountable Tech and EPIC emphasize in the 'Zero Trust AI Framework', data minimization rules are essential levers at a time when AI is tipped to further exacerbate information asymmetries between individuals and communities, on the one hand, and the large corporations that create and collect data about them which has increasing power over their lives, on the other.<sup>27</sup> Enforcers have already enforced data minimization requirements – in a recent case about Alexa, the FTC penalized Amazon for retaining the digital imprints of children's voices

---

<sup>24</sup> FTC v. Amazon Flex, <https://www.ftc.gov/legal-library/browse/cases-proceedings/1923123-amazon-flex>

<sup>25</sup> FTC v. Everalbum, <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3172-everalbum-inc-matter>

<sup>26</sup> FTC v. Bronx Honda, <https://www.ftc.gov/news-events/news/press-releases/2020/05/auto-dealership-bronx-honda-general-manager-pay-15-million-settle-ftc-charges-they-discriminated>

<sup>27</sup> "Zero Trust AI Governance", Accountable Tech, AI Now Institute, and EPIC, August 10, 2023, <https://ainowinstitute.org/publication/zero-trust-ai-governance>.

indefinitely solely for the purpose of improving its AI system Alexa.<sup>28</sup> These kinds of secondary use practices are endemic throughout the industry, and need to be curbed. However, we need a stronger ex-ante enforcement regime rather than one-off actions: we have to stop playing whack a mole, identifying harms long after they've occurred.

Lastly, we need to strengthen our legislative tools to be prepared to effectively tackle the market structure and gatekeeper power of dominant digital platforms. These firms hold an unprecedented amount of economic and political power, which extend across the tech stack. There are several proposals already on the table that are instructive, including the American Innovation and Choice Online Act and the AMERICA Act, both of which highlight the importance of tackling large tech firms' gatekeeper role and influence in the broader economy. Preparing our regulatory and enforcement capabilities to meet the needs of the moment by tackling concentrated power in the tech industry is an urgent challenge, one which will have beneficial and wide-reaching effects for the public, for businesses and for our democracy.

I thank the esteemed members of the Subcommittee for convening us today to discuss these important issues.

---

<sup>28</sup> FTC v. Amazon, [https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever?utm\\_campaign=ftc\\_and\\_doj\\_charge\\_amazon&utm\\_content=1685561109&utm\\_medium=social&utm\\_source=twitter](https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever?utm_campaign=ftc_and_doj_charge_amazon&utm_content=1685561109&utm_medium=social&utm_source=twitter)