Your Comment Submitted on Regulations.gov (ID: OSTP_FRDOC_0001-0008)

From no-reply@regulations.gov <no-reply@regulations.gov>

To Ashley Gjovik<ashleymgjovik@protonmail.com>

Date Thursday, June 29th, 2023 at 5:07 PM

Please do not reply to this message. This email is from a notification only address that cannot accept incoming email.

Your comment was submitted successfully!
Comment Tracking Number: ljh-mm9t-ux8w

Your comment has been sent for review. This process is dependent on agency public submission policies/procedures and processing times. Once the agency has posted your comment, you may view it on Regulations.gov using your Comment Tracking Number.

Agency: OFFICE OF SCIENCE AND TECHNOLOGY POLICY (OSTP)
Document Type: Notice
Title: Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management
Document ID: OSTP_FRDOC_0001-0008

Comment:
I am filing a comment on behalf of myself, a worker with US labor agency charges & cases that involve critical public policy concerns about worker surveillance and electronic monitoring. Please see attached memo in response to this request for information.

Uploaded File(s):
OSTP Gjovik Comment 2023.pdf

For further information about the Regulations.gov commenting process, please visit https://www.regulations.gov/faq.

Ashley M. Gjovik, J.D.
ashleymgjovik@protonmail.com

Request for Information:

Automated Worker Surveillance and Management

Federal Register No. 2023-12995

Doc ID: OSTP_FRDOC_0001-0008

U.S. OFFICE OF SCIENCE AND TECHNOLOGY POLICY

INFORMATION

Associated Cases:

U.S. Department of Labor:
Ashley Gjovik v Apple (9-3290-22-051)

U.S. National Labor Relations Board
NLRB v Apple (32-CA- 284428)

California Department of Labor:
Ashley Gjovik v Apple (RCI-CM-842830)

Associated Investigations:

U.S. National Labor Relations Board
Charge No. 32-CA-282142, 32-CA-283161, & 32-CA-288816 (Division of Advice & Region 31)

U.S. Federal Trade Commission
Report No. 154835129

U.S. Securities & Exchange Commission
Tip No. 16488- 304-158- 087 (SF Regional Office)

German Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Complaint No. # 11-540 II#3693 (Bavaria Office)

TABLE OF CONTENTS

ORIGINALLY SUBMITTED AS "COMPLAINT FOR INVASION OF PRIVACY" IN APRIL 2022;
REVISED FOR OSTP IN JUNE 2023

INFORMATION FOR OSTP ON AUTOMATED WORKER SURVEILLANCE AND MANAGEMENT IN THE UNITED STATES

June 29, 2023

To Whom it May Concern,

The United States' legal protections for human rights at work lags far behind countries in the European Union, especially France and Germany. Similarly, national legal protections for digital privacy are basically non-existent in the United States and are decades behind other nations.

Over the last few years, we have witnessed increasing surveillance, electronic monitoring, and digital exploitation of workers in the United States. We have also seen an increasing number of requests from politicians, agencies, unions, and civil society asking the US government for legal protections for workers.

Despite numerous and persistent requests from Senators,[1] NGOs,[2] unions, and from workers themselves[3] – there is no progress to be seen. Despite a number of agency memos[4] and social media posts, we have yet to see any new legal protections or even any meaningful enforcement of violations of existing laws.

While you will likely receive comments and information from groups with more expertise on the history, policy, and legal landscape of this topic – what I can offer you is a first-hand case study in failure.

My story as a worker in the United States, for one of the biggest companies in this country, highlights the lack of legal protections for workers, the lack of express privacy protections for citizens, and the lack of any actual enforcement mechanism even for egregious violations of the narrow privacy/labor laws we do have on the books today. My story also highlights how my employer understood this current landscape and thus acted with an aggressive

[1] Letter from Senator Casey to U.S. Department of Labor, August 26 2022, https://www.casey.senate.gov/imo/media/doc/letter_to_the_department_of_labor_re_worker_privacy.pdf

[2] *CDT, GFI, Others Send Memos Urging White House to Take Action on Electronic Workplace Surveillance,* April 3 2023, https://cdt.org/insights/cdt-gfi-others-send-memos-urging-white-house-to-take-action-on-electronic-workplace-surveillance/ ; AI Now, *Algorithmic Management: Restraining Workplace Surveillance*, https://ainowinstitute.org/publication/algorithmic-management

[3] TechCrunch, *Ex-Apple employee takes Face ID privacy complaint to Europe*, April 11 2022, https://techcrunch.com/2022/04/11/gobbler-complaint-europe/

[4] U.S. NLRB, *NLRB General Counsel Issues Memo on Unlawful Electronic Surveillance and Automated Management Practices*, https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and

disregard for the law, ethics, or social norms. So far, they were right & they have faced no consequences.

In March 2022, I received a written statement from my employer's lawyers admitting they fired me (with multiple federal investigations already open due to my charges against them for whistleblower retaliation, environmental and labor violations, and fraud); but claiming I was not fired in retaliation for that, but instead fired for supposedly 'legal' retaliation for my protests of their unlawful surveillance of employees, their intimidation and censorship of employees, and their coercive harvesting of sensitive worker information in order to build their products (in ways that they admitted in writing that would be illegal in France of Germany).[5] In response, in addition to complaining further to US agencies, I also filed a complaint to other countries where my ex-employer has large offices.[6]

Despite overwhelming evidence and even a written confession admitting what my employer has done, my charges have sat with federal agencies for nearly two years now gathering dust. Despite my being a US citizen and all of this occurring within the United States, as far as I can tell, there has been more progress investigating my claims in Germany then there has been in the United States.[7]

Introduction

I worked for Apple as a Senior Engineering Program Manager from February 2015 until my termination on September 9 2021. During my tenure with Apple, I participated in engineering project management of numerous high-profile products such as the iPhone, iPad, iPod, Apple Watch, MacBook MacBook Pro, MacBook Air, Mac Pro, iOS, macOS, watchOS -- and high-profile projects/programs such as the launch of the Apple Music subscription service, Apple's transition of computers from Intel to Apple silicon, and the development of a company-

[5] Gizmodo, *Apple Wanted Her Fired. It Settled on an Absurd Excuse*, Oct 14 2021, https://gizmodo.com/apple-wanted-her-fired-it-settled-on-an-absurd-excuse-1847868789

[6] Télérama, *Ashley Gjøvik, lanceuse d'alerte licenciée par Apple, seule contre tous*, March 14 2023, https://www.telerama.fr/debats-reportages/ashley-gjovik-lanceuse-d-alerte-licenciee-par-apple-seule-contre-tous-7014661.php

[7] Der Speigel, *Apple lädt Mitarbeiter zu Datenparty – um Gesichter zu scannen*, June 24 2022, https://www.spiegel.de/netzwelt/gadgets/apple-laedt-mitarbeiter-zu-daten-party-um-gesichter-zu-scannen-a-54c4a2da-0f39-48be-9762-1bda39fcca8e

wide Artificial Intelligence ethics policy. I was told by my Apple managers that I was both "key talent" (irreplaceable) and a "high performer."

In August 2021, I expressed public concerns about Apple's overly restrictive and invasive employee policies, and Apple pressuring its employees to participate in invasive data collection procedures, including scans of ears/ear canals (which I believed captured employee data that could be used for biometric identification and mass surveillance). I also raised concerns about an iOS application (the Face "Gobbler") on employees' iPhones that automatically took photos/videos whenever it "*thought it saw a face*." [8] I raised concerns about Apple's unlawfully invasive "*Search and Privacy Policy*" for employees, Apple's limitless access to employees' personal iCloud/Apple-server-based data, and Apple's culture of intimidation and secrecy including a private police force with access to all of the above data.[9]

Apple terminated me on September 9 2021 for reasons unknown to me at that time but assumed by myself and the press to be retaliation for my protected activities (I had filed labor and retaliation charges with the U.S. government only weeks earlier; and the US EPA demanded an inspection of my Superfund office due to my disclosures, conducted the inspection and found CERCLA non-compliance issues also only weeks prior).[10] [11]

Apple contacted me via external lawyers a week after I was fired to complain about several Twitter posts I made. Suggesting these posts were the reason for my termination was so farfetched & pretextual that a detailed article was written about it, titled "*Apple Wanted Her Fired. It Settled on an Absurd Excuse*."[12]

Last year, Apple offered their explanation for my termination to the U.S Department of Labor (in response to my allegations of federal whistleblower retaliation in violation of SOX,

[8] Zoe Schiffer, *"Apple Cares About Privacy, Unless You Work at Apple,"* The Verge, Aug 30, 2021, https://www.theverge.com/22648265/apple-employee-privacy-icloud-id

[9] Sarah Roach**,** *"Worker surveillance is making employees miserable. What to consider before implementing monitoring tools,"* Protocol, Sept 20 2021, https://www.protocol.com/workplace/worker-surveillance-is-making-employees-miserable

[10] Patrick McGee, *"US labour board examines retaliation claims against Apple: Senior engineering program manager's allegations include workplace harassment and job reassignment,"* Financial Times, Sept 2 2021, https://www.ft.com/content/484fa8be-925e-495c-91ff-54950b112754

[11] US EPA, TRW Microwave Superfund, https://cumulis.epa.gov/supercpad/SiteProfiles/index.cfm?fuseaction=second.docdata&id=0901181

[12] Dell Cameron, *Apple Wanted Her Fired. It Settled on an Absurd Excuse,* Gizmodo (Oct 2021), https://gizmodo.com/apple-wanted-her-fired-it-settled-on-an-absurd-excuse-1847868789

CERCLA, and OSHA statutes).[13] Apple doubled down on the "absurd excuse" & cited my opposition to their harvesting of employee biometrics and their secret, invasive photography of employees as a legitimate justification for my termination.[14] I am now even more concerned knowing Apple felt comfortable telling the U.S. government that they believe their unlawful invasion of employee privacy is "legitimate" and any employees who protest privacy invasions deserve to be terminated, as I was. Any argument Apple had that employees consented to these practices was thrown out the window when they formally claimed I was terminated without warning for protesting those practices.

APPLE'S CULTURE OF "LOYALTY" & INTIMIDATION

I will describe some of these practices which Apple claimed were so secret, they'd terminate an employee for protesting and exposing them. However, first, it is important to establish that at Apple, there is a long-standing tradition that workers keep their mouths shut, do what they are told, and be 'loyal' to the company above all else.

GDPR recognizes that employment relationships are inherently coercive and thus employees cannot provide meaningful consent to invasive surveillance and data collection practices. In the US, we sometimes still default to a neoliberal view that a 'request' or 'preference' from an employer is somehow optional and thus employees have agency to decline. This is not accurate and Apple provides an incredible example of how many US companies operate but may be too afraid to explain aloud. Apple says the quiet parts aloud because they have terrorized their employees to the extent Apple was sure their employees would not report the misconduct.

In stark contrast to international labor standards, Apple's "**Worldwide Loyalty Team**" *"does KGB-style lockdowns [of employees] and Gestapo interrogations that end in suicides."* [15] The team is an *"internal secret police team known for its network of informers, and ruthless,*

[13] Patrick McGee, "*Apple faces probe over whether it retaliated against whistleblower,"* Financial Times, Dec 13 2021, https://www.ft.com/content/973aae8d-21d9-4e84-8912-ead071c7935d

[14] Letter from Apple Inc (via Orrick, Herrington & Sutcliffe LLP) to U.S. Department of Labor, March 4 2022, Re: *Ashley Gjovik v. Apple Inc.*, Case No. 9-3290-22-051

[15] Gawker, *Apple's Sleazy Secret Police Lose Their Leader*, Nov 4 2011, https://www.gawker.com/5856260/apples-sleazy-secret-police-lose-their-leader

systematic pursuit of leakers."[16] "Among some employees, they are known as the "*Apple Gestapo*," *a group of moles always spying in headquarters and stores, reporting directly to the CEO*."[17] Apple holds out its security policies out as "*voluntary*" meanwhile: *"management recommends that you relinquish your phones. If you don't do it they will fire you, or they will investigate why you didn't want to give them your cellphone*."[18]

Apple's Global Security team has a sketchy history, including Apple employees accused in 2011 of impersonating policemen and searching a man's San Francisco home for a lost prototype, and threatening to have the man deported if he did not cooperate.[19] Apple was also accused in 2010 of violating California's shield law with an illegal search warrant, when they searched the home of a journalist, again looking for a prototype.[20] Gawker described Apple's secret police as "*sleazy*."

Apple employees' experience with this *Gestapo* have been described by the press as *"knowing how it feels to be watched, to always be considered guilty of crimes against another kind of state. Knowing how it felt to have no privacy whatsoever when he was working right here, in a little Californian town called Cupertino, in a legendary place located in One Infinite Loop.*"[21] Indeed, a few years later an ex-Apple executive described the culture at Apple as "*everything is on a need-to-know basis*" and that Apple has "*cells, **like a terrorist organization***."[22]

Further, while some Apple employees may report an earnestly positive experience, the company is large and has decades of history of very negative experiences for many others. Apple has gone to great lengths to conceal and cause society to forget its bad behavior. Apple has a

[16] Gawker, *Apple's Sleazy Secret Police Lose Their Leader*, Nov 4 2011, https://www.gawker.com/5856260/apples-sleazy-secret-police-lose-their-leader
[17] Gizmodo, *Apple Gestapo: How Apple Hunts Down Leaks*, Dec 15 2009, https://gizmodo.com/apple-gestapo-how-apple-hunts-down-leaks-5427058
[18] Gawker, *Apple's Sleazy Secret Police Lose Their Leader*, Nov 4 2011, https://www.gawker.com/5856260/apples-sleazy-secret-police-lose-their-leader
[19] Gawker, *Apple's Sleazy Secret Police Lose Their Leader*, Nov 4 2011, https://www.gawker.com/5856260/apples-sleazy-secret-police-lose-their-leader
[20] CNET, *Apple pushed security executive out,* https://www.cnet.com/news/source-apple-pushed-security-executive-out/ ; MarketWatch,*Police task force oversight committee has included Apple*, https://www.marketwatch.com/story/apple-has-sat-on-steering-committee-for-task-force-2010-04-27
[21] Gawker, *Apple's Sleazy Secret Police Lose Their Leader*, Nov 4 2011, https://www.gawker.com/5856260/apples-sleazy-secret-police-lose-their-leader
[22] *This Is How Apple Keeps the Secrets,* 2012, https://fortune.com/2012/01/18/the-secrets-apple-keeps/

long history of child labor,[23] "sweatshop" working conditions,[24] hexane poisoning,[25] mishandling of toxic waste,[26] worker "interrogations" leading to suicide,[27] suicides at the corporate headquarters,[28] "no-suicide vows,"[29] "suicide nets,"[30] and even lobbying **for** forced labor.[31] Workers from Silicon Valley to Albania complain of surveillance, invasions of privacy, oppression, and unsafe work conditions.[32]

Apple workers around the globe have been involved in organizing since at least the 1990s. Apple worker organizations have been made up of retail, corporate, contract, and other workers. Unionization efforts started in the United States back in 1991 with Apple's janitors successfully unionizing with SEIU through protests, boycotts, press coverage, and even a hunger strike.[33]

In 2013, retail workers started organizing a "Apple Retail Workers Union" and calling for a formal labor union.[34] Apple security guards started organizing and looking to form a union in 2014

[23] Guardian, "*Child labour uncovered in Apple's supply chain: Internal audit reveals 106 children employed at 11 factories making Apple products in past year,"* 2013 , https://www.theguardian.com/technology/2013/jan/25/apple-child-labour- supply; BBC, "*Apple, Samsung and Sony face child labour claims*," 2016, https://www.bbc.com/news/technology-35311456 ; AP, "*Lawsuit: Apple, Microsoft profit from child cobalt miners*," 2019, https://apnews.com/article/technology-business- africa-lawsuits-politics-a950d585f885f670aee416db8973e3f3

[24] Washington Post, "*Sweatshop Conditions at IPod Factory Reported*," 2006, https://www.washingtonpost.com/wp- dyn/content/article/2006/06/15/AR2006061501898.html

[25] ICRT, "*Harsh Reality Behind Apple Scandal,"* https://icrt.co/harsh-reality-behind-apple-scandal/ ; Wired, "*Workers Plan to Sue iPhone Contractor Over Poisoning*," 2010 https://www.wired.com/2010/05/wintek-employees-sue/

[26] California DTSC, "*Apple Agrees to Pay $450,000 to Settle Hazardous Waste Violations*," 2016, https://dtsc.ca.gov/2016/12/06/apple-agrees-to-pay-450000-to-settle-hazardous-waste-violations/

[27] Gizmodo, "*Report: iPhone Leak Interrogations Drive Foxconn Employee to Suicide,"* 2009, https://gizmodo.com/report- iphone-leak-interrogations-drive-foxconn-employ-5319275

[28] CNN, *"Apple employee found dead at HQ shot himself,"* 2016, https://money.cnn.com/2016/04/28/technology/apple- employee-death-gun-suicide/index.html

[29] NBC News, "*Chinese factory asks for 'no suicide' vow,"* 2010, nbcnews.com/id/wbna37354853

[30] WIRED, "*Foxconn Rallies Workers, Leaves Suicide Nets in Place*," 2010, https://www.wired.com/2010/08/foxconn- rallies-workers-installs-suicide-nets/

[31] Washington Post, "*Apple is lobbying against a bill aimed at stopping forced labor in China*," 2020, https://www.washingtonpost.com/technology/2020/11/20/apple-uighur/

[32] What It's Like to Work Inside Apple's 'Black Site': Contractors a few miles from the company's spaceship-like headquarters live in fear of termination—and the bathroom lines. Bloomberg, (Feb 2019), https://www.bloomberg.com/news/features/2019-02-11/apple-black-site-gives-contractors-few-perks-little-security ; Big Tech call center workers face pressure to accept home surveillance: Workers at one of the world's largest call center companies said additional monitoring would violate the privacy of their families in their homes. NBC News: (Aug 2021), https://www.nbcnews.com/tech/tech-news/big-tech-call-center-workers-face-pressure-accept-home-surveillance-n1276227

[33] UNION CLAIMS KEY VICTORY IN BID TO `CLEAN UP` SILICON VALLEY, Chicago Tribune, 1992, https://www.chicagotribune.com/news/ct-xpm-1992-07-20-9203050495-story.html

[34] Apple Store Employee Cory Moll Seeks Union For Retail Staffers, Huffpost, Jun 13 2011, https://www.huffpost.com/entry/apple-store-employees-union-cory-moll-retail-workers_n_875767

with SEIU.[35] At that time, a USWW union executive complained, "*Apple frequently intimidates workers and retaliates against those who get involved with the union around the country*." [36]

