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

Bureau of Consumer Protection
Division of Privacy and Identity Protection

Remarks of Benjamin Wiseman at the Harvard Journal of Law & Technology on Worker Surveillance and AI

Harvard Law School
February 8, 2024[1]

Good afternoon. The last time I was at Harvard Law School was in February 2019 to attend the AGTech Forum organized by the Berkman Klein Center. The program was designed to bring together students and researchers at Harvard with privacy enforcers from State Attorneys General Offices. I left that event with an even greater appreciation for the important work that students and faculty at institutions like this one do to advance conversations around privacy and technology, and lift the enforcement work that regulators do across the country.

The goal of AGTech Forum was to address new and emerging technologies and the potential privacy implications for consumers. The focus that year centered on artificial intelligence, algorithms, and machine learning. Credit goes to the organizers for having the foresight to elevate these issues. At the time, though, we were just beginning to understand the potential impact of these technologies; indeed, our concerns then feel almost quaint now as we grapple with the consequences stemming from the explosion of generative AI, the sometimes startling capabilities (and equally unexpected deficiencies) of large language models, and what the press frequently describes as an AI "arms race" of deep-pocketed, highly invested corporate competitors.

As the 2019 workshop noted, with all of the promise of AI also come deep concerns. From a privacy perspective, one of the greatest concerns today is that many AI business models incentivize some of the same problematic conduct that we have seen over the past two decades when it comes to commercial surveillance. To power many AI models, companies want to maximize data collection, often collecting enormous amounts of personal information from unwitting consumers – and often without regard to the potential harms to those users from privacy invasions or from the models themselves.[2] In other words, on the heels of a decade of

[1] The views expressed here are my own and do not necessarily represent the views of the Commission or any Commissioner. I am grateful to David Walko for his substantial assistance in preparing these remarks.
[2] *AI Companies: Uphold Your Privacy and Confidentiality Commitments* (Jan. 9 2024), *available at* https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/ai-companies-uphold-your-privacy-confidentiality-commitments (explaining that many AI models "have a continuous appetite for data to develop new or customer specific models or refine existing ones"); *see also FTC v. Ring LLC*, 1:23-cv-1549 (D.D.C.), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/2023113-ring-llc; *US v. Amazon.com, Inc. et al.*, 2:23-cv-00811-TL (W.D. Wa. July 19, 2023), *available at* https://www.ftc.gov/legallibrary/browse/cases-proceedings/192-3128-amazoncom-alexa-us-v; Jonathan Turley, *ChatGPT falsely accused me of sexually harassing my students. Can we really trust AI?*, USA Today (April 3, 2023), https://www.usatoday.com/story/opinion/columnist/2023/04/03/chatgptmisinformation-

behavioral advertising fueling the overcollection of Americans' data, firms training algorithms and AI models are further entrenching commercial surveillance.

Much of the conversation around commercial surveillance focuses on how it impacts consumers when they're browsing the web, connecting with friends, sharing sensitive information with apps, or using connected products. And rightfully so. As our Director of the Bureau of Consumer Protection Samuel Levine, who spoke at your symposium last year, noted in a recent speech, unchecked commercial surveillance endangers consumers' privacy, financial welfare, and liberty.[3]

Today, however, I want to focus on how new surveillance and decision-making technologies are impacting Americans as workers. On one hand, these new technologies, which have emerged amid the rise of AI and gig work, are powering decision-making processes that can increase businesses' efficiency, potentially redounding to the benefit of consumers. On closer look, however, we also see troubling conduct: an emerging era of worker surveillance plagued with many of the same problems that characterize commercial surveillance. As workers across markets are increasingly data points subjected to automated decision-making, there are new threats to both their privacy and their autonomy. For us to realize the benefits of workplace AI, we need to grapple with the potential dark side of these technologies.

1. **Companies are collecting increasing amounts of personal information, including sensitive information, from workers.**

When it comes to surveillance and tracking, companies are collecting increasing amounts of personal information from workers. This includes collection of statistics on workers' activities, such as the number of messages workers send or receive as well as the frequency and length of meetings.[4] It also includes collection of data to purportedly monitor productivity. For example, one available software tool monitors salespersons' speaking pace, among other behaviors, to evaluate workers' sales interactions.[5] This type of tracking can be non-stop throughout the workday. Indeed, companies are tracking the time workers take to complete tasks down to the minute,[6] and how workers complete tasks, such as by taking screenshots of workers' computers and measuring the frequency of their keystrokes.[7]

---

bias-flaws-ai-chatbot/11571830002/.