In 2015, Apple shuttle and bus drivers successfully unionized with the Teamsters.[37] Starting in 2022, numerous Apple Retail Stores in the US have attempted to unionize.[38] Union-busting tactics were already reported early on.[39] Apple retail store employees in Atlanta Georgia withdrew an election citing 'illegal union-busting tactics' by Apple.[40] "*Apple has conducted a systematic, sophisticated campaign to intimidate them and interfere with their right to form a union,"* the CWA representative said. [41] NLRB General Counsel found merit Apple was unlawfully forcing workers to attend captive audience meetings.[42] In September 2022, an Oklahoma City Apple retail store petitioned for an election, represented by CWA, and voted to unionize in October of 2022. They also filed charges with the NLRB against Apple for *"illegally surveilling, threatening and questioning workers at the Oklahoma City store."* [43] [44]

In October 2022, the NLRB issued a complaint against Apple over accusations that Apple interrogated its retail workers about their union support and prevented pro-labor fliers in a store break room.[45] The union accused Apple of interrogating staff at a World Trade Center store and

[35] Guards Need Job Security of Their Own, Say Apple Store Protesters, In These Times, 2014, https://inthesetimes.com/article/guards-need-security-of-their-own-say-apple-store-protesters
[36] Guards Need Job Security of Their Own, Say Apple Store Protesters, In These Times, 2014, https://inthesetimes.com/article/guards-need-security-of-their-own-say-apple-store-protesters
[37] Silicon Valley Shuttle Drivers Vote to Join Union, Feb 2015, NYT, https://archive.nytimes.com/bits.blogs.nytimes.com/2015/02/28/silicon-valley-shuttle-drivers-vote-to-join-union/?_r=0
[38] Some U.S. Apple Store employees are working to unionize, part of a growing worker backlash, Washington Post, Feb 18 2022, https://www.washingtonpost.com/technology/2022/02/18/apple-retail-stores-union-labor/
[39] Some U.S. Apple Store employees are working to unionize, part of a growing worker backlash, Washington Post, Feb 18 2022, https://www.washingtonpost.com/technology/2022/02/18/apple-retail-stores-union-labor/
[40] Apple Atlanta Workers Drop Bid for Union Vote Next Week, Claiming Intimidation, Bloomberg, May 27 2022, https://www.bloomberg.com/news/articles/2022-05-27/apple-atlanta-workers-drop-bid-for-unionization-vote-next-week
[41] Apple Atlanta Workers Drop Bid for Union Vote Next Week, Claiming Intimidation, Bloomberg, May 27 2022, https://www.bloomberg.com/news/articles/2022-05-27/apple-atlanta-workers-drop-bid-for-unionization-vote-next-week
[42] The Fallout From Apple's Bizarre, Dogged Union-Busting Campaign, WIRED, July 28 2022, https://www.wired.com/story/apples-union-busting-campaign-caused-a-bad-fallout/
[43] An Apple Store in Oklahoma City votes to unionize, TechCrunch, Oct 15 2022, https://techcrunch.com/2022/10/15/an-apple-store-in-oklahoma-city-votes-to-unionize/
[44] Apple Employees in Oklahoma City Petition to Unionize Store, Bloomberg, September1 2022, https://www.bloomberg.com/news/articles/2022-09-01/apple-employees-in-oklahoma-city-petition-to-unionize-store?sref=ExbtjcSG
[45] NLRB Issues Complaint Against Apple, NYT, Oct 4 2022, https://www.nytimes.com/2022/10/04/business/apple-store-nlrb-ruling.html

discriminating against union supporters in enforcing a no-soliciting policy.[46] In June 2023, an NLRB judge ruled against Apple, finding Apple violated federal labor law.[47]

In December 2022, Apple retail workers organizing with CWA in Columbus Ohio filed a complaint to the NLRB alleging Apple was "*soliciting employees to join an employer-created / employer-dominated labor organization as a means of stifling union activities"* (aka an unlawful company union) in addition to holding captive audience meetings and making threats. [48] In December 2022, NLRB found merit that Apple violated the NLRA in Atlantic Georgia.[49] In January 2023, NLRB found merit in five unfair labor practice charges filed by corporate employees.[50]

In China, Apple directly employs 12,000 workers across its retail and corporate divisions and claims agency over 4.8 million workers in the country; likely most are contracted through Apple's suppliers and manufacturing plants, including at least 1.2 million working at Foxconn's iPhone assembly factories.[51] Foxconn is the largest unionized company in the world. Foxconn made global headlines with a wave of worker suicides at the company's Chinese plants in 2009 and 2010, and after its treatment of its huge workforce has attracted intense scrutiny. Foxconn and Apple's response to the suicides was to have large nets installed outside many of the buildings to catch falling bodies ("suicide nets"), and workers were made to sign pledges stating they would not attempt to kill themselves.[52] Foxconn has become a focus for criticism of practices widespread in Chinese factories including illegal overtime, low pay, and the use of underage workers.[53] Even last year, Foxconn's Apple factories were in the news again – now with allegations of indentured servitude and

[46] Apple Created a Pseudo-Union to Defeat Organizers in Ohio, Complaint Claims, Bloomberg, December 16 2022, https://www.bloomberg.com/news/articles/2022-12-16/apple-created-pseudo-union-to-defeat-organizers-complaint-says

[47] Bloomberg, *Apple Illegally Interrogated Staff About Union, Judge Rules*, June 2023, https://www.bloomberg.com/news/articles/2023-06-21/apple-illegally-interrogated-staff-about-union-judge-rules

[48] Apple Created a Pseudo-Union to Defeat Organizers in Ohio, Complaint Claims, Bloomberg, December 16 2022, https://www.bloomberg.com/news/articles/2022-12-16/apple-created-pseudo-union-to-defeat-organizers-complaint-says

[49] Apple Created a Pseudo-Union to Defeat Organizers in Ohio, Complaint Claims, Bloomberg, December 16 2022, https://www.bloomberg.com/news/articles/2022-12-16/apple-created-pseudo-union-to-defeat-organizers-complaint-says

[50] Apple Executives Violated Worker Rights, Labor Officials Say, Bloomberg, Jan 30 2023, https://www.bloomberg.com/news/articles/2023-01-30/apple-executives-violated-worker-rights-us-labor-officials-sa

[51] Apple Supports 4.8 Million Jobs in China, More Than Double US Total, Yahoo, March 17 2017 , https://www.yahoo.com/news/apple-supports-4-8-million-135220928.html

[52] Life and death in Apple's forbidden city, The Guardian, Jun 18 2017, https://www.theguardian.com/technology/2017/jun/18/foxconn-life-death-forbidden-city-longhua-suicide-apple-iphone-brian-merchant-one-device-extract

[53] Foxconn plans Chinese union vote, CNN, Feb 4 2013, https://edition.cnn.com/2013/02/03/business/china-foxconn-union/index.html

trafficking, and when workers protested the abuse, they were met with beatings by state police.[54]

On December 18, 2014, retail workers in Apple's Japan stores announced a union affiliated with Tozen. Three of Japan's ten Apple stores are now unionized with Tozen.[55] There have also been unions and worker protests in India. In December 2020, thousands of contract workers at a Bangalore factory owned by Apple supplier Wistron Corp protested over alleged non-payment of wages.[56] Other violations highlighted found upon further investigation included underpayment of wages to contract workers and housekeeping staff, and making female staff work overtime without legal authorization.[57] In December 23 2021, 159 workers protested for poor working conditions and a mass poisoning incident.[58] Twenty-two activists, including leaders of the Centre of Indian Trade Unions (CITU), were put behind bars for extending support to the workers and visiting them. [59]

In September 2022, Australian workers brought Apple to the Fair Work Commission over employee demands for better pay and a guaranteed weekend.[60] The workers secured a protected action order with the nation's Fair Work Commission, which would allow them to protest without risking their jobs or getting sued.[61] The national secretary of the SDA Union, accused Apple of acting like "a cheap bully in a cheap suit" and said it never should have taken intervention from the Fair Work Commission for Apple to come to the table. "This giant multinational should have more regard for the welfare of its Australian workforce than to try to dictate a pre-determined outcome it wants to impose rather than engaging in genuine bargaining. This is Australia not the United States," he said.[62] In October 2022, with three Australian unions negotiating with Apple for better pay,

---

[54] Foxconn apologizes for pay dispute at China factory, San Diego Union-Tribune, Nov 24 2022, https://www.sandiegouniontribune.com/business/nation/story/2022-11-24/foxconn-apologizes-for-pay-dispute-at-china-factory

[55] Apple Retail Workers Unionize in Japan, Tozen, 2014, https://tozenunion.org/apple-retail-workers-unionize-in-japan/

[56] India: arrests made after protest over food poisoning at Apple supplier Foxconn site in Chennai , SCMP, December 20 2021, https://www.scmp.com/news/asia/south-asia/article/3160425/india-arrests-made-after-protest-over-food-poisoning-apple

[57] Apple puts supplier Wistron on notice after Indian factory violence, Reuters, December 19 2020, https://www.reuters.com/article/apple-india-idCAKBN28T0DW

[58] TN: Underpaid and Exploited Foxconn Workers Burst in Protest After Workers Fell ill, Newsclick, 23 December 2021, https://www.newsclick.in/TN-Underpaid-Exploited-Foxconn-Workers-Burst-Protest-Workers-Fell-ill

[59] TN: Underpaid and Exploited Foxconn Workers Burst in Protest After Workers Fell ill, Newsclick, 23 December 2021, https://www.newsclick.in/TN-Underpaid-Exploited-Foxconn-Workers-Burst-Protest-Workers-Fell-ill

[60] 'Bully in a cheap suit': Apple agrees to negotiate with Australian staff after union showdown, The Guardian, September 21 2022, https://www.theguardian.com/technology/2022/sep/21/bully-in-a-cheap-suit-apple-agrees-to-negotiate-with-australian-staff-after-union-showdown

[61] Australian Workers Are the Latest International Apple Staff to Unionise, VICE, September 8 2022, https://www.vice.com/en/article/qjk3eb/australian-workers-union-apple-strike

[62] 'Bully in a cheap suit': Apple agrees to negotiate with Australian staff after union showdown, The Guardian, September 21 2022, https://www.theguardian.com/technology/2022/sep/21/bully-in-a-cheap-suit-apple-agrees-to-negotiate-with-australian-staff-after-union-showdown

benefits, and working conditions – 150 workers engaged in a strike.[63]

Apple is a huge multinational corporation based in the United States with a long history of labor and human rights violations in their domestic and international supply chain and operations. If Apple is not held accountable in the country the corporation is headquartered in, what hope do other countries have in enforcing international labor standards against Apple abroad? The United States must set expectations for Apple here & abroad – that whether it is California labor and privacy laws, United States labor statutes, foreign national labor laws, or international standards such as from the International Labor Organization – whether it is employees, contractors, or vendors – Apple should be expected to made a good faith effort to follow the law, and governments should be able to investigate allegations of misconduct with independence and integrity. But that is not occurring; enter, my case study.

Electronic Monitoring & Data Collection

"FACE ID"& APPLE'S FACE "GOBBLER" APPLICATION

Apple announced its "Face ID" iPhone authentication feature on September 12, 2017.[64] Face ID captures, collects, and possesses Face ID users' facial geometry by *"projecting and analyzing tens of thousands of invisible dots to create a depth map of [the user's] face and also captures an infrared image of [the user's] face."*[65] Face ID data is "*refined and updated as [users] use Face ID*."[66] Apple says their average users unlock their phones 80 times a day, but other reports state people look at their phones upwards of 130 times a day.[67] Apple says Face ID is "*attention aware*" and only unlocks an iPhone when the user's eyes are open and looking at the screen.[68]

---

[63] New Crack in Apple's Armor as Dozens Strike at Its Stores in Australia, NYT, Oct 18 2022, https://www.nytimes.com/2022/10/17/business/apple-store-strike-australia.html
[64] Apple announced Face ID during the unveiling of the iPhone X on September 12, 2017, https://www.theverge.com/2017/9/12/16288806/apple-iphone-x-price-release-date-features-announced
[65] Apple Inc, *About Face ID advanced technology*, https://support.apple.com/en-us/HT208108
[66] Apple Inc, *Face ID Privacy*, https://www.apple.com/legal/privacy/data/en/face-id/
[67] Ben Bajarin, *Apple's Penchant for Consumer Security*, Techpinions, April 2016, https://techpinions.com/apples-penchant-for-consumer-security/45122,
[68] Apple Inc, *Change Face ID and attention settings on iPhone*, https://support.apple.com/en-ph/guide/iphone/iph646624222/ios

Privacy concerns arose quickly after launch, the security of biometrics gathered/stored by Face ID.[69] TechCrunch wrote, *"Face ID raises a range of security and privacy concerns because it encourages smartphone consumers to use a facial biometric for authenticating their identity and specifically a sophisticated full three-dimensional model of their face.*"[70] Concerns were also raised the year before about Apple's "faceprints" in its Photos applications. The Verge wrote, *"There's a real privacy issue at stake… Facial recognition can be put to some very creepy uses when faceprints are freely available."* [71]

A researcher warned in 2017, "*once the Face ID system is enabled, the iPhone X can become a potential technology for users to be spied on without noticing. Information about faces can contain a lot of personal information like age, gender, race but also emotions. Face ID can recognize these emotions and this information can for example be combined with on-screen content like advertisements and websites. Face ID technology might also 'read' the environment of the iPhone's user. The technology might be aware of the user's specific living conditions."* [72]

In 2017, Senator Al Franken wrote to Apple (via Tim Cook), expressing concerns and requesting clarifications about the privacy of Apple's Face ID feature. Apple responded saying, "*Face ID uses facial matching neural networks that we developed using over a billion images, including IR and depth images collected* ***in studies conducted with the participants' informed consent***." [73] Meanwhile, however, Apple was pressuring employees to upload their "faceprint data" to Apple internal servers, capturing secret photographs and videos of employees, and told employees that face-related logs were automatically uploaded from their iPhones daily. Further, with Apple's internal Mobile Device Management (MDM) profiles and other security tools, it's doubtful whether the data would even need to be "uploaded" or if Apple already had access if they wanted it. [74]

---

[69] App developer access to iPhone X face data spooks some privacy experts, https://www.reuters.com/article/us-apple-iphone-privacy-analysis/app-developer-access-to-iphone-x-face-data-spooks-some-privacy-experts-idUSKBN1D20DZ

[70] Natasha Lomas, *Apple responds to Senator Franken's Face ID privacy concerns*, TechCrunch (October 17, 2017), https://techcrunch.com/2017/10/17/apple-responds-to-senator-frankens-face-id-privacy-concerns/

[71] The Verge, *Apple's new facial recognition feature could spur legal issues,* 2016, https://www.theverge.com/2016/6/16/11934456/apple-google-facial-recognition-photos-privacy-faceprint

[72] Amber de Zeeuw, *iPhone Face ID: Privacy issues we should worry about*, 2017, https://mastersofmedia.hum.uva.nl/blog/2017/09/25/iphone-face-id-privacy-issues-we-should-worry-about/

[73] Natasha Lomas, *Apple responds to Senator Franken's Face ID privacy concerns*, TechCrunch (October 17, 2017), https://techcrunch.com/2017/10/17/apple-responds-to-senator-frankens-face-id-privacy-concerns/

[74] CDEMI, *Never accept an MDM policy on your personal phone,* 2019, https://blog.cdemi.io/never-accept-an-mdm-policy-on-your-personal-phone/

In 2017, Craig Federighi said that because "*the [Face ID training] data needed to include a high-fidelity depth map of facial data*," "*Apple **went out and got consent from subjects** to provide scans that were **quite exhaustive**. Those scans were taken from many angles and contain a lot of detail that was then used to train the Face ID system*." [75]

On Jan 9 2019, the Apple manager running Gobbler, posted an article to LinkedIn called "Data Collection" where he wrote, "*During the lead up to Face ID being launched, **my team went out and collected a large set of potential aggressors** to see if we were missing anything in our larger data collections, things would be normal to a regular user*." [76] Later that year, he posted again about the work Apple did on Face ID, saying that *"**tons of data was being collected** at the time to cover all the bases." [77]*

In 2017, Craig Federighi said Apple "***went to great lengths** to gather **its own data** on facial shapes and angles*."[78] Federighi said, Apple "***retains a high-fidelity depth map** of that [training] data"* and "*as Apple trains these models and iterate on these algorithms*," Apple "*wants **raw** sensor data to use and develop and optimize them*." [79] Federighi, said "*When it comes to customers, Apple gathers absolutely nothing itself via Face ID and that Apple does not gather customer data when you enroll in Face ID, it stays on your device, we do not send it to the cloud for training data*." [80] Federighi did not distinguish a customer in range of the hot & hungry camera of an Apple employee's iPhone with Gobbler installed.

Apple never responded directly to one of the Senator's questions, either to the U.S. Senate or to the press. The Senator asked, "*Apple has stated that it used more than one billion images in developing the Face ID algorithm. Where did these one billion face images come from?"*[81] **Apple would not answer**. What Federighi omitted is that those images came from employees just like me, whether I wanted to share them or not.

---

[75] TechCrunch, *Interview: Apple's Craig Federighi answers some burning questions about Face ID*, 2017, https://techcrunch.com/2017/09/15/interview-apples-craig-federighi-answers-some-burning-questions-about-face-id/
[76] LinkedIn, https://www.linkedin.com/pulse/design-experiment-data-collection-robert-mckeon-aloe/
[77] LinkedIn, https://www.linkedin.com/pulse/ml-examining-test-set-robert-mckeon-aloe/
[78] TechCrunch, *Interview: Apple's Craig Federighi answers some burning questions about Face ID*, 2017, https://techcrunch.com/2017/09/15/interview-apples-craig-federighi-answers-some-burning-questions-about-face-id/
[79] TechCrunch, *Interview: Apple's Craig Federighi answers some burning questions about Face ID*, 2017, https://techcrunch.com/2017/09/15/interview-apples-craig-federighi-answers-some-burning-questions-about-face-id/
[80] TechCrunch, *Interview: Apple's Craig Federighi answers some burning questions about Face ID*, 2017, https://techcrunch.com/2017/09/15/interview-apples-craig-federighi-answers-some-burning-questions-about-face-id/
[81] Letter from Senator Al Franken to Tim Cook about Face ID, (Sept 13 2017), https://web.archive.org/web/20170914201224/https://www.franken.senate.gov/files/letter/170913_AppleFaceID.pdf

The Gobbler User Study

I worked in Apple Research & Development. We were frequently pressured to "live on" one device for both work and personal use. Apple wanted to use our uncompensated labor to test new hardware and software using customer scenarios 24/7, at the expense of our privacy and work/life balance. This extended to my "live on" and testing of these devices, with my personal data and usage, being cited in my annual review. I even received emails noting what device I was 'living on' and nagging me to move to a future software build or prototype hardware model. We were also pressured to participate in very personal "user studies" using company devices.

On August 3 2017, an Apple engineering manager emailed an unknown list of Apple employees, including myself, about a "Gobbler" user study.[82] The manager wrote the study used an iOS application called "Gobbler," and told employees "*as you continue to use your device, use the Gobbler application to periodically upload data that has been logged."*[83] The manager then wrote, *"**In terms of data collection, we want more**. The algorithm uses deep learning and the more data the better."* He wrote that the Gobbler algorithms are "***hungry for data***" and that *"for uploading data: **all data that has your face in it is good data**."*[84] I did not respond to or act on the email; it was a weird email and by the way it was described, I wanted nothing to do with that tool/study, even if it meant I was being 'disloyal.'

Figure 1: One of the Twitter posts Apple claims they fired Gjovik over

On Aug 7 2021, I received a different email from a group account saying "*Come join us! We look forward to seeing*

[82] Email from R.M. in Apple Video Engineering, to "recipients not specified," Date: August 3 2017 7:45am PST, Subject: *Participating in [codename]Loop…*
[83] Email from R.M. in Apple Video Engineering, to "recipients not specified," Date: August 3 2017 7:45am PST, Subject: *Participating in [codename]Loop…*
[84] Email from R.M. in Apple Video Engineering, to "recipients not specified," Date: August 3 2017 7:45am PST, Subject: *Participating in [codename] Loop…*

you there!" [85] The email appeared to be a mandatory social event, though I was confused why the email said not to attend if I was *"taking photosensitizing medications or have any known photosensitizing medical conditions."* Regardless, I promptly accepted, assuming it was expected of me. (The message said nothing about Face ID.) I received another response later that day saying, *"Hello there! Thank you very much for responding to our invite! ..... You will receive an iCal invite to the event shortly… Please arrive at [Apple's Mathilda 3B office building] Patio at your scheduled time. Do not hesitate to reach out if you have any questions or concerns regarding the study. See you soon!*" [86]

It still sounded like some sort of mandatory social event, however the email also stated "*Prior to your participation, we kindly request that you do the following: Review the ICF [Informed Consent Form] and email sign the ICF by registering your email and completing the short pre-study survey that will be sent."* During my time at Apple, I was forced to sign hundreds of contracts to get access to everything from offices, conference rooms, documentation, and the basic to do my job, so I "signed" the ICF as requested. As far as I can tell, I never received a confirmation I signed it, nor did I get a copy of the ICF, and when I tried to access the ICF [87] again in 2021 the link went to website with an error message saying "connection insecure."

I showed up to the "Social Event" as requested. The "patio" was actually a parking lot. The temperature that day was very hot. As I approached the destination, if my memory serves me right, I saw a ~40ft diameter circular compound, with ~10ft high fence around it. There was a chain link fence, with black plastic lining it and then another chain link fence and more black plastic. On top, there were security cameras pointed inside and outside. There were one, maybe two, armed security guards standing outside the compound. One of the guards checked me in and told me to sit at a picnic table until called. I remember being hot, dehydrated, and scared. I wanted to leave, but didn't want to ask to leave, because then the armed guard might get upset or suspicious, so I waited. They finally let in 4 or 5 employees. They opened the first door of the gate, we went in, then they close the outer gate and open the inner gate – so no one on the outside could see in. I believe the gate was locked behind us.

---

[85] Email from SSP User Study Group to "recipients not specified," Date: August 7 2017 7:45am PST, Subject: *Social Hour Study: You're Invited!*

[86] Email from SSP User Study Group to "recipients not specified," Date: August 7 2017 6:55pm PST, Subject: *Social Hour Study: Registration*

[87] "Attache" link

Upon entering, there was music playing in the background & we were told to sit in the circle. The armed guard left and there were two Global Security guys remaining. One was at the make-shift bar & the other guy sat with the employees in a circle. I wanted to leave but I was locked in a compound with 10ft high gates, security cameras, and an armed guard, so I thought "*I'm too young to die*" and stayed put.

The guy in the circle explained what we're doing, we're going to enroll in Face ID and we're going to test it on iPhones with this Gobbler application and we must complete a set list of testing objectives before we are allowed to leave. The ICF had to be complete before we could set up the accounts, and he helped us set up the Gobbler accounts on the test phones. Then we had to try to enroll in Face ID and then complete our task list. It was like 12 tasks (put sunglasses on & take 10-20x pics, make a "silly" faces & take 10-20x pics, etc). He explained this testing set-up was specifically because they were having trouble with direct sunlight conditions, so even though they wanted to keep all testing in secure lockdowns, they set up this compound in the 100-degree sun so we could do real world testing for them.

I remember being miserable and desperately wanting to leave, so I did the testing as quickly as I could so I could go. When each of employee was done, I remember the guard unlocked the inner gate, then had the employee step in, closed the inner door, and opened the outer door and let them out. After that, the Gobbler application was always pre-installed and logged in on my iPhone, even if I changed phones. I kept attempting to log out and turn it off, but it would keep reopening and logging back in and collecting more videos/photos.

Figure 2: Photos captured by "Gobbler" in Gjovik's home bathroom, including Gjovik washing her face without clothing

Apple would later rename the application from Gobbler to "Glimmer" after criticism about the *facial "Gobbler*" name. On Apple's internal "Living On" help page, it explains that when you "live on" Apple devices, *"You are encouraged to make full use of your living on devices as you regularly would, and try to log as many bugs as possible. This will help us provide a better and bug free product to our*

customers. [88] The page also has a section on Gobbler/Glimmer, explaining *"Glimmer is an app that's included in internal development installs of Face ID equipped devices*." [89]

The page suggests uploading data from the app *"**captured in employee's homes.**"* [90] Apple's internal "Face ID FAQ" page said "*Users are encouraged to use Face ID in all places Touch ID is replaced on iPhone X….please use in a variety of conditions: From the bright outdoors to the **darkest rooms**. In workday, evening and **weekend attire**. With and without makeup*." [91] It said the Gobbler data "*can be previewed and included in radars and/or **donated** otherwise via the Gobbler to help make the feature better (there are many other things beside training the neural nets, that the data can be used for to improve the product)."* The page did not elaborate further.[92]

In the documentation pages, several restrictions were noted. One said*, "Data gathering **may be restricted in some countries**. You will be notified if that is the case.*"[93] Another said, *"Data privacy laws only allow us to gather and upload data from the US, Canada or Israel. Please **do not upload any data gathered outside of these countries**."*[94] Another said, "*To participate, please take the time to download the Informed Consent Form… and review it."* The Apple manager said the study was being conducted in "*the USA, Brazil, Tel Aviv,"* and the EU "*but not France or Germany*." [95] A page said, *"**some data should not be submitted from certain regions,"*** [96] while another page said, "*For now, Glimmer is only available for Apple employees working in the United States*." [97]

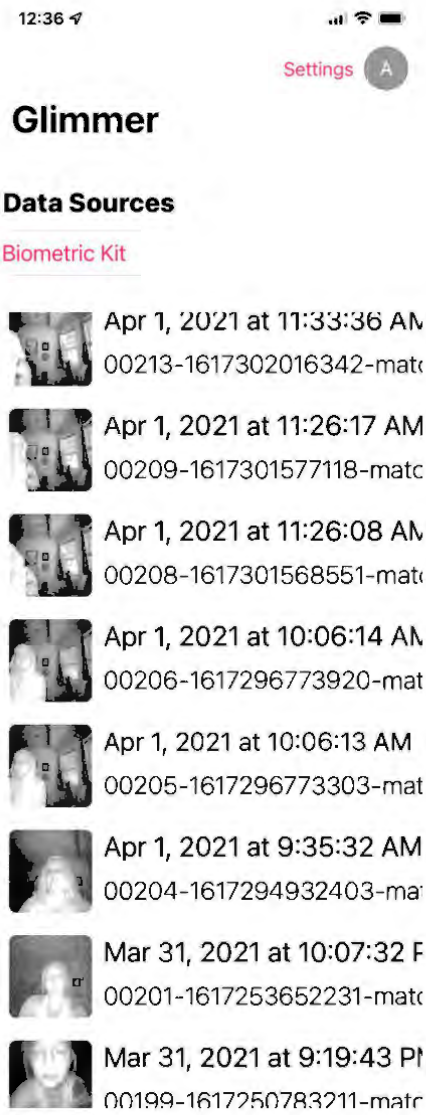
I also saw in notes that the app was forbidden to be used in Japan and China, but then at some point, Apple decided to gather some logs there anyways. On October 16, 2019 an engineer filed a Radar titled, "*Add Geo Location into Glimmer,"* saying

> *"*We're going to change how we deal with blacklisted countries. We're going to allow auto-A files to upload…. The aim is to better understand Japan and China because we have a number of people over there know...We're adding another

[88] Apple, *Living On*, Dev Pubs, Confluence page
[89] Apple, *Using Glimmer*, Confluence page
[90] Apple, *Using Glimmer*, Confluence page
[91] Apple, *Face ID FAQ*, Confluence page
[92] Apple, *Face ID FAQ*, Confluence page
[93] Standard Operating Procedure (SOP) for Glimmer usage
[94] Apple, Face ID FAQ, Confluence page
[95] Email from R.M. in Apple Video Engineering, to "recipients not specified," Date: August 3 2017 7:45am PST, Subject: *Participating in [codename] Loop…*
[96] Apple, *Living On*, Dev Pubs, Confluence page
[97] Apple, *Using Glimmer*, Confluence page

> field… specifying geo location is needed for distinguishing the location.... Once the ICF is updated, the geo location for all previous black-list countries as China and Japan can also collect autoAFile data."[98]

The engineer noted the changes were made as of Glimmer v3.25.0 on Dec 3, 2019.[99]



It was extraordinarily unclear what data was being automatically uploaded, how and when. I saw another employee complaining in 2019, "*why is Glimmer always running*?"[100] The engineer responded, *"Glimmer is launched every day at 2 am to collect non-PI logs from FaceD, zip them, and upload them to a server for machine learning algorithms and data analysis tools to be computed. This allows to monitor non-regression and algorithm updates impacts.*" [101]

Another employee asked in 2019, "*Why is Glimmer launching automatically*?" He wrote, "*I noticed on my device there's some kind of launch job started by root to launch Glimmer as suspended all the time. Why is this happening? What is it for?*" The engineer responded, "*Glimmer is launched to upload some non PI (logs) data automatically.*" [102]

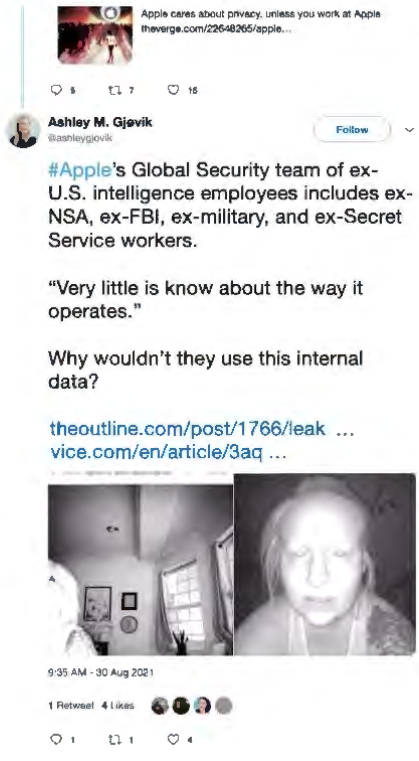
My open questions included whether my personal data was being backed up on employee iCloud backups, synced via iCloud, and/or accessed/copied by Apple's corporate MDM profiles – or other Global Security surveillance of employee phones. It also disturbed me that the app was taking photos/videos without any notification (sound, signal, etc), which made me think that Apple, if it wanted to, could activate my device cameras and watch me without me knowing at any time as well. I talked to other employees, including managers, with similar concerns.

[98] Radar filed on October 16, 2019 at at 4:35 PM, Title: *Add Geo Location into Glimmer*
[99] Radar filed on October 16, 2019 at at 4:35 PM, Title: *Add Geo Location into Glimmer*
[100] Radar filed on December 13, 2019 at 6:08 PM, Title: *Why is Glimmer always running?*
[101] Radar filed on December 13, 2019 at 6:08 PM, Title: *Why is Glimmer always running?*
[102] Radar filed on September 25, 2019 at 1:53 PM, Title: *Why is Glimmer launching automatically?*

I partnered with a journalist to expose my concerns and the article was published on August 30, 2021 – while I was still employed by Apple, but while I had been forced on paid administrative leave. The article was titled, "***Apple Cares About Privacy, Unless You Work at Apple.*"** [103] The article discussed the Gobbler app and that "*images are recorded every time employees open their phones*" and "*every time an employee picked up their phone, the device recorded a short video — hopefully of their face*." The article quoted the internal email saying "*all data that has your face in it is good data,"* and also quoted me saying ***"If they did this to a customer, people would lose their goddamn minds,*** *says Ashley Gjøvik, a senior engineering program manager."* [104] The article noted that two employees confirmed that participation in studies like Gobbler was not just "*encouraged*" but "*even expected*." The article also noted employees had **no idea "*what was happening with the hundreds of images*** " taken by their phones. [105]

[103] Zoe Schiffer, *Apple Cares About Privacy, Unless You Work at Apple*, The Verge (Aug 30 2021), https://www.theverge.com/22648265/apple-employee-privacy-icloud-id
[104] Zoe Schiffer, *Apple Cares About Privacy, Unless You Work at Apple*, The Verge (Aug 30 2021), https://www.theverge.com/22648265/apple-employee-privacy-icloud-id
[105] Zoe Schiffer, *Apple Cares About Privacy, Unless You Work at Apple*, The Verge (Aug 30 2021), https://www.theverge.com/22648265/apple-employee-privacy-icloud-id

106



107 108

^ *The Twitter Posts Apple's Lawyer's Demanded that I Delete on Sept 15 2021* ^

Twitter Post: August 30 2021 [109]

[106] https://twitter.com/ashleygjovik/status/1432381395955900416
https://web.archive.org/web/20210830170534/https://twitter.com/ashleygjovik/status/1432381395955900416
[107] https://twitter.com/ashleygjovik/status/1432381497370034184
https://web.archive.org/web/20210830170723/https://twitter.com/ashleygjovik/status/1432381497370034184
[108] https://twitter.com/ashleygjovik/status/1432400136471072769
https://web.archive.org/web/20210830182052/https://twitter.com/ashleygjovik/status/1432400136471072769
[109] Twitter, https://twitter.com/ashleygjovik/status/1432416891201490944

ASHLEY M. GJØVIK
@ashleygjovik

I still love #Apple products & brand. I devoted nearly 7 years & much blood/sweat/tears ensuring Apple's products are exceptional. However, Apple the corporation needs a reckoning. Apple's policy of "secrecy" should not shield it from public scrutiny about human rights & dignity.

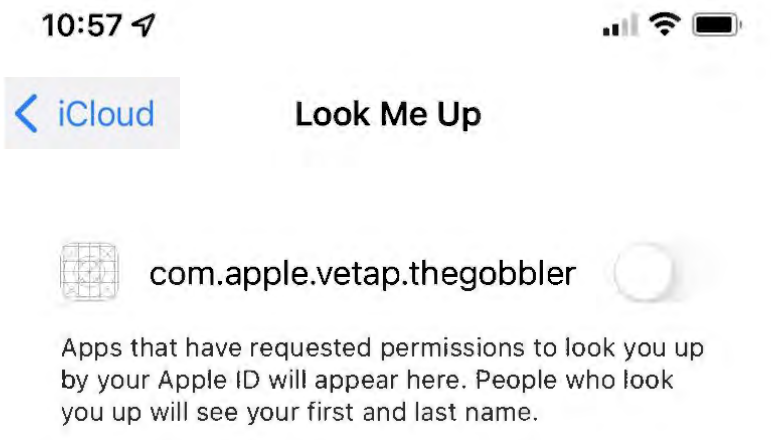
Working at Apple in "normal" times, I walked in circles around their glass-walled panopticon, only able to badge into select lockdowns (a constant reminder that Apple has absolute control over my resources and access), and was immersed in a culture where it is implicitly forbidden to critique Apple policies or even speak openly to your coworkers with concerns about your employment & work conditions, lest you upset the cronyism, ex-CIA/ex-FBI security teams, and other "powers that be." I realize now that during those times, I didn't question a lot of things that I should have. Not just the abuse I suffered, but also the constant invasion of privacy — and perhaps those two things are linked.

There seems to be limitless ways Apple can access employee data and monitor us. I recently shared how violating it felt for Apple to demand to copy & permanently store my nudes for completely unrelated litigation. After the public outcry, I questioned other policies & actions Apple had taken. The internal "Glimmer" app had always troubled me, but I never voiced that concern, because inside we don't question the way things are or what we're asked to do. But now, in the light of day, considering everything Apple's already done to me, this app, the photos & data it gathers, and how little we know about what it does with all of that — is deeply troubling and I felt compelled to make it public. Apple's policy of "secrecy" should not shield it from public scrutiny about human rights & dignity.

11:56 AM · Aug 30, 2021 · Twitter Web App

Responses to my disclosures included, but were not limited to:

- "This is creepy. I don't have words to express what is running through my head. "[110]
- "Straight up abusive and creepy behavior how can deployed iOS devices even run stuff like this?"[111]
- "Whatttt" [112] & "What the hell…."[113] & "Excuse me WHAT"[114]
- "Ah, but does the employee handbook say workers are human?" [115]
- "I've heard a manager say we don't have civil rights as employees" [116]
- "if anyone talks about apple privacy. show them this" [117]
- "No, just no." [118]
- This entire article is.. wow. [119]
- Because privacy is a fundamental human right* * that you need to give up to work for the company that cares so much about privacy. [120]
- [inserte su referencia a 1984 aquí] [121]
- This is terrible and so bothersome on many levels. [122]
- Quel enfer... [123]



The "Gobbler" applications attempted to access my fully personal iPhone, even after I was fired.