[3] Samuel Levine, *Surveillance in the Shadows – Third-Party Data Aggregation and the Threat to our Liberties* (Sept. 21, 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf.

[4] Danielle Abril, *Here's what your boss might be able to see while you're at work*, The Washington Post (June 7, 2023), *available at* https://www.washingtonpost.com/technology/2023/06/07/work-monitoring-tools-surveillance-home-in-person/.

[5] Danielle Abril, *Companies want to use AI Tracking to make you better at your job*, The Washington Post (June 7, 2023), *available at* https://www.washingtonpost.com/technology/2023/06/07/ai-work-monitoring-surveillance-tools/.

[6] Lauren Kaori Gurley, *Internal Documents Show Amazon's Dystopian System for Tracking Workers Every Minute of Their Shifts*, VICE (June 2, 2022), *available at* https://www.vice.com/en/article/5dgn73/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts.

[7] Caroline O'Donovan, *This "Creepy" Time-Tracking Software Is Like Having Your Boss Watch You Every Second*, BuzzFeed News (Aug. 7, 2018), *available at* https://www.buzzfeednews.com/article/carolineodonovan/upwork-freelancers-work-diary-keystrokes-screenshot.

This pervasive worker surveillance by firms also increasingly involves the collection of highly sensitive personal information. For one, companies are now routinely collecting location data from their employees, such as when they clock in to start a shift or arrive at a field-based job.[8] We also have seen reports of new software and devices that measure workers' emotional and physical states implemented in multiple industries. These include wearable devices that collect and monitor health information,[9] as well as software that monitors call workers' tone and emotion.[10]

Perhaps most concerning, this collection doesn't just happen when a worker enters an office building or logs into their work device. It can also happen on workers' personal devices, including when workers are off site or at home – bringing employers directly into workers' personal lives. The opacity surrounding worker surveillance also means that few workers know precisely what information their employers collect and retain about them, how it is used, and whether it is sold to third parties and data brokers.

2. **The vast collection of data from workers creates serious risk of privacy harms and threatens workers' autonomy**.

Just as the overcollection of data can cause – and has caused – harm to consumers in their personal capacity, it also creates serious risks for consumers on the job. The FTC has brought numerous law enforcement actions alleging that commercial surveillance can, among other things, invade consumers' privacy and fuel highly targeted scam campaigns.[11] Our recent enforcement actions against firms that use and sell precise geolocation information also show how location data can track people's visits to sensitive locations such as medical and reproductive health clinics, places of religious worship, and domestic abuse shelters.[12] Such tracking invades consumers privacy[13] and exposes them to potential discrimination, physical

---

[8] *See*, *e.g.*, Janette Novak & Kelly Main, *Best Employee Time Tracking Apps of 2024*, Forbes (Jan. 7, 2024), *available at* https://www.forbes.com/advisor/business/software/best-employee-time-tracking-apps/ (highlighting the location tracking features available in many products); Colin Lecher, *What Happens When Nurses Are Hired Like Ubers*, The Markup (Oct. 5, 2023), *available at* https://themarkup.org/working-for-an-algorithm/2023/10/05/what-happens-when-nurses-are-hired-like-ubers.

[9] *See*, *e.g.*, Edward Ongweso Jr, *Amazon's New Algorithm Will Set Workers' Schedules According to Muscle Use*, VICE (April 15, 2021), *available at* https://www.vice.com/en/article/z3xeba/amazons-new-algorithm-will-set-workers-schedules-according-to-muscle-use; Ruqaiyah Zarook, *How the Trucking Industry Became the Dystopian Frontier of Workplace Surveillance*, Mother Jones (Dec. 6, 2022), *available at* https://www.motherjones.com/media/2022/12/data-driven-karen-levy-trucking-industry-surveillance/.

[10] *See, e.g.*, Tom Simonite, *This Call May Be Monitored for Tone and Emotion*, WIRED (Mar. 19, 2018), *available at* https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/.