[110] https://web.archive.org/web/20210830182052/https:/twitter.com/ashleygjovik/status/1432400136471072769
[111] https://web.archive.org/web/20210830182052/https:/twitter.com/ashleygjovik/status/1432400136471072769
[112] https://web.archive.org/web/20210830182052/https:/twitter.com/ashleygjovik/status/1432400136471072769
[113] https://web.archive.org/web/20210830182052/https:/twitter.com/ashleygjovik/status/1432400136471072769
[114] https://web.archive.org/web/20210830182052/https:/twitter.com/ashleygjovik/status/1432400136471072769
[115] https://twitter.com/ashleygjovik/status/1432381235926499332
[116] https://twitter.com/ashleygjovik/status/1432381235926499332
[117] https://twitter.com/verge/status/1432381006670147587
[118] https://twitter.com/verge/status/1432381006670147587/retweets/with_comments
[119] https://twitter.com/verge/status/1432381006670147587/retweets/with_comments
[120] https://twitter.com/verge/status/1432381006670147587/retweets/with_comments
[121] https://twitter.com/verge/status/1432381006670147587/retweets/with_comments
[122] https://twitter.com/verge/status/1432381006670147587/retweets/with_comments
[123] https://twitter.com/verge/status/1432381006670147587/retweets/with_comments

In 2010, the Electronic Frontiers Foundation wrote an article about Apple seeking a patent to do just the kind of thing the "Gobbler" application does today. EFF called the technology "*spyware*," "*traitorware*," and "*especially creepy*."[124] EFF warned the patent provided "a roadmap for how Apple can — and presumably will — spy on its customers and control the way its customers use Apple products." [125] The technology would allow Apple to record the voice of the device's user, take a photo of the device's user's current location or *even detect and record the heartbeat of the device's user*. [126]

EFF called the technology "*dangerous*" and warned, "*this patented device enables Apple to secretly collect, store and potentially use sensitive biometric information about the user*." The patented technology can: "*take a picture of the user's face without a flash, any noise, or any indication that a picture is being taken to prevent the current user from knowing he is being photographed" and "can take a photograph of the surrounding location to determine where it is being used*." [127] EFF warned, "*Apple will know who you are, where you are, and what you are doing and saying and even how fast your heart is beating*." [128]

"*Apple does not explain what it will do with all of this collected information on its users, how long it will maintain this information, how it will use this information, or if it will share this information with other third parties*." [129] EFF urged, "*This patent is downright creepy and invasive…. Spyware, and its new cousin traitorware, will hurt customers and companies alike — Apple should shelve this idea before it backfires on both it and its customers*." [130]

In 2010, *Inc* also wrote about Apple's "*spyware*" patent,[131] calling it "*creepy*" and "*Orwellian*." The reporter said concerns may vary based on how much users trusted Apple and how intimate their "relationship is with a faceless mega-corporation." The writer queried readers, "*Are you comfortable enough with Apple that it's okay for them to have the power to turn on your iPhone camera, snap a picture of whatever is in plain site of the lense and then upload it to Apple for analysis?"* And if you respond that yes you think that's fine, then what if *"... it's all a big misunderstanding and the camera takes a picture for the Apple mothership while you are in*

[124] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[125] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[126] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[127] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[128] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[129] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[130] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[131] Patent: Systems and methods for identifying unauthorized users of an electronic device (10657238)

the middle of sexy time?" [132] "Apple filed another patent in 2011 for iPhone remote surveillance capabilities, such as transmission of the images and sounds that the device secretly captures." [133]

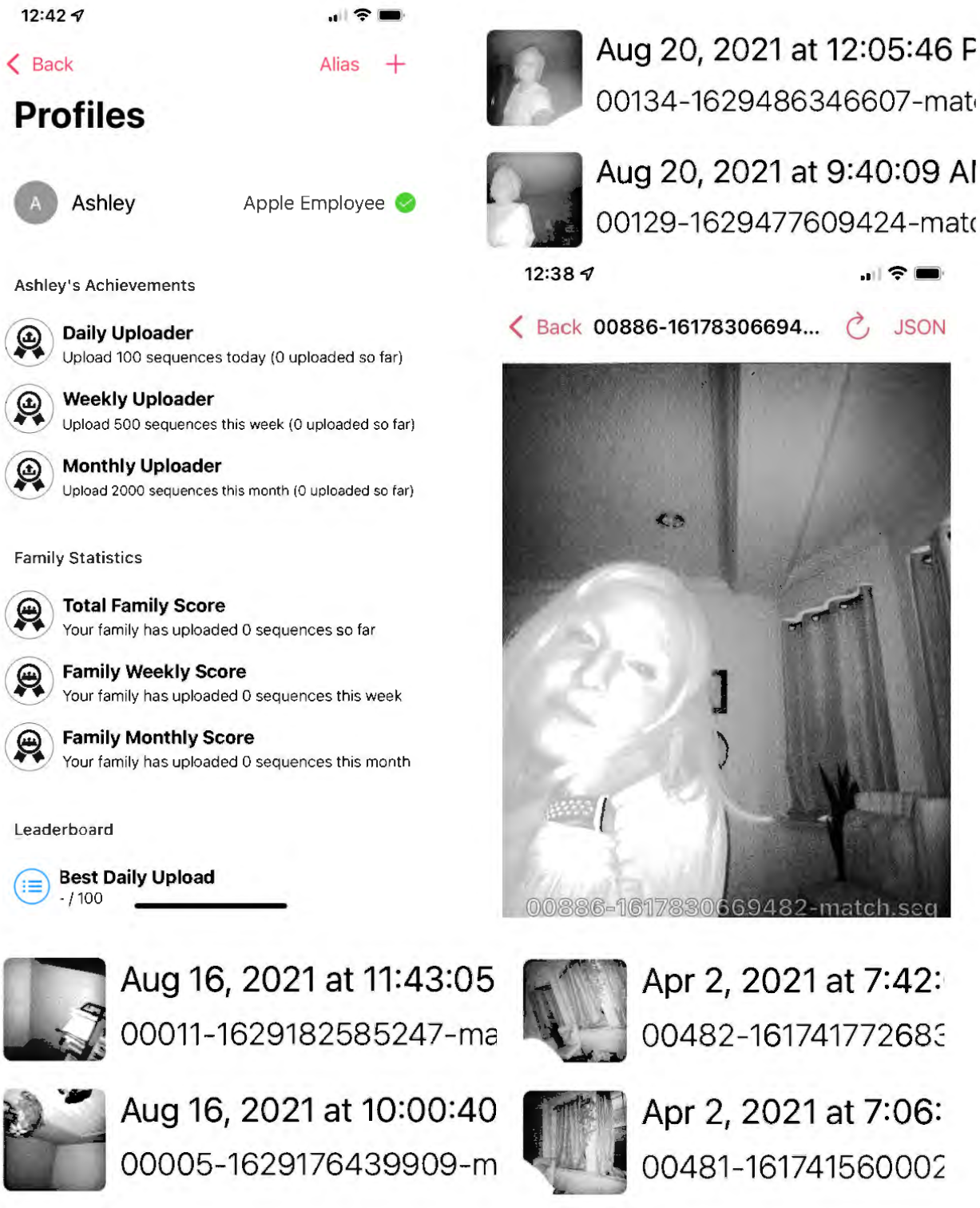
Courts have acknowledged the intrusive effect of hidden cameras and video recorders in settings that otherwise seem private. It has been said that the "*unblinking lens*" can be more penetrating than the naked eye with respect to "*duration, proximity, focus, and vantage point.*"[134]

On March 4 2022 Apple (via Orrick lawyers) wrote to the U.S. federal government that:

> "Apple terminate Ms. Gjovik's employment … because she violated Apple policy by intentionally disclosing confidential information about Apple products on Twitter and, as Apple later discovered, to the press … On August 30, 2021, Ms. Gjovik tweeted photographs and a video of herself created by the [Gobbler] application, thus disclosing Apple confidential information. She also linked to a story published in The Verge, a technology blog, in which she disclosed her participation in the [Gobbler user] study. As discussed above, Ms. Gjovik's very involvement with the [Gobbler user] study constitutes confidential information, as do any details about the study or photos or other documents that are the product of it. Apple's subsequent confirmation that she admitted to disclosing confidential information publicly and intentionally further justifies Apple's termination decision."[135]

[132] Renee Oricchio, *Orwellian Watch: Apple's Creepy Patent Application*, Inc., https://www.inc.com/tech-blog/orwellian-watch-apples-creepy-patent-application.html
[133] 9to5 Staff, *Patent indicates sophisticated remote surveillance for Find My iPhone*, (Jun. 16th 2011), https://9to5mac.com/2011/06/16/patent-indicates-sophisticated-remote-surveillance-for-find-my-iphone/
[134] *Cowles v. State* (Alaska 2001) 23 P.3d 1168, 1182 (dis. opn. of Fabe, J.)
[135] Letter from Apple Inc (via Orrick, Herrington & Sutcliffe LLP) to U.S. Department of Labor, March 4 2022, Re: *Ashley Gjovik v. Apple Inc.*, Case No. 9-3290-22-051

Apple's Face "Gobbler"

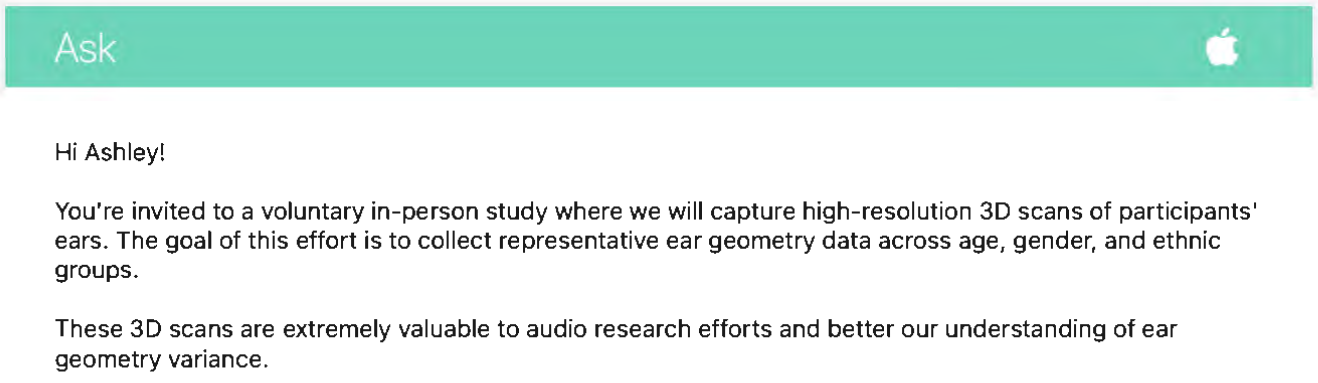


EAR STUDIES

On Aug 10 2018, I was invited to a "HE User Study" for "anthropometry HH" sent by two Apple employees who previous asked for photos of my ears, and had discussed wanting to take scan my ears. I replied declining "***indefinitely***. "[136] I assumed I'd be taken off the list for ear studies, but then in 2021, while I was on Indefinite Administrative Leave in August, I received three separate emails from Apple asking to scan my ears/ear canals, again. The email was titled, "*HE 3D Ear Scan Invitation!*"

The emails said, "*You're invited to a voluntary in-person study where we will capture high-resolution 3D scans of participants' ears. The goal of this effort is to collect representative ear geometry data across age, gender, and ethnic groups. These 3D scans are extremely valuable to audio research efforts and better our understanding of ear geometry variance."* The email said I'd be asked to review an ICF prior to taking a recruitment survey and then another ICF for study participation. [137] I did not respond to any of the emails nor did I sign any ICFs.

I was disturbed by Apple's lack of respect for the privacy of its employees. I also wondered if Apple may have been emailing me these on purpose, since I already opted out, in order to harass me further. The emails didn't say "*Apple Confidential*," nor did they include anything that appeared actually secret or material. Regardless, I redacted them heavily when I publicly complained about the matter, since my point was to protest an employer pressuring its employees to gather such sensitive information (biometrics).


Ask

Hi Ashley!

You're invited to a voluntary in-person study where we will capture high-resolution 3D scans of participants' ears. The goal of this effort is to collect representative ear geometry data across age, gender, and ethnic groups.

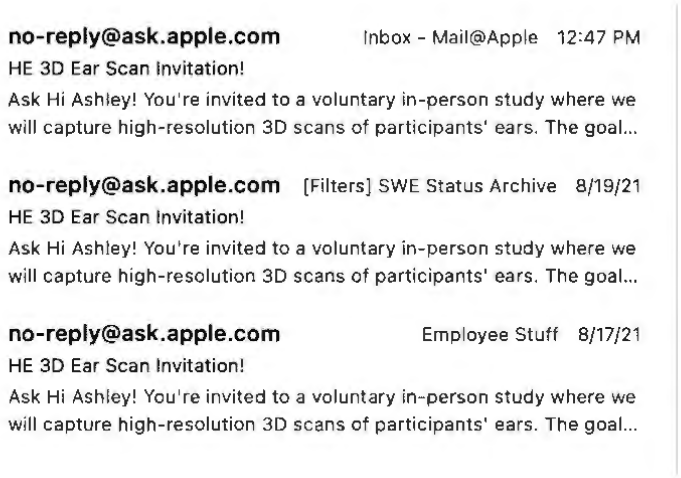
These 3D scans are extremely valuable to audio research efforts and better our understanding of ear geometry variance.

[136] Aug 10 2018, Gjovik to SJ
[137] Ask survey

The Tweet Gjovik was fired over:

"I'm still over here in Apple's time-out chair & they keep telling me to respect my abuser's privacy & be silent. Meanwhile I got 3x of these in the last month since being on leave. NO, APPLE, STOP IT. I can't tell if they're harassing me or just being super intrusive or both."[138]

[138] *Aug 28 Twitter Post:* https://twitter.com/ashleygjovik/status/1431824501457633283 https://web.archive.org/web/20210829034222/https://twitter.com/ashleygjovik/status/1431824501457633283



Further, this wasn't news. On September 5 2020, Apple VP of Marketing , Greg Joswiak ("Joz") was interviewed by Wired about Apple AirPods.[139] Joz said,*"We did work with Stanford to **3D-scan hundreds of different ears** and ear styles and shapes in order to make a design that would work as a one-size solution across a broad set of the population,"* Joswiak says. "*With AirPods Pro, we took that research further – **studied more ears, more ear types.** And that enabled us to develop a design that, along with the three different tip sizes, works across an overwhelming percentage of the worldwide population."*

On December 9 2021, two Apple Product Design executives were interviewed by Wallpaper about Apple's product design team. [140] The article said, "*When AirPods' development began a decade or so ago, human factors researcher Kristi Bauerly found herself researching the 'crazily complex' human ear. '**We moulded and scanned ears**, worked with nearby academics, focusing on outer ears for the earbud design and inner ears for the acoustics,' she says. **Thousands of ears were scanned,** and only by bringing them all together did the company find the 'design space' to work within. '**I think we've assembled one of the largest ear libraries anywhere,'** Hankey says. 'The database is where the design starts,' Bauerly continues, 'and then we iterate and reiterate*.' " On July 28 2021, Apple was referred to as *"[an] ear-canal innovator*."[141]

In 2020, Apple's patent filings describe a system for deriving biometrics using embedded biometric sensors on the AirPods (Earbuds). [142] The patent captures waveforms associated with the cycling profusion of blood to the skin, so multiple biometric parameters can be collected,

[139] The secrets behind the runaway success of Apple's AirPods: The wireless headphones have been a surprise hit. Here's how: Sept 5 2020, https://www.wired.co.uk/article/apple-airpods-success
[140] Inside Apple Park: first look at the design team shaping the future of tech, Dec 9 2021, https://www.wallpaper.com/design/apple-park-behind-the-scenes-design-team-interview
[141] Can you ID me now? Apple les for ear- canal biometrics patent, Jan 28, 2022,, https://www.biometricupdate.com/202201/can-you-id-me-now-apple-files-for-ear-canal-biometrics-patent
[142] Patent number 10856068; Apple's future AirPods/earbuds could facilitate biometric measurements, Niel Smith, December 30, 2020 https://www.myhealthyapple.com/apples-future-airpods-earbuds-could-facilitate-biometric-measurements/

including, for example, heart rate, blood volume, and respiratory rate.[143] Ears have been flagged as the future of biometric-based mass surveillance. [144] [145]

On March 4 2022 Apple (via Orrick lawyers) wrote to the U.S. federal government that:

> "On August 28, 2021, Ms. Gjovik tweeted details about a proprietary study Apple was conducting…. . Like the [Gobbler] study, the details of [this ear scanning study] were not known except to a small select group within Apple, and certainly not outside Apple, and Ms. Gjovik agreed to keep them confidential under her Confidentiality Agreement. Despite this, Ms. Gjovik's tweet both identified the name and purpose of the study regarding an unreleased product under development….. Apple terminated Ms. Gjovik's employment because she chose to disclose confidential Apple product information she was under an obligation to keep in confidence… The ***only*** reason that Apple terminated Ms. Gjovik's employment was due to her own deliberate breaches of her confidentiality agreements and violations of Apple policy."[146]

While we still believe these reasons are pretext for Apple's retaliation against me for reporting safety issues, discrimination, labor violations, and fraud – if Apple really thinks I violated their policies in protesting these invasive technologies, then their policies are wrong.