[11] *See, e.g.*, *FTC v. Kochava Inc.*, 2:22-cv-00377-BLW (D. Idaho Aug. 29, 2022), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/ftc-v-kochava-inc; *FTC v. Sequoia One, LLC*, 2:15-cv-01512-JCM-CWH (D. Nev. Nov. 30, 2016), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3253-x150055-sequoia-one-llc.

[12] *In re InMarket Media, LLC*, No. C-XXXX (FTC Jan. 18, 2024), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/2023088-inmarket-media-llc; *In re X-Mode Social, Inc.*, No. C-XXXX (FTC Jan. 9, 2024), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/2123038-x-mode-social-inc.

[13] In a recent FTC action against data broker Kochava, the Court denied the Company's motion to dismiss finding that that the FTC adequately pled that Kochava's sale of precise geolocation information has the potential to "inflict a substantial injury on consumers by invading their privacy." Memorandum Decision and Order on Motion to

violence, stalking, and emotional distress.[14] And more broadly, companies' failure to minimize the data they collect creates systemics risks when more information is available to hackers and identity thieves.[15]

Workers subjected to invasive surveillance technologies may face these same risks. But workers may also face unique harms from the vast collection of their data. This includes, for example, the potential to deteriorate workers' rights. Indeed, some companies and vendors are building tools that purport to predict the risk of workers unionizing.[16]

Companies are also funneling the information they collect into AI models to make automated decisions that can have serious consequences for workers' autonomy, their physical and mental health, and their pay. AI management tools are increasingly used across industries and sectors, impacting delivery drivers, factory workers, and others.[17] As more workers become classified as gig-workers, some of the most problematic practices are becoming further entrenched.[18] AI wage setting software, for example, is commonly used to automatically set (and sometimes change in real time) workers' wages.[19] These tools often lack transparency so that workers can't understand how their work impacts their pay and they can unfairly lower wages.[20] Another common tool is in-time scheduling that sets workers' schedules without advance notice, subjecting workers to strenuous and unpredictable scheduling.[21] Notably, these potential harms may occur when the systems are working as designed. When they don't, the consequences could be even more severe. Inaccurate outputs or faulty algorithms raise the likelihood that workers

---

Dismiss First Amended Complaint, *FTC v. Kochava, Inc*, 2:22-cv-00377-BLW (D. Idaho Feb. 3, 2024), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/71-OpinionMTD.pdf.

[14] *See e.g.*, *In re InMarket Media, LLC*, *supra* note 12; *In re X-Mode Social, Inc.*, *supra* note 12.

[15] *See e.g.*, *US v. Amazon.com, Inc. et al.*, *supra* note 2.

[16] Sarah Kessler, *Companies Are Using Employee Survey Data to Predict – and Squash – Union Organizing*, OneZero (Jul. 30, 2020), *available at* https://onezero.medium.com/companies-are-using-employee-survey-data-to-predict-and-squash-union-organizing-a7e28a8c2158.

[17] *See, e.g.*, Ongweso, *supra* note 9; Dan Calacci and Alex Pentland, *Bargaining with the Black-Box: Designing and Deploying Worker-Centric Tools to Audit Algorithmic Management*, Proc. ACM Hum. Comput. Interact. 6, CSCW2, Article 428 (November 2022), *available at* https://doi.org/10.1145/3570601; *and* Veena Dubal, *On Algorithmic Wage Discrimination* (Jan. 19, 2023), at 37-38, UC San Francisco Research Paper No. Forthcoming, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4331080.

[18] Terri Gerstein, *More People Are Being Classified as Gig Workers. That's Bad for Everyone*, New York Times (Jan. 28, 2024), *available at* https://www.nytimes.com/2024/01/28/opinion/rights-workers-economy-gig.html.

[19] *See, e.g.*, Megan Cerullo, *How companies get inside gig workers' heads with "algorithmic wage discrimination"*, CBS News (April 18, 2023), *available* at https://www.cbsnews.com/news/algorithmic-wage-discrimination-artificial-intelligence/; Brian Merchant, *Column: If you work for Uber or Amazon, you may be a victim of algorithmic wage discrimination*, Los Angeles Times (April 11, 2023), *available at* https://www.latimes.com/business/technology/story/2023-04-11/algorithmic-wage-discrimination.

[20] *See* Calacci and Pentland, *supra* note 17 (finding for a large group of workers, a gig company's implementation of algorithmic wage setting led to an unannounced decrease in pay, sometimes resulting wages lower than the minimum wage).