OTHER USER STUDIES

Despite Apple's censoring of employee concerns about user studies, Apple is quite public about its user studies. Just searching LinkedIn for "Apple User Study," numerous people/positions are returned with detailed descriptions of the roles and projects. In these descriptions, Apple talked about *"**small, focused research studies**" and **"large-scale worldwide [user study] operations**."* [147] Positions talked about user studies and data collection for "***sensor and health technology,"*** [148] ***"biometric data"*** [149] and for *"**product comfort.**"* [150] Positions

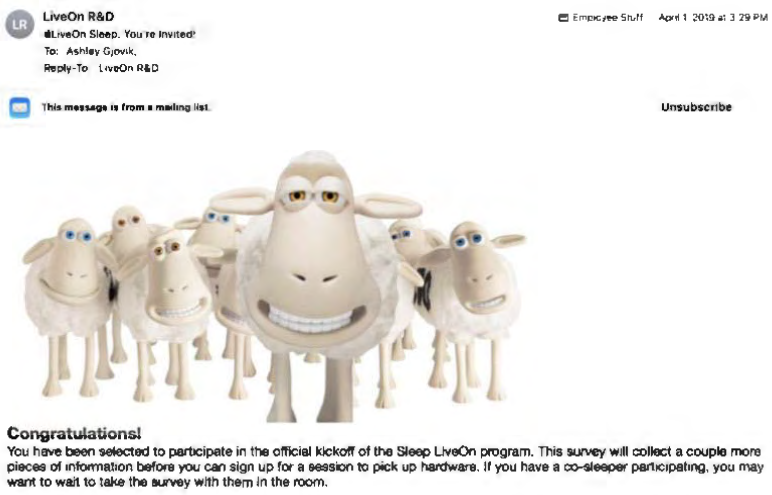
[143] Patent number 10856068
[144] Ahila Priyadharshini, R., Arivazhagan, S. & Arun, M. A deep learning approach for person identification using ear biometrics. *Appl Intell* **51,** 2161–2172 (2021). https://doi.org/10.1007/s10489-020-01995-8
[145] 3D Ear Biometrics BIR BHANU, HUI CHEN, Center for Research in Intelligent Systems, University of California, Riverside, CA, USA , Springer
[146] Letter from Apple Inc (via Orrick, Herrington & Sutcliffe LLP) to U.S. Department of Labor, March 4 2022, Re: *Ashley Gjovik v. Apple Inc.*, Case No. 9-3290-22-051
[147] https://www.linkedin.com/jobs/view/2942922643; https://www.linkedin.com/jobs/view/2944339533
[148] https://www.linkedin.com/jobs/view/2942922643; https://www.linkedin.com/jobs/view/2944339533
[149] https://www.linkedin.com/jobs/view/2944349447
[150] https://www.linkedin.com/jobs/view/2944349447

included responsibilities such as to "***identify and recruit user study participants.***"[151] and *"**observe behavior"** and **"administer complex testing protocols."*** [152]

During my time at Apple, I was invited to employee user studies looking to study me on topics ranging from my "eye movements," "grip on an iPhone," "voice", "blood pressure," physical response to "yoga, swimming, and running," to studying my "menstruation" and "sleep." Indeed, in April 2019 I was invited to a user study program to study my sleep.[153]

> "Congratulations! You have been selected to participate in the official kickoff of the Sleep LiveOn program. This survey will collect a couple more pieces of information before you can sign up for a session to pick up hardware. If you have a **co-sleeper** participating, you may want to wait to take the survey with them in the room." [154]

Going forward, I would then be surveyed via email about my "insomnia severity index" and other medical information while a Beddit monitor[155] was required to be placed under me as I slept, monitoring my heart rate, respiratory rate, and other data.[156]



The request for **co-sleeper** information also extended to requesting co-sleepers sign NDAs, and even participate in the study themselves – even if they are not an employee. Personally, I didn't want my employer to know who I was sleeping with and I stopped participating in that study.

---

[151] https://www.linkedin.com/jobs/view/2938135938
[152] https://www.linkedin.com/jobs/view/2944353441
[153] Email from LiveOn R&D to Ashley Gjovik, April 1 2019, Subj: *LiveOn Sleep: You're Invited!*
[154] Email from LiveOn R&D to Ashley Gjovik, April 1 2019, Subj: *LiveOn Sleep: You're Invited!*
[155] iMore, *Apple cans the Beddit Sleep Monitor 5 years after buying the business*, https://www.imore.com/apple-cans-beddit-sleep-monitor-5-years-after-buying-business
[156] Email from LiveOn R&D to Ashley Gjovik, April 16 2019, Subj: *LiveOn Sleep: Insomnia Severity Index Survey*

RADAR & SYSDIAGNOSE

When Apple employees file "Radar" tickets to track software development work and "bugs," they include detailed information about the problems they are seeing. The default sharing settings for most Radar ticket included all of software engineering. Radar tickets also are not removable. Even when the tickets are closed, they remain searchable. In training, employees say they are told: "*Radar is forever*." [157]

When employees file Radar tickets, they are often asked to include diagnostic files, internally called "sysdiagnose" to give Apple more information about the problem. If they are filing a bug about iMessage, they might be asked to install a sysdiagnose profile that exposes their iMessages to the team tasked with fixing the issue. For employees using a live-on device, default settings can mean that, as they are filing a Radar ticket, a sysdiagnose profile is being automatically created in the background, sending data to Apple without the employee realizing it. When sysdiagnose profiles are not included, employees have been known to post memes calling out the omission. [158]

I told The Verge journalist that in 2019, I filed a ticket about Apple's photo search capabilities. I was quoted as writing, "*If I search for 'infant' in my photo library, it returns a selfie I took of myself in bed after laparoscopic surgery to treat my endometriosis*." [159] This Radar, and many of the Radars I submitted with detailed logging and personal details were visible to tens of thousands of people.

Whether it is the text content of the Radar, or the logs attached, if a coworker wanted to learn intimate details about your life, they could by simply searching through the Radars you've filed. Reviewing logs quickly exposes locations, routines, friends, and other highly personal data. Assumably far more data would be made available to the Worldwide Loyalty Team.

---

[157] Zoe Schiffer, *"Apple Cares About Privacy, Unless You Work at Apple,"* The Verge, Aug 30, 2021, https://www.theverge.com/22648265/apple-employee-privacy-icloud-id
[158] Zoe Schiffer, *"Apple Cares About Privacy, Unless You Work at Apple,"* The Verge, Aug 30, 2021, https://www.theverge.com/22648265/apple-employee-privacy-icloud-id
[159] Zoe Schiffer, *"Apple Cares About Privacy, Unless You Work at Apple,"* The Verge, Aug 30, 2021, https://www.theverge.com/22648265/apple-employee-privacy-icloud-id

Secrecy

SECRECY POLICIES

The New York Times wrote in 2009 that, "*Few companies are more secretive than Apple, or **as punitive to those who dare violate the company's rules** on keeping tight control over information. Secrecy at Apple … is baked into the corporate culture."* [160] Anil Dash (EFF board member and advisor to the Obama administration) wrote that Apple *"chooses to operate with an **extreme and excessive layer of secrecy**, even when making reasonable business decisions."* [161] Dash wrote, *"the cost of Apple keeping secrets has become morally and ethically untenable"* and that "*Apple spends an enormous amount of money on protecting and obfuscating normal business operations that any other company can do in the open."*[162]

A 2017 internal training video included a quote from VP of Marketing, Greg Joswiak, telling employees that "*I have faith deep in my soul that if we hire smart people they're gonna think about this, they're gonna understand this, and ultimately they're gonna do the right thing, and **that's to keep their mouth shut**."* [163]

Apple's "New Product Security (Secrecy)" team is part of the larger Global Security team. Before joining Apple, the Global Security team manager, David Rice,[164] worked at the NSA as a Global Network Vulnerability Analyst for four years, and before that was a Special Duty Cryptologist in the U.S. Navy. [165] Before joining Apple, other Apple Global Security managers have worked in US Coast Guard port security,[166] local Police Chiefs,[167] as U.S. Secret

[160] Brad Stone and Ashlee Vance, *Apple's Obsession With Secrecy Grows Stronger,* New York Times (Jun 2009), https://www.nytimes.com/2009/06/23/technology/23apple.html
[161] Anil Dash, *Apple: Secrecy Does Not Scale*, Jul 31, 2009, dashes.com/2009/07/31/apple_secrecy_does_not_scale/
[162] Anil Dash, *Apple: Secrecy Does Not Scale*, Jul 31, 2009, dashes.com/2009/07/31/apple_secrecy_does_not_scale/
[163] William Turton, *Leaked recording: Inside Apple's global war on leakers: Former NSA agents, secrecy members on product teams, and a screening apparatus bigger than the TSA.*, The Outline (2017), theoutline.com/post/1766/leaked-recording-inside-apple-s-global-war-on-leakers
[164] David Rice, https://www.linkedin.com/in/david-rice-7b3686/
[165] William Turton, *Leaked recording: Inside Apple's global war on leakers: Former NSA agents, secrecy members on product teams, and a screening apparatus bigger than the TSA.*, The Outline (2017), theoutline.com/post/1766/leaked-recording-inside-apple-s-global-war-on-leakers
[166] Sean Downey, https://www.linkedin.com/in/sean-downey-64a942119/
[167] Greg Finch, https://www.linkedin.com/in/greg-finch-74a3228/

Service Special Agents,[168] U.S. Department of State Special Agents & Executive Protection managers for weapons manufacturers,[169] etc.

In 2017, Rice complained that "*U.S. employees have griped about [Apple's] draconian security measures*." [170] With McCarthyism-flavored PSYOPs, Apple tells its employees that "leakers" at Apple "*look like [regular employees],"* and that "*they come to work, they don't appear any different, and they start off with the exact same motivation about 'I love Apple, I think this is a cool place to work, I wanna make it better*." [171]

I had grown deeply disturbed by the horrific lack of privacy for Apple corporate employees and was happy to expose to the issue to the public, as the anti-privacy policy for employees was a "feature" not a "bug" to Apple, and thus there was no internal complaint process on the matter, and even if there was, it seemed like a certain way to face additional retaliation. I posted on Twitter on August 30-31 2021 about The Verge article and complaining about Apple's work conditions saying:

- "Apple has an internal culture of **surveillance**, **intimidation**, & alienation. Employees are closely monitored & our data hoarded in the name of secrecy & quality. We're told we have no expectation of privacy, while Apple says publicly: **privacy is a human right**."[172]
- "Apple probably considers what they're doing to employees "**internal information**." Why? For secrecy? For quality? Or because Apple knows **the public would be outraged**, & that outrage might start to "deprogram" their employees? " [173]
- Cult: "great devotion to a person, idea, object, movement, or work." Information control: "**encourage spying on other members**" Behavior control: "instill obedience"[174]
- "I still love Apple products & brand. I devoted nearly 7 years & much blood/sweat/tears ensuring Apple's products are exceptional. However, Apple the corporation needs a reckoning. **Apple's policy of "secrecy" should not shield it from public scrutiny about human rights & dignity."**
- "We're learning about Apple's long history of systemic oppression & **retaliation** against employees when employees express concerns about discrimination, harassment, & other

[168] Michael Rovins, https://www.linkedin.com/in/michael-rovins-84880626/; Jeff Hill: https://www.linkedin.com/in/sajah/
[169] Scott Nishi, https://www.linkedin.com/in/scott-nishi-963591109/
[170] William Turton, *Leaked recording: Inside Apple's global war on leakers: Former NSA agents, secrecy members on product teams, and a screening apparatus bigger than the TSA.*, The Outline (2017), theoutline.com/post/1766/leaked-recording-inside-apple-s-global-war-on-leakers
[171] William Turton, *Leaked recording: Inside Apple's global war on leakers: Former NSA agents, secrecy members on product teams, and a screening apparatus bigger than the TSA.*, The Outline (2017), theoutline.com/post/1766/leaked-recording-inside-apple-s-global-war-on-leakers
[172] https://twitter.com/ashleygjovik/status/1432381777658613762; https://twitter.com/ashleygjovik/status/1432381235926499332
[173] https://twitter.com/ashleygjovik/status/1432383062273191937
[174] https://twitter.com/ashleygjovik/status/1432382993046200323

> abuse. Why wouldn't Apple try to use our data & their internal **surveillance** infrastructure against us?"[175]

Thomas le Bonniec, an ex-Apple contractor and whistleblower, wrote to regulators in 2019: "*It is worrying that Apple keeps ignoring and violating fundamental rights and continues their massive collection of data. "I am extremely concerned that big tech companies are basically wiretapping entire populations despite European citizens being told the EU has one of the strongest data protection laws in the world. Passing a law is not good enough: it needs to be enforced upon privacy offenders.*"[176] Le Bonniec, said Apple has been, "*operating on a moral and legal grey area and they have been doing this for years on a massive scale. They should be called out in every possible way*."[177]

Le Bonniec exposed that Siri is recording when it is not triggered by the users. Thousands of recordings were sent to Apple in order for hundreds of Apple employees to listen, analyse and transcribe their content. The public statement reveals that Apple collected millions of confidential messages, full of intimate details, political opinions, sexual preferences, and discussions between persons in a room, without the users even being aware of it. In 2019, Apple admitted that these practices were not up to the privacy standards. According recent disclosures it seems that contrary to Apple's statement, no end was put to the recording of Apple's users.[178]

In January 2023, the NLRB found merit in my charge that Apple's NDAs do violate federal labor laws.[179] There are still no decisions on my or Le Bonniec's surveillance charges.

SEARCH AND PRIVACY POLICIES

In September of 2021, a journalist wrote about my experience realizing just how intensively Apple could and likely was surveilling me. She wrote,

---

[175] https://twitter.com/ashleygjovik/status/1432381802602110976
[176] The Guardian, *Apple whistleblower goes public over lack of action,* May 2020,, https://www.theguardian.com/technology/2020/may/20/apple-whistleblower-goes-public-over-lack-of-action
[177] he Guardian, *Apple whistleblower goes public over lack of action,* May 2020,, https://www.theguardian.com/technology/2020/may/20/apple-whistleblower-goes-public-over-lack-of-action
[178] Noyb, "*Siri: Are you recording me?" "No but I am listening to you*," May 2020, https://noyb.eu/en/former-apple-employee-blows-whistle-apple-again
[179] TechCrunch, *Labor officials found that Apple execs infringed on workers' rights,* https://techcrunch.com/2023/01/30/labor-officials-found-that-apple-execs-infringed-on-workers-rights/

> "Last weekend, Ashley Gjøvik walked around her apartment unplugging all of her electronics. Apple had just fired her for allegedly leaking information, and for months before then, she had spoken out with claims of harassment, intimidation and surveillance at the company. She'd been thinking through Apple's employee privacy policy, which states that workers have no expectation of privacy when using a personal device for Apple business, and wondered if that meant the company could watch her through her home devices, too."

I was quoted saying, "*I think the worst moment was realizing that they were probably watching me through my Eve cameras and listening to me on my HomePod, It was this frantic moment. I don't even have words for it yet, of how violating and horrifying and terrifying it was."* [180] I told the journalist it "wasn't until I began speaking out about the company that I started to realize [Apple's surveillance] could be used against me." [181]

In 2019, a former Apple executive also had a rude awakening and alleged that Apple reviewed his private text messages.[182] He wrote, "*To further intimidate any current Apple employee who might dare consider leaving Apple, Apple's complaint shows that it is monitoring and examining its employees' phone records and text messages, in a stunning and disquieting invasion of privacy."*[183]

In 2021, I filed complaints with the U.S. NLRB and the California Dept of Labor over Apple's unlawful employee policies, including their "*Workplace and Searches Privacy*."[184]

> "In order to protect Apple confidential and sensitive[185] information and maintain the security and integrity of our networks and equipment, any use of Apple property, as well as use of your personal devices for Apple business or for accessing Apple networks, is subject to this policy."

---

[180] Sarah Roach, *Worker surveillance is making employees miserable*, Protocol, Sept 2021, https://www.protocol.com/workplace/worker-surveillance-is-making-employees-miserable

[181] Sarah Roach, *Worker surveillance is making employees miserable*, Protocol, Sept 2021, https://www.protocol.com/workplace/worker-surveillance-is-making-employees-miserable

[182] Mark Gurman and Edvard Pettersson, *Ex-Apple Executive Accused of Betrayal Says He Was Snooped On*, Bloomberg (December 9, 2019), https://www.bloomberg.com/news/articles/2019-12-10/ex-apple-executive-accused-of-betrayal-says-he-was-snooped-on

[183] CNBC, *Apple accused of monitoring employee text messages in lawsuit against ex-chip exec*, Dec 2019, https://www.cnbc.com/2019/12/10/apple-accused-of-monitoring-employee-text-messages-in-lawsuit-against-ex-chip-exec.html;

[184] Apple Inc: https://people.apple.com/US/en/subtopic/845; Photographing employees engaged in protected concerted activities constitutes unlawful surveillance because it has a tendency to intimidate employees and interfere with exercise of Section 7 rights. Photographing in the mere belief that something "might" happen is not a sufficient justification. *F.W. Woolworth Co.*, 310 NLRB 1197 (1993); see also, *National Steel and Shipbuilding Co.*, 324 NLRB 499 (1997) (peaceful union rallies); *Labor Ready, Inc.*, 327 NLRB 1055 (1999), (employer videotapes of workers employed by temporary service in waiting room waiting for assignments unlawful).

[185] Note: Overbroad

> "Workplace Searches [186] Only in cases where allowed under local law, [187] Apple may: Access, search, monitor, archive, and delete Apple data stored on all of its property, as well as non-Apple property, if used for Apple business or if used for accessing Apple data, servers, or networks. This includes all data and messages sent, accessed, viewed, or stored (including those from iCloud, Messages, or other personal accounts) using Apple equipment, networks, or systems.
> Conduct physical, video, or electronic surveillance, search your workspace such as file cabinets, desks, and offices (even if locked), review phone records, or search any non-Apple property (such as backpacks, purses) on company premises."
> "This means that you have no expectation of privacy when using your or someone else's personal devices for Apple business, when using Apple systems or networks, or when on Apple premises."
> "The search or removal of Apple-related content on a device will be determined on a case-by-case basis when there is a business need and subject to local approval processes. Refusing to permit a search or removal of Apple-related content may result in disciplinary action up to and including termination of employment." **[188]**

The GDPR notes that employee monitoring may result in the collection of non-employees' personal data. The GDPR and the BDSG also apply to the collection, processing, and use of non-employees' personal data. Accordingly, the employer must have a valid legal basis for processing non-employees' personal data and **must notify nonemployees about potential personal data collection**.[189] Here, Apple simply tell employees they have no expectation of privacy whatsoever and makes no statements to non-employees who may get caught in Apple's mass-surveillance infrastructure.

Apple is in a unique position, perhaps only comparable to Google & ISPs/carriers, where they have access to an incredible amount of data as system administrators of services and those services are provided by monopolies. If Apple wanted to read its employee's personal emails, and that employee used iCloud, Apple could simply login to its own systems and read the emails. This is the same for data backed up in iCloud backups, or saved on iCloud drive, or send through iMessages. Apple owns the hardware of one of the handful of phones and computers, and even if Apple employees were to use a different company's products, anyone they interacted with who

[186] *Boeing Corporation Advice Memo (2013),* Boeing must cease and desist from creating the impression that its employees' union and/or protected concerted activities are under surveillance. *Register Guard,* 344 NLRB 1142, 1144 (2005) (test is whether the employee would reasonably assume from the statement that their union activities had been placed under surveillance*." Flexsteel Industries*, 311 NLRB 257, 257 (1993).
[187] Note: Overbroad
[188] Note: Overbroad. Do organizing and union materials count as Apple-related?
[189] Employee Monitoring (Germany), Resource ID: W-008-3362, HOLGER LUTZ AND SIMONE BACH, BAKER MCKENZIE, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

did use Apple's products would give Apple a way to spy on that employee through their friends. The same is comparable for Google employees. In this sense, there is no such thing as a "personal" device for an Apple employee. That also weaponizes many consumer products if the non-employee user is simply communicating with an Apple employee on that product.

[190]

I also provided Apple's "*Employee Workplace Search & Privacy Policy*" to Zoe Schiffer back in June and Schiffer quoted it for The Verge's August privacy article:

> Underpinning all of this is a stringent employment agreement that gives Apple the right to conduct extensive employee surveillance, including "physical, video, or electronic surveillance" as well as the ability to "search your workspace such as file cabinets, desks, and offices (even if locked), review phone records, or search any non-Apple property (such as backpacks, purses) on company premises." Apple also tells employees that they should have "no expectation of privacy when using *your or someone else's personal devices for Apple business*, when using Apple systems or networks, or when on Apple premises" [191]

Further, I also filed charge against an email Tim Cook sent his employees on September 21 2021 responding to an employee or employees speaking with journalist about a meeting where Tim Cook talked about the pandemic, remote work, employee benefits, and pay equity.[192]

> "I want you to know that I share your frustration. These opportunities to connect as a team are really important. But they only work if we can trust that the content will stay within Apple. I want to reassure you that we are doing everything in our power to

[190] Twitter, Oct 7 2021, https://twitter.com/ashleygjovik/status/1446368610679730233
[191] Zoe Schiffer, *"Apple Cares About Privacy, Unless You Work at Apple,"* The Verge, Aug 30, 2021, https://www.theverge.com/22648265/apple-employee-privacy-icloud-id
[192] Apple Inc, Tim Cook to Apple_Employees$@group.apple.com, Date: Sept 21, 2021, Subj: *Follow-up on global team meeting*

> identify those who leaked.[193] As you know, we do not tolerate disclosures of confidential information, whether it's product IP or the details of a confidential meeting.[194] We know that the leakers constitute a small number of people. We also know that people who leak confidential information do not belong here.[195] [196] [197][198]

The NLRB agreed with me and found there was merit to my charge against Cook in January 2023.[199] Shortly after Apple hired a prior NLRB Board Chair to defend them (Harry Johnson), and shortly after that, NLRB told me there will be a 're-decision' of merit on the charge. **There is no such thing as a 're-decision of merit'.** I filed a complaint with General Counsel's office arguing there must have been unlawful *ex parte* communications by Johnson leading to the regulatory subterfuge of a 'redecision of merit' (avoiding settlement or adjudication), which violates the NLRA, APA, and my Due Process rights. I have not heard back from NLRB for months.

[193] *Register Guard*, 344 NLRB 1142, 1144 (2005) (test is whether the employee would reasonably assume from the statement that their union activities had been placed under surveillance." *Flexsteel Industries, 311 NLRB 257, 257 (1993),*

[194] *Report of the General Counsel Concerning Employer Rules, NRLB Memorandum GC 15-04 (2015)*

[195] *Yale New Haven Hospital*, 309 NLRB 363, 368 (1992) (supervisor unlawfully threatened employee with reprisal by telling an employee that if he did not stop protected activities he would "talk" to him again; implies that the talk will not be mere conversation but will concern the employment of the offending employee).

[196] *Valerie Manor,Inc.*,351NLRB1306(2007)(threat of unspecified reprisals).

[197] *Equipment Trucking Co.,Inc*.,336NLRB277(2001)(statement, If you don't like it, find another job, implied threat of discharge).

[198] *Medco Health Solutions Of Las Vegas, Inc.*,357NLRBNo.25(2011) (respondent's statement that, if employee could not support the respondent's policies, there were other jobs out there and perhaps "this wasn't the place for him" was an implied threat in violation of 8(a)(1)).

[199] Bloomberg, Apple Executives Violated Worker Rights, Labor Officials Say, https://www.bloomberg.com/news/articles/2023-01-30/apple-executives-violated-worker-rights-us-labor-officials-say

Public Policy

[Collecting user data] is surveillance.
These stockpiles of personal data serve only to enrich the companies that collect them.
-Tim Cook (2018) [200]

I can't think of any other company that has so proudly, and so publicly, distributed spyware to its own devices. The only restraint is Apple's all-too-flexible company policies.
-Edward Snowden (2021) [201]

"Ubiquitous employer surveillance of workers has a long and rich history as a defining characteristic of workplace power dynamics, including the de facto abrogation of almost any substantive legal restraints on its use. This history can be traced through many pivotal points including massive efforts through warfare, slavery, globalization, and other forms of colonialism used to control and exploit workers. [202] What is novel, and of real concern to privacy law, is that rapid technological advancements and diminishing costs now mean employee surveillance occurs both inside and outside the workplace - bleeding into the private lives of employees."[203] There are areas of an employee's life in which his employer has no legitimate interest.[204]

"The protection of workers' privacy is a civil rights issue: both for the protection of human dignity rights and because privacy invasions can serve as vehicles for unlawful discrimination. History has shown that economic pressures are an unreliable regulator for the preservation of the civil rights of those with comparatively lower economic power. We cannot simply look to the market to curtail abuses of power regarding worker surveillance."[205]

---

[200] Ian Bogost, *Apple's Empty Grandstanding About Privacy*, The Atlantic (2019), https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/
[201] Edward Snowden, *The All-Seeing "i": Apple Just Declared War on Your Privacy, Aug 25, 2021,* https://edwardsnowden.substack.com/p/all-seeing-i
[202] Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, *Limitless Worker Surveillance*, 105 Calif. L. Rev. 735 (2017).
[203] Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, *Limitless Worker Surveillance*, 105 Calif. L. Rev. 735 (2017).
[204] *Borse v. Piece Goods Shop, Inc., 963 F.2d 611 (3d Cir. 1992); Geary v. United States Steel Corp., 319 A.2d 174 (Pa. 1974)*
[205] Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, *Limitless Worker Surveillance*, 105 Calif. L. Rev. 735 (2017).

The predominant view of the U.S. Courts is that consent is not effective if it is not freely and voluntarily given.[206] The protection for privacy & autonomy is a default rule that recognizes a sphere of protection, not only to protect civic and personal life, but also to mirror the likely implicit bargain between the employer and employee about where the employment relationship ends and personal life begins. [207] **Even in the context of initial employment, consent to a particular type of invasion does not mean consent to all varieties of that invasion, reasonable or unreasonable.[208]**

The employer also cannot discharge employees for refusing to waive a nonnegotiable or nonwaivable right. [209] When an employee successfully refuses to submit to an employer's wrongful intrusion into protected employee privacy interests and the employee suffers a termination of employment or such adverse conditions of employment as to amount to a constructive discharge because of the employee's refusal to submit, the employee has a claim for wrongful discharge in violation of public policy. The public policy is the protection against wrongful employer intrusions into protected employee privacy interests. [210]

However, companies may be able to process personal data if they obtain either subjects' voluntary affirmative consent to process data for the specific purpose intended or have a legitimate justification. Corporations in countries such as Germany and France tend not to rely on consent because employees must be expressly asked for it, must be able to refuse without risk of sanction, and can withdraw it at any time. Moreover, in the corporate investigation context, courts tend to assume that such consent is involuntary because of the imbalance of power between the employer and employee.[211]

U.S. organizations that control or process the personal data of European Union residents likely are subject to the EU's new data protection requirements, the General Data Protection

---

[206] See *Stores, Inc. v. Lee, 74 S.W.3d 634, 647 (Ark. 2002); Papa Gino's of America, Inc., 780 F.2d 1067, 1072 (1st Cir. 1986)* (applying New Hampshire law; employee contracted away certain rights by accepting employment from employer who forbade drug use, but employer's demand that employee submit to polygraph exceeded scope of employee's consent to allow reasonable investigation into drug use).
[207] *Restatement of the Law, Employment Law* § 7.03, Protected Employee Privacy Interests in the Employee's Physical Person and in Physical and Electronic Locations, *Comments*
[208] *Frye v. IBP, Inc., 15 F. Supp. 2d 1032, 1041 (D. Kan. 1998)*
[209] *Restatement of the Law, Employment Law > Chapter 7- Employee Privacy and Autonomy* § 7.07, Discharge in Retaliation for Refusing Privacy Invasion, *Comment*
[210] *Restatement of the Law, Employment Law > Chapter 7- Employee Privacy and Autonomy* § 7.07, Discharge in Retaliation for Refusing Privacy Invasion, *Comment*
[211] ARTICLE: THE LAW OF CORPORATE INVESTIGATIONS AND THE GLOBAL EXPANSION OF CORPORATE CRIMINAL ENFORCEMENT, 93 S. Cal. L. Rev. 697 May 2020

Regulation (GDPR). A common practice in the U.S. is to rely on blanket consent clauses in employment contracts or handbooks that permit employers to process employee personal data. U.S. employers often also rely on implied consent from employees. However, such practices may not be considered valid forms of consent for lawful processing of personal data under the GDPR. The GDPR provides that consent must be *"freely given, specific, informed and unambiguous."* Moreover, the GDPR adds, consent is not *"freely given"* where a *"clear imbalance of power"* between the data controller (*i.e.*, employer) and the data subject (*i.e.,* employee) exists.[212]

The Article 29 Working Party emphasized the imbalance of power in the employment context: "*Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent."* The Working Party also advises that the imbalance of power in the employment relationship makes voluntary consent questionable and, for most work-related data processing, the GDPR lawful basis relied upon "*cannot and should not*" be the employee's consent. [213]

Multiple GDPR factors invaliding employee to employer consent are present with Apple's user studies. First, when I responded to the initial email about the Gobbler user study, I had no idea what I consented to/initiated., as it was "*vague or unclear*." Next, I had no "*clear records to demonstrate they consented*," as no receipt was sent and I was never given a copy of the ICF. It appears Apple also no longer has a copy of the ICF, otherwise it seems they would have provided it to me on Sept 15 or quoted it in their position statement.

Next, there was "*a clear imbalance of power between [the employer] and the individual*," the "*employee would be penalized for refusing consent,"* and *"there was no genuine free choice over whether to opt in."* Between the general pressure for Apple R&D employees to "live on" new products and software, and to participate in studies, and my performance reviews

[212] Is Employee Consent under EU Data Protection Regulation Possible?, Joseph J. Lazzarotti and Maya Atrakchi, February 27, 2018
[213] Is Employee Consent under EU Data Protection Regulation Possible?, Joseph J. Lazzarotti and Maya Atrakchi, February 27, 2018

mentioning my participation in these programs, but also that barbed wire compound with armed guards, too.

Finally, apparently later some employees were given the option to use the Gobbler application but not be "whitelisted" so their PII would not be uploaded. However, I was not given this option nor even told it was an option, so *"consent was a precondition of a service, but the processing is not necessary for that service."* Finally, once I apparently signed the ICF and after the Gobbler app was installed on my phone, I had no way to disable the app, nor was I given any way to withdraw consent. I had talked to other employees about the app with similar concerns over the years. Thus, the "consent' was invalid because Apple *"did not tell people about their right to withdraw consent"* and "*people cannot easily withdraw consent."* [214]

This non-consensual user data harvesting doesn't only have implications on Apple's employees and their families and friends. Intellectual Property rights cannot be granted for unlawful things/acts. Apple has deployed technology across the world, based on arguably illegal data and the fruit (algorithms and features) grown from that illegal data. What rights does Apple actually have to their technology if the people the data was harvested from had their own rights violated? What does that mean for customers using Apple products built off of human rights violations (again)? Today, the success of the global economy depends on Apple's success. Apple cannot take these kind of risks when the fall-out may land everywhere.

Apple says privacy is a fundamental right and "fundamental rights should not differ depending on where you live in the world." Apple says, *"they treat any data that relates to an identified or identifiable individual or that is linked or linkable to them by Apple as 'personal data,' no matter where the individual lives.*"[215]

California courts have found, "*The constitutional [privacy] provision is self-executing; hence, it confers a judicial right of action on all Californians. Privacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone."* [216] California accords privacy the constitutional status of an inalienable right, on a par with defending life and possessing property.[217]

---

[214] Information Commissioner's Office Consultation: GDPR consent guidance Start date: 2 March 2017 End date: 31 March 2017

[215] Apple Inc, *Worldwide Privacy Policy*, https://www.apple.com/legal/privacy/en-ww/

[216] *Wilkinson v. Times Mirror Corporation* (1989) 215 Cal.App.3d 1034.

[217] *Vinson v. Superior Court* (1987) 43 Cal. 3d 833, 841 [239 Cal. Rptr. 292, 740 P.2d 404] [limiting right to discover one's sexual history, habits and practices in action for sexual harassment and emotional distress].

Apple Is headquartered in California. Article I, section 1 of the California Constitution provides that the right of "privacy" is among the people's inalienable rights. California appellate courts and at least one federal court have consistently held, in varying contexts, that Article I, section 1 provides some protection against non-governmental intrusion, as well as state conduct.[218] The legislative history (ballot argument) stated,

> "The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us."[219]

California employees have a cause of action against their private employer for violating their Constitutional right to privacy if the intrusion is against a legally protected privacy interest, including: "*conducting personal activities without observation, intrusion, or interference*" as determined by "*established social norms*."[220] While California employees could contractually agree not to assert a right to privacy, the employer cannot be allowed to use such an agreement to circumvent the public policy favoring privacy, and the employer could not successfully enforce such a contractual agreement if it intruded on plaintiff's right to privacy.[221] The public policy here "*affects the duty not to intrude on the right of privacy, which inures to the benefit of the public at large rather than to a particular employer or employee*."[222]

California employees have the right to privacy, even at the workplace, in areas where there is a reasonable expectation of being left alone. For example, the California Labor Code prohibits video or audio monitoring of employees in restrooms, showers, locker rooms, and dressing rooms.[223] Further, California Penal Code section 647j makes it a crime for a person

---

[218] *Porten v. University of San Francisco* (1976) 64 Cal.App.3d 825; *Cutter v. Brownbridge* (1986) 183 Cal.App.3d 836; *Miller v. National Broadcasting Company* (1986) 187 Cal.App.3d 1463; *Chico Feminist Women's Health Center v. Scully* (1989) 208 Cal.App.3d 230; *Chico Feminist Women's Health Center v. Butte Glenn Medical S.* (1983) 557 F.Supp. 1190; *Wilkinson v. Times Mirror Corporation* (1989) 215 Cal.App.3d 1034; *Semore v. Pool* (1990) 217 Cal.App.3d 1034; Luck v. Southern Pacific Trans. Co. (1990) 218 Cal.App.3d 1.

[219] *Wilkinson v. Times Mirror Corporation* (1989) 215 Cal.App.3d 1034.

[220] *Hill*, 7 Cal.4th 1, 35, 26 Cal.Rptr.2d 834, 865 P.2d 633.

[221] *Foley v. Interactive Data Corp*., 47 Cal.3d at p. 670 (1988)

[222] *Semore v. Pool* (1990) 217 Cal. App. 3d 1088

[223] California Labor Code § 435, Contracts and Applications for Employment; *§ 435* was enacted to clarify "privacy rights in the workplace for both employers and employees" since court decisions had "left a definite gray area in regards to employee surveillance." Hearing on A.B. 2303 Before the Assemb. Comm. on Labor & Emp't, 1997-98

unlawfully to invade someone else's privacy via a device to view in a private room, or by secret recording or photograph of a person's body.[224]

At a federal level, under the National Labor Relations Act (NLRA), employers may not monitor or surveil employees participating in protected concerted activities, including "*creating the impression of surveillance*."[225] Further, 18 U.S.C. § 1801 makes it a federal crime to capture images of a private area of an individual (naked or undergarment clad genitals, pubic area, buttocks, or female breast) without their consent and to knowingly do so under circumstances in which the individual has a reasonable expectation of privacy. [226]

While the legislative history for federal labor laws probably never anticipated a mega-corporation using a tool they called the "Face Gobbler" to capture secret videos of employees 24/7 – one would think The Congress would be outraged by an employer, one that markets that "privacy is a human right" none the less – justifying the termination of an employee who already had an open NLRB charge against the employer – on the employee protesting invasions of privacy & *Gobbling* of their face.

Leg. Sess. (Cal. Apr. 22, 1998). Since such surveillance was on the rise, the proponents of the statute felt that a "reasonable limitation" should be placed on it. Hearing on A.B. 2303 Before the S. Comm. on Indus. Relations, 1997-98 Leg. Sess. (Cal. June 11, 1998).

[224] California Penal Code Section 647(j) PC, Criminal Invasion of Privacy in California,

[225] Gov Docs, *More video surveillance in the workplace. But is it legal*?, https://www.govdocs.com/can-employers-use-video-surveillance-monitor-workers/; *NLRB v Boeing (2017)*

[226] 18 U.S. Code § 1801 - Video voyeurism, https://www.law.cornell.edu/uscode/text/18/1801

Conclusion

No matter what it says, Apple is not a company committed to data privacy. Apple's business model helped stimulate the data-privacy dystopia we now occupy. Apple is allowing the surveillance-capitalism atrocities it claims to oppose.
- Ian Bogost, The Atlantic (2019) [227]

It's clear Apple's use of surveillance and electronic monitoring in the workplace is illegal, unlawful, and otherwise unethical. It's clear Apple knows this.

The Restatement makes clear: information regarding an employer's illegal activities is not a trade secret.[228] Further, information regarding an employer's illegal activities is not protectable by means of restrictive covenant. [229] The public policy protecting whistleblowers would be completely thwarted if the employer could retaliate with impunity against any employee who decided to reveal improper conduct by the employer.[230]

Yet, Apple is notorious for oppressing & silencing their workforce. An opinion piece was written by Anil Dash about the issue. Dash is "recognized as one of the most prominent voices advocating for a more humane, inclusive & ethical technology industry," was an advisor to the Obama White House, and is a Board Member of the EFF (Electronic Frontier Foundation) an international, non-profit digital rights group.[231] Dash wrote about Apple:

> The sad truth is that Apple is still stuck in an **anachronistic, 1984 mode** of communicating with the world. If Apple doesn't evolve, it'll become a pathetic-looking giant, constantly playing whack-a-mole with information leaks, diminishing its relevance by antagonizing the very creators it has so long sought to identify with. … The reckoning Apple has reached, whether it's admitted or not, is that its **secrecy is compromising its humanity…**It's incumbent upon Apple to do the moral thing here. Treat your **employees**, customers, suppliers and partner companies better, by letting them participate in the thing most of your products are designed for: Human self-expression. If the ethical argument is unpersuasive, then focus on the long-term viability of your marketing and branding efforts, and realize that a technology company that is determined to

[227] Ian Bogost, *Apple's Empty Grandstanding About Privacy*, The Atlantic (2019), https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/
[228] Restatement of the Law, Employment Law, § 8.02, Definition of Employer's Trade Secret**,** *Comment*
[229] Restatement of the Law, Employment Law, § 8.02, Definition of Employer's Trade Secret**,** *Comment*
[230] *Harris v. City of Santa Monica* (2013) 56 Cal.4th 203, 229-230, 152 Cal.Rptr.3d 392, 294 P.3d 49; *Green v. Ralee Engineering Co.* (1998) 19 Cal.4th 66, 90, 78 Cal.Rptr.2d 16, 960 P.2d 1046 Whitehall v. County of San Bernardino, 17 Cal.App.5th 352 (2017)
[231] EFF, Anil Dash, https://www.eff.org/about/staff/anil-dash

> prevent information from being spread is an organization at war with itself. **Civil wars are expensive, have no winners, and incur lots of casualties**.[232]

Apple clearly did not listen.