[21] *See* Dubal, *supra* note 17.

will be unfairly subjected to adverse employment actions like pay cuts, discipline, or even termination.[22]

3. What is the role for the FTC?

What is the role of the FTC in all of this? The Commission's primary enforcement tool is Section 5 of the FTC Act, which prohibits unfair, deceptive, and anticompetitive trade practices. As the nation's leading privacy regulator, the Commission has years of experience addressing some of the most pressing privacy and technological issues facing the American public. The Commission's recent actions addressing AI facial recognition technology[23], data brokers[24], and health apps and websites[25] demonstrate that the FTC will not hesitate to combat emerging privacy harms and other abuses in the marketplace. The same applies to worker surveillance.

Indeed, the Commission is actively using the FTC Act to stop unfair, deceptive, and anticompetitive trade practices as they affect workers. For example, in 2021, the Commission resolved a case against Amazon, in which the FTC alleged that Amazon failed to pay tips to delivery drivers. The settlement required the company to turn over $60 million to compensate affected drivers.[26] Just last year, the Commission resolved an action against HomeAdvisor for making allegedly deceptive statements to contractors and other service providers who used the platform to find customers. The company was required to pay up to $7.2 million in redress.[27] And last year, the FTC proposed a new rule that would ban firms from imposing noncompete clauses on their workers.[28]

As worker surveillance and AI management tools continue to permeate the workplace, the Commission has made clear that it will protect Americans from potential harms stemming from these technologies. For example, in a 2022 policy statement on gig work, the Commission made clear how the FTC Act can apply in the worker context. In that policy statement, the Commission emphasized that companies may violate the FTC Act if they, for example, deploy surveillance technology to monitor gig workers' every move without transparency about how it impacts pay or performance evaluation.[29] And just last year, the Commission issued another policy statement

---

[22] The FTC's recent action against Rite Aid illustrates the potentially harmful consequences from AI tools generating inaccurate outputs. *See FTC v. Rite Aid Corporation*, 2:23-cv-5023 (E.D. Penn. Dec. 19, 2023), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

[23] *Id.*

[24] *FTC v. Kochava Inc.*, *supra* note 11; *In re X-Mode Social, Inc.*, *supra* note 12.

[25] *US v. GoodRx Holdings, Inc.*, 23-cv-460 (N.D. Cal. Feb. 1, 2023), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *US v. Easy Healthcare Corp.*, 23-cv-03107 (N.D. Ill. May 17, 2023), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In re BetterHelp, Inc.*, C-4796, *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter.

[26] *In re Amazon.com, Inc. and Amazon Logistics, Inc.*, C-4746, *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/1923123-amazon-flex.

[27] *In re HomeAdvisor, Inc.*, D-9407, *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/1923106-homeadvisor-matter .

[28] FTC, *Non-Compete Clause Rule* (January 9, 2023), *available at* https://www.regulations.gov/docket/FTC-2023-0007/document.

[29] FTC, *Policy Statement on Enforcement Related to Gig Work* (Sept. 15, 2022), *available at* https://www.ftc.gov/legal-library/browse/policy-statement-enforcement-related-gig-work (The statement further put

on biometric technologies, like facial recognition and iris scans, warning that companies that make deceptive statements about biometric technologies, fail to inform users about its use, or use biometric information in ways that are likely to cause harm without taking reasonable measures to mitigate injury may violate the FTC Act.[30]

To understand what the Commission expects from worker surveillance tools that collect sensitive information like geolocation information and biometrics, we can look to recent Commission actions against companies deploying such tools in other contexts. Last month, the Commission resolved an action against data broker X-Mode Social over allegations that the company sold consumers' precise geolocation data, including visits to sensitive locations, without reasonable safeguards to prevent misuse by third parties downstream.[31] The Complaint also alleges that the company failed to obtain or verify consumers' informed consent for the collection, use, and disclosure of their location data.[32]

The Commission also recently charged pharmacy chain Rite Aid with recklessly deploying facial recognition surveillance technology that erroneously tagged consumers, in particular women and people of color, as shoplifters.[33] The Complaint alleges that these false tags led to innocent consumers being followed by store employees, being asked to leave stores, and even having the police called on them. Among other things, we alleged that the company failed to conduct reasonable testing of the technology, failed to properly train those charged with using it, and failed to periodically assess the technology to identify and mitigate risks.[34]

The principles from these cases apply with equal force to individuals subjected to surveillance on the job. After all, a consumer's right to be protected from privacy harms and other injuries doesn't evaporate the minute they enter a factory or log into their computer. Companies that mislead workers about worker surveillance technologies, that fail to be transparent with workers about their collection of personal information, or that deploy technologies in ways that harm workers without corresponding benefits may face liability under the FTC Act.