The US government has not taken this seriously either. Both the NLRB and US Dept of Labor initially responded to my charges by attempting to intimidate me to withdraw those charges, and then when I refused, attempting to intimidate me and interfere with my due process rights. NLRB is now supposedly investigating. US Dept of Labor has only escalated it animosity towards me. California Dept of Labor says it won't even start investigating for another 1-3 years. Meanwhile I'm now unemployed, denylisted, broke, in debt, severely ostracized, & my reputation destroyed by smears and defamation.

What is the point of 'worker protection laws' or 'privacy 'laws' if they are never enforced? Do we live in a democracy if corporations are above the law? The first step here is not passing new laws or enacting more MOUs; the first step is deciding that no company is above the law. The first step is ensuring labor agencies will actually fulfill their statutory obligations. We must all agree that labor rights are human rights, and human rights must be protected.

Please let me know if I can be of any help. I'm more than happy to provide documents, testimony, or other additional resources. Thank you.

Respectfully,

Ashley M. Gjovik, JD
Albany, New York
ashleymgjovik@protonmail.com

[232] Anil Dash, Apple: Secrecy Does Not Scale, Anil Dash, https://anildash.com/2009/07/31/apple_secrecy_does_not_scale/

Comment Period Ends: **5 Days**

NOTICE

Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Posted by the **Office of Science and Technology Policy** on Jun 20, 2023

Comment (/commenton/OSTP_FRDOC_0001-0008)

View More Documents 4 (/docket/OSTP_FRDOC_0001/document)

Share

Document Details

(/document/OSTP_FRDOC_0001-0008)

Content

Action

Notice of request for information (RFI).

Summary

Employers are increasingly using automated systems to monitor, manage, and evaluate their workers. These systems may allow employers to manage supply chains, improve health and safety, or make other informed business decisions. At the same time, applications of surveillance and monitoring systems can also pose risks to workers, including to their health and safety, equal employment opportunities, privacy, ability to meet critical needs, access to workplace accommodations, and exercise of workplace and labor rights, including their rights to form or join a labor union. The White House Office of Science and Technology Policy (OSTP) seeks comments from the public to better understand automated surveillance and management of workers, including its prevalence, purposes, deployment, and impacts, as well as opportunities for Federal agencies to work with employers, workers, and other stakeholders to ensure that these systems do not undermine workers' rights, opportunities, access, health, or safety.

Dates

Interested persons and organizations are invited to submit comments on or before 5 p.m. ET, June 29, 2023.

Addresses

Comments must be submitted via the Federal eRulemaking Portal at *regulations.gov.* However, if you require an accommodation or cannot otherwise submit your comments via *regulations.gov,* please contact the program contact person listed under FOR FURTHER INFORMATION CONTACT . OSTP will not accept comments by fax, or comments submitted after the comment period closes. To ensure that OSTP does not receive duplicate copies, please submit your comments only once. Additionally, please include the Docket ID at the top of your comments.

Federal eRulemaking Portal: Go to *www.regulations.gov* to submit your comments electronically. Information on how to use *Regulations.gov,* including instructions for accessing agency documents, submitting comments, and viewing the docket, is available on the site under “FAQ” (*https://www.regulations.gov/faq*).

Privacy Note: OSTP's policy is to make all comments received from members of the public available for public viewing in their entirety on the Federal eRulemaking Portal at *www.regulations.gov.* Therefore, commenters should be careful to include in their comments only information that they wish to make publicly available. OSTP requests that no proprietary information, copyrighted information, or personally identifiable information be submitted in response to this RFI.

Instructions: Response to this RFI is voluntary. Respondents may answer as many or as few questions as they wish. Responses containing references, studies, research, and other empirical data that are not widely published should include copies of or electronic links to the referenced materials. Any information obtained from this RFI is intended to be used by the Government on a non-attribution basis for planning and strategy development. OSTP will not respond to individual submissions. A response to this RFI will not be viewed as a binding commitment to develop or pursue the project or ideas discussed. This RFI is not accepting applications for financial assistance or financial incentives. All comments, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Proprietary information or sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included in the body of your response. Respondents interested in submitting anonymous comments should use the option on *www.regulations.gov/.*

For Further Information Contact

Alan Mislove, Assistant Director for Data and Democracy, *workersurveillance@ostp.eop.gov,* 202–456–4444.

Supplementary Information

Background: Employers are increasingly using automated systems to monitor, manage, and evaluate their workers—both on and off the job. According to a 2022 investigation by the *New York Times,* eight of the ten largest private U.S. employers track the productivity metrics of individual workers. [(1)] Use of automated surveillance and management systems has increased with the spread of remote work during the pandemic, and now often extends to workers' homes. [(2)] Private-sector research suggests that the percentage of large employers using automated tools to track their workforce may have doubled since the beginning of the pandemic to some 60%. [(3)]

Automated worker surveillance and management systems may track workers' location, pace or quality of work, communications (*e.g.,* text, chats, emails, social media), interactions with other workers or customers, and computer activity. Such surveillance can be accomplished through a variety of techniques, ranging from software on workers' computers to dedicated electronic devices that workers wear or carry on their person. The market for these technologies and systems has greatly expanded in recent years, and a number of vendors are now developing products to help employers electronically monitor and manage their workers in a variety of contexts.

Examples of applications of automated surveillance and management of workers that have been reported in the press include:

- Warehouse workers who are tracked by whether they are actively moving products
- Grocery store cashiers who are monitored on the speed of their transactions with customers
- Office workers whose keystrokes, chats, emails, and other communications are collected and monitored
- Lawyers whose computer cameras track whether their eyes are actively focused on the screen
- Call center workers whose calls are monitored by a computer that judges the emotional state of customers
- Copywriters whose computers automatically take screenshots of their activity to track which applications they are using
- Home healthcare workers whose locations are monitored by an app that verifies patient visits
- Nurses whose time on task and location are tracked through radio frequency identification (RFID) tags in identification badges
- Delivery or rideshare drivers whose vehicles track their location, speed, and driving behavior
- Long-haul truckers whose eye movements are monitored and locations tracked
- Fast food workers whose pace of work in preparing meals is tracked and reported
- Teachers whose lessons delivered remotely online are recorded and analyzed electronically

These systems may allow employers to more closely monitor worker performance; protect public health and safety; make decisions about promotion, discipline, or termination; or manage work assignments, schedules, and supply chains. At the same time, applications of automated surveillance and management systems can also pose risks to workers and even violate labor and employment laws. [(4)] Emerging research suggests that certain applications of these systems may undermine the quality of work; workers' rights to a safe and healthy workplace; compensation for time worked; labor market competition; and workers' ability to organize and work collectively with their coworkers to improve working conditions, including through labor unions. Certain applications of these systems—when paired with decisions about working conditions, promotion, discipline, or termination—may also treat otherwise similar workers differently on the basis of their race, ethnicity, gender, religion, age, national origin, health or disability, or other protected status. Some systems may also violate antitrust and privacy laws, for instance, if employers use technologies to artificially reduce wages.

Automated worker surveillance and management can also cause and exacerbate disabilities and interfere with legal protections for those with disabilities. Automated worker surveillance and management systems can potentially put workers at risk for physical injury and mental health distress that can cause or exacerbate anxiety, depression, cognitive disability, and trauma responses; interfere with legally-protected workplace accommodations that enable individuals with disabilities to participate in the workforce; and reveal workers' otherwise-undisclosed disabilities to employers.

In 2022, the White House Office of Science and Technology Policy released the *Blueprint for an AI Bill of Rights* (“Blueprint”), which stated that individuals “should be free from unchecked surveillance.” [(5)] The Blueprint noted that continuous surveillance can pose harms to workers, using the example of electronic

monitoring intended to stymie workers' efforts to organize a labor union. Consistent with the Blueprint, the Office of Science and Technology Policy seeks to further study the use of automated surveillance and management systems in the workplace, including their prevalence, impacts, and deployment, as well as opportunities for Federal agencies to work together with employers and workers to ensure that these systems do not undermine workers' rights or their safety.

This focus on automated surveillance and management in the workplace is also consistent with the Administration's commitment to ensuring that all workers have access to high-quality, well-paying jobs, including jobs with opportunities to organize and bargain collectively with their employers through labor unions, as articulated in the Executive Order 14025 (*Worker Organizing and Empowerment*) [(6)] and through a competitive market for their labor, as articulated in Executive Order 14036 (*Promoting Competition in the American Economy*). [(7)] This initiative advances the Biden-Harris Administration's historic commitment to racial equity and support for underserved communities, by investigating whether automated surveillance and management systems “contribute to unjustified different treatment or impacts,” as articulated in Executive Order 14091 (*Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*) as well as the Administration's call for robust protections for Americans' privacy.

Request for Comment: This request for information seeks input from the public on the prevalence, uses and purposes, and deployment of automated worker surveillance and management systems, including impacts of these systems on workers' legal rights and lives. It includes workers' physical and mental health; privacy, dignity, and autonomy; and ability to exercise workplace rights, including rights to collective action, pay, reasonable accommodation, health, and safety, and freedom from retaliation, discrimination, and harassment. It also seeks input on how employers may share data collected through these surveillance applications and how worker surveillance may contribute to unfair competition between firms.

This RFI focuses on automated surveillance and management by employers that may track workers' locations, pace of work, performance or output, compliance with policy or regulations, or social media activity; their emails, texts, chats, phone calls, and other communications; or other similar measures. Such surveillance may take place during or outside of work hours, and on or off the worksite. This request for information also covers workers in traditional employment relationships (*i.e.,* W–2 employment) as well as other employment relationships, such as independent contractors and gig economy workers.

OSTP is particularly interested in hearing from:

- Workers who have experienced automated surveillance and management (including workers of color, low-paid workers, immigrant workers, and workers with disabilities);
- Worker organizations (including worker advocacy groups, worker centers, labor unions, and workplace legal services providers);
- Civil rights and privacy organizations;
- Employers (including for-profit, non-profit, and government employers) that are using automated surveillance and management systems or considering using such systems;
- Platforms, crowdsourcing websites, transportation network companies, ride-hailing services, and other entities that match workers with opportunities to generate income;
- Trade and business associations representing employers;
- Developers and vendors developing or selling automated surveillance or management systems;
- Researchers (including researchers using both qualitative and quantitative methods to understand the use, prevalence, benefits and risks, and impacts of automated surveillance and management systems on individuals and society); and
- State, Tribal, local, and Territorial governments.

To assist commenters in developing responses, OSTP has crafted the questions below that commenters may answer. Respondents may provide information for one or more of the topics below, as desired. *However, OSTP welcomes members of the public to submit any personal experiences, data, information, and research relating to the use and impact of automated worker surveillance and management systems. Please do not to include personally identifying information in the body of your response.*

1. If you are a *worker or organization representing workers (such as a worker center, union, or legal services provider),* please tell us about your experiences with automated worker surveillance and management systems or the experiences of the workers you interact with, including:

a. The type of work you do (*e.g.,* describe the relevant job, employer, and industry);

b. Whether you are a member of a labor union;

c. The type of automated surveillance or management you have experienced, including the location of the monitoring technology (such as an app you had to use or download; a device you had to use, carry, or wear; or a camera that monitors you);

d. Whether the automated surveillance or management was used during a labor organizing drive;

e. Whether and when your employer informed you about their use of automated worker surveillance and management systems;

f. Whether you (or, if relevant, your representative, like a labor union) have any input or control over how, where, and over what automated surveillance occurs;

g. Whether you know how the data generated by surveillance is used for management or other purposes (including purposes related to employment or labor market competition);

h. Whether you (or, if relevant, your representative, like a labor union) have any visibility into the data collected on you or how it is used, including whether data on you collected by surveillance can be shared with other companies, trade groups, or third parties;

i. How the use of automated surveillance and management systems has changed how you do your job or how your employer treated you at your job;

j. Whether your employer has used information from an automated surveillance and management system in support of any discipline against you—and if so, what the action was, how and when you were informed, and what information was provided to you or your representative (such as a labor union);

k. How automated surveillance and management has affected you—whether positively or negatively—including any economic, safety, physical, mental, and emotional impacts;

l. How automated surveillance and management systems have affected your workplace rights, including rights around collective action, labor organizing, collective bargaining, pay, reasonable accommodations, health and safety, discrimination, and harassment—or your expectation of retaliation when exercising these rights;

m. How these systems have impacted your non-working hours, personal time, or the privacy of other members of your household;

n. If you are disabled or have a health condition, how automated surveillance and management systems have impacted or may impact your use of reasonable accommodations; such as assistive technology or accessibility features of software or breaks, or affected your ability to keep information about your condition private from your employer, supervisor, or coworkers;

o. If you are disabled or have a health condition, how automated surveillance and management systems have affected performance reviews or other management activities, or concerns about how these systems may affect performance reviews or how your management treats you; and

p. Whether you work for an employer that receives Federal funds (for instance, as a Federal contractor).

2. If you are an *employer or organization representing employers,* please tell us about your experiences implementing or using automated worker surveillance and management systems, including:

a. The type of business you are in, or represent, including your industry and roughly how many workers you employ;

b. Whether any of your employees are represented by a labor union;

c. The types of automated worker surveillance and management systems your business has implemented or is considering implementing;

d. The purposes for which your business decided to implement automated worker surveillance and management systems, such as safety and health, productivity, competition, liability or insurance, compliance, or resource and worker management;

e. How your business decided to use specific automated worker surveillance and management systems, including decisions not to use particular products or types of systems, to limit their scope, and relevant training;

f. In what ways your business uses the information collected through automated surveillance and management systems, such as for management, human resources, and business operations, including whether the information is sold or shared with other businesses or otherwise influenced by other businesses' activities;

g. Any steps your business has taken to solicit or incorporate worker input into how automated worker surveillance and management systems are adopted, implemented, and used; whether workers may opt out of such systems (and any consequences for doing so); and how generated data is used or shared with other parties;

h. Any involvement of third parties (such as vendors) in collecting or maintaining information on workers and any control retained by the employer;

i. Any steps you have taken to ensure that the use or sharing of automated worker surveillance and management systems does not infringe on workers' rights;

j. How you decide the categories of workers for whom you deploy automated worker surveillance and management systems (*e.g.,* managerial versus non-managerial workers);

k. Any policies or protocols adopted to govern the use of automated worker surveillance and management systems or the data they produce; and Whether your organization receives Federal funds.

3. If you are a *technology developer or vendor,* please tell us about your experience developing or distributing automated worker surveillance and management systems, including:

a. The purposes for which employers adopt your products and how they deploy these products;

b. How the impact, performance, and efficacy of your products is audited and validated by you, employers, and workers;

c. How you and the users of your products manage data collection, storage, and maintenance, including access to data by third parties;

d. Whether you provide guidance to employers on your products and their appropriate use, including guidance on notifying workers about the use of technology, and offering opportunities for workers to consent to or opt out of data collection;

e. Whether you engage with employers to help them implement your products in ways that protect workers' rights, health, and safety—or otherwise take steps to help protect workers who will engage with your products; and

f. Any steps you have taken to ensure that the use of automated worker surveillance and management systems does not infringe on workers' rights.

4. Data and research-related questions we are interested in include:

a. What data and evidence exist on the prevalence of automated worker surveillance and management systems across different industries, occupations, and regions, including changes over time?

b. What data and evidence exist on the impact of automated worker surveillance and management systems on workers, including workers' pay, benefits, and employment, physical and mental health, and ability to exercise workplace rights?

c. What data and evidence exist on the impact of automated worker surveillance and management systems on labor rights, including workers' abilities to form and join unions and bargain collectively with their employers?

d. What data and evidence exist on how the impact of automated worker surveillance and management systems differs across groups of workers, including based on characteristics such as race, national origin, sex, age, disability, religion, or health status?

e. What data or evidence exists on whether automated worker surveillance and management systems are being used for discriminatory purposes or resulting in discrimination?

f. What data and evidence exist on whether automated workers surveillance and management systems impact employers' ability to recruit and retain workers?

g. What data or evidence exists on how the provision of reasonable accommodations is accounted for in the design and operation of automated worker surveillance and management systems?

h. What data and evidence exist on why employers decide to adopt automated worker surveillance and management systems?

i. Are there any existing or new systems that aggregate worker surveillance data across multiple employers?

j. What are new or emergent automated worker surveillance and management systems—or new and emergent uses of existing technologies—that Federal agencies should be tracking?

k. Where might further research, including by the Federal Government, be helpful in understanding the prevalence and impact of automated worker surveillance and management systems?

5. Last, we are especially interested in the following questions about policies, practices, or standards that could protect workers:

a. What guidelines, standards, or best practices might inform the design of automated worker surveillance and management systems to protect workers' rights?

b. Are there policy approaches to regulating automated worker surveillance and management systems from state, Tribal, territorial, or local governments or other countries that Federal agencies could learn from?

c. What policies or actions should Federal agencies consider to protect workers' rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?

Dated: June 13, 2023.
Stacy Murphy,
Deputy Chief Operations Officer/Security Officer.
[FR Doc. 2023–12995 Filed 6–16–23; 8:45 am]
BILLING CODE 3270–F1–P

Footnotes

(1) *https://www.yahoo.com/video/bosses-giving-return-office-fight-191121126.html* .

(2) *https://www.shrm.org/hr-today/news/all-things-work/pages/monitoring-remote-workers.aspx* .

(3) *https://www.gartner.com/en/articles/the-right-way-to-monitor-your-employee-productivity* .

(4) See for instance, *https://laborcenter.berkeley.edu/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf, https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/,* and *https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/.*

(5) *https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/* .

(6) *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/04/26/executive-order-on-worker-organizing-and-empowerment/* .

(7) *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/* .

Document Details

Comment Due Date
Jun 29, 2023

Federal Register Number
2023-12995

Received Date
Jun 20, 2023

Comment Start Date
Jun 20, 2023

available in ADAMS) is provided the first time that it is mentioned in this document.

FOR FURTHER INFORMATION CONTACT: Edward Harvey, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001; telephone: 301–415–3704; email: *Edward.Harvey@nrc.gov.*

SUPPLEMENTARY INFORMATION: Section 208 of the Energy Reorganization Act of 1974, as amended (Pub. L. 93–438), defines an ''abnormal occurrence'' as an unscheduled incident or event that the NRC determines to be significant from the standpoint of public health or safety. The FY 2022 AO report, NUREG–0090, Volume 45, ''Report to Congress on Abnormal Occurrences: Fiscal Year 2022'' (ADAMS Accession No. ML23158A228), describes those events that the NRC identified as AOs during FY 2022.

This report describes eight events involving Agreement State licensees and one event involving an NRC licensee. Seven of the AOs occurred at medical facilities and the other two events involved overexposures.

The NRC identified no events at NRC-licensed facilities during FY 2022 that met the guidelines for inclusion in Appendix B, ''Other Events of Interest.''

One event met the guidelines for inclusion in appendix C, ''Updates of Previously Reported Abnormal Occurrences.''

Agreement States are the 39 U.S. States that currently have entered into formal agreements with the NRC pursuant to section 274 of the Atomic Energy Act of 1954, as amended (AEA), to regulate certain quantities of AEA-licensed material at facilities located within their borders.

The Federal Reports Elimination and Sunset Act of 1995 (Pub. L. 104–68) requires that AOs be reported to Congress annually. The full report, NUREG–0090, Volume 45, ''Report to Congress on Abnormal Occurrences: Fiscal Year 2022,'' is also available electronically at the NRC's public website at *https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff.*

Dated: June 14, 2023.

For the Nuclear Regulatory Commission.

Brooke P. Clark,

Secretary of the Commission.

[FR Doc. 2023–13083 Filed 6–16–23; 8:45 am]

BILLING CODE 7590–01–P

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

AGENCY: Office of Science and Technology Policy (OSTP).

ACTION: Notice of request for information (RFI).

SUMMARY: Employers are increasingly using automated systems to monitor, manage, and evaluate their workers. These systems may allow employers to manage supply chains, improve health and safety, or make other informed business decisions. At the same time, applications of surveillance and monitoring systems can also pose risks to workers, including to their health and safety, equal employment opportunities, privacy, ability to meet critical needs, access to workplace accommodations, and exercise of workplace and labor rights, including their rights to form or join a labor union. The White House Office of Science and Technology Policy (OSTP) seeks comments from the public to better understand automated surveillance and management of workers, including its prevalence, purposes, deployment, and impacts, as well as opportunities for Federal agencies to work with employers, workers, and other stakeholders to ensure that these systems do not undermine workers' rights, opportunities, access, health, or safety.

DATES: Interested persons and organizations are invited to submit comments on or before 5 p.m. ET, June 29, 2023.

ADDRESSES: Comments must be submitted via the Federal eRulemaking Portal at *regulations.gov.* However, if you require an accommodation or cannot otherwise submit your comments via *regulations.gov,* please contact the program contact person listed under **FOR FURTHER INFORMATION CONTACT**. OSTP will not accept comments by fax, or comments submitted after the comment period closes. To ensure that OSTP does not receive duplicate copies, please submit your comments only once. Additionally, please include the Docket ID at the top of your comments.

Federal eRulemaking Portal: Go to *www.regulations.gov* to submit your comments electronically. Information on how to use *Regulations.gov,* including instructions for accessing agency documents, submitting comments, and viewing the docket, is available on the site under ''FAQ'' (*https://www.regulations.gov/faq*).

Privacy Note: OSTP's policy is to make all comments received from members of the public available for public viewing in their entirety on the Federal eRulemaking Portal at *www.regulations.gov.* Therefore, commenters should be careful to include in their comments only information that they wish to make publicly available. OSTP requests that no proprietary information, copyrighted information, or personally identifiable information be submitted in response to this RFI.

Instructions: Response to this RFI is voluntary. Respondents may answer as many or as few questions as they wish. Responses containing references, studies, research, and other empirical data that are not widely published should include copies of or electronic links to the referenced materials. Any information obtained from this RFI is intended to be used by the Government on a non-attribution basis for planning and strategy development. OSTP will not respond to individual submissions. A response to this RFI will not be viewed as a binding commitment to develop or pursue the project or ideas discussed. This RFI is not accepting applications for financial assistance or financial incentives. All comments, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Proprietary information or sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included in the body of your response. Respondents interested in submitting anonymous comments should use the option on *www.regulations.gov/.*

FOR FURTHER INFORMATION CONTACT: Alan Mislove, Assistant Director for Data and Democracy, *workersurveillance@ostp.eop.gov,* 202–456–4444.

SUPPLEMENTARY INFORMATION:

Background: Employers are increasingly using automated systems to monitor, manage, and evaluate their workers—both on and off the job. According to a 2022 investigation by the *New York Times,* eight of the ten largest private U.S. employers track the productivity metrics of individual workers.[1] Use of automated surveillance and management systems has increased with the spread of remote work during the pandemic, and now often extends to workers' homes.[2] Private-sector research

[1] *https://www.yahoo.com/video/bosses-giving-return-office-fight-191121126.html.*

[2] *https://www.shrm.org/hr-today/news/all-things-work/pages/monitoring-remote-workers.aspx.*

suggests that the percentage of large employers using automated tools to track their workforce may have doubled since the beginning of the pandemic to some 60%.[3]

Automated worker surveillance and management systems may track workers' location, pace or quality of work, communications (*e.g.,* text, chats, emails, social media), interactions with other workers or customers, and computer activity. Such surveillance can be accomplished through a variety of techniques, ranging from software on workers' computers to dedicated electronic devices that workers wear or carry on their person. The market for these technologies and systems has greatly expanded in recent years, and a number of vendors are now developing products to help employers electronically monitor and manage their workers in a variety of contexts.

Examples of applications of automated surveillance and management of workers that have been reported in the press include:

- Warehouse workers who are tracked by whether they are actively moving products
- Grocery store cashiers who are monitored on the speed of their transactions with customers
- Office workers whose keystrokes, chats, emails, and other communications are collected and monitored
- Lawyers whose computer cameras track whether their eyes are actively focused on the screen
- Call center workers whose calls are monitored by a computer that judges the emotional state of customers
- Copywriters whose computers automatically take screenshots of their activity to track which applications they are using
- Home healthcare workers whose locations are monitored by an app that verifies patient visits
- Nurses whose time on task and location are tracked through radio frequency identification (RFID) tags in identification badges
- Delivery or rideshare drivers whose vehicles track their location, speed, and driving behavior
- Long-haul truckers whose eye movements are monitored and locations tracked
- Fast food workers whose pace of work in preparing meals is tracked and reported
- Teachers whose lessons delivered remotely online are recorded and analyzed electronically

These systems may allow employers to more closely monitor worker performance; protect public health and safety; make decisions about promotion, discipline, or termination; or manage work assignments, schedules, and supply chains. At the same time, applications of automated surveillance and management systems can also pose risks to workers and even violate labor and employment laws.[4] Emerging research suggests that certain applications of these systems may undermine the quality of work; workers' rights to a safe and healthy workplace; compensation for time worked; labor market competition; and workers' ability to organize and work collectively with their coworkers to improve working conditions, including through labor unions. Certain applications of these systems—when paired with decisions about working conditions, promotion, discipline, or termination—may also treat otherwise similar workers differently on the basis of their race, ethnicity, gender, religion, age, national origin, health or disability, or other protected status. Some systems may also violate antitrust and privacy laws, for instance, if employers use technologies to artificially reduce wages.

Automated worker surveillance and management can also cause and exacerbate disabilities and interfere with legal protections for those with disabilities. Automated worker surveillance and management systems can potentially put workers at risk for physical injury and mental health distress that can cause or exacerbate anxiety, depression, cognitive disability, and trauma responses; interfere with legally-protected workplace accommodations that enable individuals with disabilities to participate in the workforce; and reveal workers' otherwise-undisclosed disabilities to employers.

In 2022, the White House Office of Science and Technology Policy released the *Blueprint for an AI Bill of Rights* (''Blueprint''), which stated that individuals ''should be free from unchecked surveillance.'' [5] The Blueprint noted that continuous surveillance can pose harms to workers, using the example of electronic monitoring intended to stymie workers' efforts to organize a labor union. Consistent with the Blueprint, the Office of Science and Technology Policy seeks to further study the use of automated surveillance and management systems in the workplace, including their prevalence, impacts, and deployment, as well as opportunities for Federal agencies to work together with employers and workers to ensure that these systems do not undermine workers' rights or their safety.

This focus on automated surveillance and management in the workplace is also consistent with the Administration's commitment to ensuring that all workers have access to high-quality, well-paying jobs, including jobs with opportunities to organize and bargain collectively with their employers through labor unions, as articulated in the Executive Order 14025 (*Worker Organizing and Empowerment*) [6] and through a competitive market for their labor, as articulated in Executive Order 14036 (*Promoting Competition in the American Economy*).[7] This initiative advances the Biden-Harris Administration's historic commitment to racial equity and support for underserved communities, by investigating whether automated surveillance and management systems ''contribute to unjustified different treatment or impacts,'' as articulated in Executive Order 14091 (*Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*) as well as the Administration's call for robust protections for Americans' privacy.

Request for Comment: This request for information seeks input from the public on the prevalence, uses and purposes, and deployment of automated worker surveillance and management systems, including impacts of these systems on workers' legal rights and lives. It includes workers' physical and mental health; privacy, dignity, and autonomy; and ability to exercise workplace rights, including rights to collective action, pay, reasonable accommodation, health, and safety, and freedom from retaliation, discrimination, and harassment. It also seeks input on how employers may share data collected through these surveillance applications and how worker surveillance may contribute to unfair competition between firms.

[3] *https://www.gartner.com/en/articles/the-right-way-to-monitor-your-employee-productivity.*

[4] See for instance, *https://laborcenter.berkeley.edu/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf, https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/,* and *https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/.*

[5] *https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/.*

[6] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/04/26/executive-order-on-worker-organizing-and-empowerment/.*

[7] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.*

This RFI focuses on automated surveillance and management by employers that may track workers' locations, pace of work, performance or output, compliance with policy or regulations, or social media activity; their emails, texts, chats, phone calls, and other communications; or other similar measures. Such surveillance may take place during or outside of work hours, and on or off the worksite. This request for information also covers workers in traditional employment relationships (*i.e.,* W–2 employment) as well as other employment relationships, such as independent contractors and gig economy workers.

OSTP is particularly interested in hearing from:

- Workers who have experienced automated surveillance and management (including workers of color, low-paid workers, immigrant workers, and workers with disabilities);
- Worker organizations (including worker advocacy groups, worker centers, labor unions, and workplace legal services providers);
- Civil rights and privacy organizations;
- Employers (including for-profit, non-profit, and government employers) that are using automated surveillance and management systems or considering using such systems;
- Platforms, crowdsourcing websites, transportation network companies, ride-hailing services, and other entities that match workers with opportunities to generate income;
- Trade and business associations representing employers;
- Developers and vendors developing or selling automated surveillance or management systems;
- Researchers (including researchers using both qualitative and quantitative methods to understand the use, prevalence, benefits and risks, and impacts of automated surveillance and management systems on individuals and society); and
- State, Tribal, local, and Territorial governments.

To assist commenters in developing responses, OSTP has crafted the questions below that commenters may answer. Respondents may provide information for one or more of the topics below, as desired. *However, OSTP welcomes members of the public to submit any personal experiences, data, information, and research relating to the use and impact of automated worker surveillance and management systems. Please do not to include personally identifying information in the body of your response.*

1. If you are a *worker or organization representing workers (such as a worker center, union, or legal services provider),* please tell us about your experiences with automated worker surveillance and management systems or the experiences of the workers you interact with, including:

a. The type of work you do (*e.g.,* describe the relevant job, employer, and industry);

b. Whether you are a member of a labor union;

c. The type of automated surveillance or management you have experienced, including the location of the monitoring technology (such as an app you had to use or download; a device you had to use, carry, or wear; or a camera that monitors you);

d. Whether the automated surveillance or management was used during a labor organizing drive;

e. Whether and when your employer informed you about their use of automated worker surveillance and management systems;

f. Whether you (or, if relevant, your representative, like a labor union) have any input or control over how, where, and over what automated surveillance occurs;

g. Whether you know how the data generated by surveillance is used for management or other purposes (including purposes related to employment or labor market competition);

h. Whether you (or, if relevant, your representative, like a labor union) have any visibility into the data collected on you or how it is used, including whether data on you collected by surveillance can be shared with other companies, trade groups, or third parties;

i. How the use of automated surveillance and management systems has changed how you do your job or how your employer treated you at your job;

j. Whether your employer has used information from an automated surveillance and management system in support of any discipline against you—and if so, what the action was, how and when you were informed, and what information was provided to you or your representative (such as a labor union);

k. How automated surveillance and management has affected you—whether positively or negatively—including any economic, safety, physical, mental, and emotional impacts;

l. How automated surveillance and management systems have affected your workplace rights, including rights around collective action, labor organizing, collective bargaining, pay, reasonable accommodations, health and safety, discrimination, and harassment—or your expectation of retaliation when exercising these rights;

m. How these systems have impacted your non-working hours, personal time, or the privacy of other members of your household;

n. If you are disabled or have a health condition, how automated surveillance and management systems have impacted or may impact your use of reasonable accommodations; such as assistive technology or accessibility features of software or breaks, or affected your ability to keep information about your condition private from your employer, supervisor, or coworkers;

o. If you are disabled or have a health condition, how automated surveillance and management systems have affected performance reviews or other management activities, or concerns about how these systems may affect performance reviews or how your management treats you; and

p. Whether you work for an employer that receives Federal funds (for instance, as a Federal contractor).

2. If you are an *employer or organization representing employers,* please tell us about your experiences implementing or using automated worker surveillance and management systems, including:

a. The type of business you are in, or represent, including your industry and roughly how many workers you employ;

b. Whether any of your employees are represented by a labor union;

c. The types of automated worker surveillance and management systems your business has implemented or is considering implementing;

d. The purposes for which your business decided to implement automated worker surveillance and management systems, such as safety and health, productivity, competition, liability or insurance, compliance, or resource and worker management;

e. How your business decided to use specific automated worker surveillance and management systems, including decisions not to use particular products or types of systems, to limit their scope, and relevant training;

f. In what ways your business uses the information collected through automated surveillance and management systems, such as for management, human resources, and business operations, including whether the information is sold or shared with other businesses or otherwise influenced by other businesses' activities;

g. Any steps your business has taken to solicit or incorporate worker input into how automated worker surveillance and management systems are adopted, implemented, and used; whether workers may opt out of such systems (and any consequences for doing so); and how generated data is used or shared with other parties;

h. Any involvement of third parties (such as vendors) in collecting or maintaining information on workers and any control retained by the employer;

i. Any steps you have taken to ensure that the use or sharing of automated worker surveillance and management systems does not infringe on workers' rights;

j. How you decide the categories of workers for whom you deploy automated worker surveillance and management systems (*e.g.,* managerial versus non-managerial workers);

k. Any policies or protocols adopted to govern the use of automated worker surveillance and management systems or the data they produce; and Whether your organization receives Federal funds.

3. If you are a *technology developer or vendor,* please tell us about your experience developing or distributing automated worker surveillance and management systems, including:

a. The purposes for which employers adopt your products and how they deploy these products;

b. How the impact, performance, and efficacy of your products is audited and validated by you, employers, and workers;

c. How you and the users of your products manage data collection, storage, and maintenance, including access to data by third parties;

d. Whether you provide guidance to employers on your products and their appropriate use, including guidance on notifying workers about the use of technology, and offering opportunities for workers to consent to or opt out of data collection;

e. Whether you engage with employers to help them implement your products in ways that protect workers' rights, health, and safety—or otherwise take steps to help protect workers who will engage with your products; and

f. Any steps you have taken to ensure that the use of automated worker surveillance and management systems does not infringe on workers' rights.

4. Data and research-related questions we are interested in include:

a. What data and evidence exist on the prevalence of automated worker surveillance and management systems across different industries, occupations, and regions, including changes over time?

b. What data and evidence exist on the impact of automated worker surveillance and management systems on workers, including workers' pay, benefits, and employment, physical and mental health, and ability to exercise workplace rights?

c. What data and evidence exist on the impact of automated worker surveillance and management systems on labor rights, including workers' abilities to form and join unions and bargain collectively with their employers?

d. What data and evidence exist on how the impact of automated worker surveillance and management systems differs across groups of workers, including based on characteristics such as race, national origin, sex, age, disability, religion, or health status?

e. What data or evidence exists on whether automated worker surveillance and management systems are being used for discriminatory purposes or resulting in discrimination?

f. What data and evidence exist on whether automated workers surveillance and management systems impact employers' ability to recruit and retain workers?

g. What data or evidence exists on how the provision of reasonable accommodations is accounted for in the design and operation of automated worker surveillance and management systems?

h. What data and evidence exist on why employers decide to adopt automated worker surveillance and management systems?

i. Are there any existing or new systems that aggregate worker surveillance data across multiple employers?

j. What are new or emergent automated worker surveillance and management systems—or new and emergent uses of existing technologies—that Federal agencies should be tracking?

k. Where might further research, including by the Federal Government, be helpful in understanding the prevalence and impact of automated worker surveillance and management systems?

5. Last, we are especially interested in the following questions about policies, practices, or standards that could protect workers:

a. What guidelines, standards, or best practices might inform the design of automated worker surveillance and management systems to protect workers' rights?

b. Are there policy approaches to regulating automated worker surveillance and management systems from state, Tribal, territorial, or local governments or other countries that Federal agencies could learn from?

c. What policies or actions should Federal agencies consider to protect workers' rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?

Dated: June 13, 2023.

Stacy Murphy,

Deputy Chief Operations Officer/Security Officer.

[FR Doc. 2023–12995 Filed 6–16–23; 8:45 am]

BILLING CODE 3270–F1–P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–97707; File No. SR–NYSENAT–2023–09]

Self-Regulatory Organizations; NYSE National, Inc.; Notice of Filing and Immediate Effectiveness of Proposed Rule Change To Amend Rule 7.37 To Specify the Exchange's Source of Data Feeds From MEMX LLC

June 13, 2023.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (the ''Act''),[1] and Rule 19b–4 thereunder,[2] notice is hereby given that on May 31, 2023, NYSE National, Inc. (''NYSE National'' or the ''Exchange'') filed with the Securities and Exchange Commission (the ''Commission'') the proposed rule change as described in Items I and II below, which Items have been prepared by the self-regulatory organization. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization's Statement of the Terms of Substance of the Proposed Rule Change

The Exchange proposes to amend Rule 7.37 to specify the Exchange's source of data feeds from MEMX LLC (''MEMX'') for purposes of order handling, order execution, order routing, and regulatory compliance. The proposed rule change is available on the Exchange's website at *www.nyse.com,* at the principal office of the Exchange, and at the Commission's Public Reference Room.

[1] 15 U.S.C. 78s(b)(1).

[2] 17 CFR 240.19b–4.