---

firms on notice the vast collection of worker data through surveillance tools implicates several other laws and regulations enforced by the FTC, including the Safeguards Rule and the Fair Credit and Reporting Act).

[30] FTC, *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act* (May 18, 2023), *available at* https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-biometric-information-section-5-federal-trade-commission.

[31] Complaint at 3, *In re X-Mode Social, Inc.*, No. C-XXXX (FTC Jan. 9, 2024), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf.

[32] *Id.* The proposed order obtained by the FTC prohibits X-Mode from selling sensitive location data as well as requires the company to ensure that consumers have provided informed consent to the collection, use, and sale of their location data – if they don't, X-Mode can't use it. *In re X-Mode Social, Inc.*, No C-XXXX (FTC Jan. 9, 2024) (Provisions II, VI and VII), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-D%26O.pdf

[33] *See* Complaint for Permanent Injunction and Other Relief at 11-13, *FTC v. Rite Aid Corporation*, 2:23-cv-5023 (E.D. Penn. Dec. 19, 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf.

[34] *Id.* at 11-23. The proposed order in the case bans Rite Aid from using any facial recognition surveillance technology for five years. And if the company elects to use any biometric surveillance in the future, it must implement rigorous safeguards to prevent harm to consumers. Proposed Stipulated Order for Permanent Injunction and Other Relief, *FTC v. Rite Aid Corporation*, 2:23-cv-5023 (E.D. Penn. Dec. 19, 2023) (Attachment A at Provisions I and III), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_stipulated_order_filed.pdf.

Finally, under Chair Khan's leadership, the Commission is also taking steps to ensure that the FTC has the resources and expertise to address harms workers face from surveillance tools. We are doing this in two ways.

First, the Commission is forging relationships with partner agencies in federal government with expertise in the labor market. In the past two years, the Commission has entered into memoranda of understandings with both the National Labor Relations Board and the Department of Labor, recognizing our shared interest in protecting workers and, among other things, addressing the impact of algorithmic decision-making in the workplace.[35]

Second, the Commission is increasing its in-house capacity to investigate and analyze new technologies. In particular, last year the Commission voted to create the Office of Technology to build on the expertise at the agency and ensure we have the resources and skills to take on emerging technological developments in the marketplace.[36] Since its creation, the Office of Technology has recruited some of the best technologists – not just in government, but in the country – with a diverse range of backgrounds and expertise. Attorneys, economists, investigators, and other Commission staff work hand in hand with technologists every day to better understand new technologies, assess trends in the marketplace, and elevate our enforcement work.

* * *

In 2019, we were just starting to understand how AI, algorithms, and automated surveillance tools would impact the American public. Now several years later, we continue to encounter an ever-shifting technological landscape. We must continue the important work to keep pace with changing technologies, so that we can harness their benefits while staving off potential harms to consumers, including workers. That is where we need you – to stay engaged, to keep researching and exploring emerging technologies, and to remain focused on realizing the benefits of AI while ensuring that the privacy of *all* Americans, whether in their homes or on the job, is protected.

Thank you.

---

[35] FTC, *Memorandum of Understanding Between the Federal Trade Commission (FTC) and the National Labor Relations Board (NLRB) Regarding Information Sharing, Cross-Agency Training, and Outreach in Areas of Common Regulatory Interest* (July 2022), *available at* https://www.ftc.gov/legal-library/browse/cooperation-agreements/memorandum-understanding; FTC, *Memorandum of Understanding Between The U.S. Department of Labor and the Federal Trade Commission* (Sept. 2023), *available at* https://www.ftc.gov/legal-library/browse/cooperation-agreements/memorandum-understanding-between-us-department-labor-federal-trade-commission.

[36] FTC, *FTC Launches New Office of Technology to Bolster Agency's Work* (Feb. 17, 2023), *available at* https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-launches-new-office-technology-bolster-agencys-work.